# Руководство по личной безопасности пользователя

Стратегии и решения

# Содержание

# Обзор

## Обзор информации о личной безопасности

В этом руководстве подробно описано, как просмотреть настройки доступа, а также ограничить, закрыть и предотвратить доступ других пользователей к Вашим устройствам Apple, учетным записям и личной информации.


*Примечание.* Это руководство в первую очередь относится к устройствам Apple с новейшей операционной системой (iOS 18, iPadOS 18 и macOS 15), а также к Apple Watch и HomePod.

## Не уверены, что именно Вам нужно?

- В Руководстве по восстановлению безопасности приведены инструкции по быстрому решению проблем.
- Руководство по личной безопасности поможет Вам спланировать свои действия на будущее.

## Ищете решение конкретной проблемы?

- Функция «Проверка безопасности» и контрольные списки (приведены далее) помогут Вам просмотреть и настроить список данных, которыми Вы делитесь, и список людей, имеющих к ним доступ.
- Десятки пошаговых руководств можно найти с помощью поля поиска или просмотреть в оглавлении (слева вверху на каждой странице руководства), а для тематического поиска доступны указатели по темам.

## Проверка безопасности

Функция «Проверка безопасности» помогает быстро просмотреть или изменить настройки доступа приложений и людей к Вашей информации прямо на iPhone с iOS 16 или новее. Чтобы узнать, какая версия iOS у Вас установлена, выберите «Настройки» > «Основные» > «Об этом устройстве». Инструкции по обновлению ПО см. в разделе Обновление программного обеспечения Apple далее в этом руководстве.

Чтобы открыть функцию «Проверка безопасности», на iPhone выберите «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».

Подробнее о функции «Проверка безопасности» (системные требования, руководства, часто задаваемые вопросы) см. в разделе Проверка безопасности далее в этом руководстве.

## Контрольные списки

Функция «Проверка безопасности» удобна для многих пользователей, но в этом руководстве также доступны составленные Apple контрольные списки, с помощью которых Вы можете просмотреть и настроить доступ к своей информации.

- Контрольный список 1. Ограничение доступа к устройству и учетной записи
- Контрольный список 2. Управление данными о геопозиции
- Контрольный список 3. Управление контентом

## Офлайн-ресурсы

Вы можете сохранить эту информацию и просматривать ее офлайн. Для этого выполните любое из указанных действий.

- Загрузите полную версию этого руководства в формате PDF, используя ссылку *Загрузите это руководство* (слева внизу на всех страницах руководства).
- Напечатайте нужные Вам страницы: для этого нажмите сочетание клавиш ⌘-P или нажмите при нажатой клавише Control, а затем выберите «Напечатать страницу». Чтобы ссылки в загруженной копии продолжили работать, выберите вариант «Сохранить как PDF» в левом нижнем углу меню PDF в окне принтера.

## Помощь при других проблемах

- Служба поддержки Apple (https://support.apple.com/): Здесь Вы найдете решения для любых продуктов и сервисов Apple, в том числе руководства пользователя, помощь при забытом пароле и другую информацию.
- Другие ресурсы поддержки (далее в этом руководстве). Если Вам угрожает опасность, Вам могут оказаться полезными дополнительные ресурсы, указанные далее.

Это руководство регулярно обновляется, чтобы у Вас была вся необходимая информация и Вы чувствовали себя в безопасности и защищенности при использовании продукции Apple. См. раздел Что нового далее в этом руководстве.

# Что нового в функциях личной безопасности

## Изменение названия Apple ID

Apple ID теперь называется Аккаунт Apple. Это глобальное изменение, затронувшее все сервисы Apple.

## Обновления в Руководстве по личной безопасности пользователя

Компания Apple внесла ряд изменений в Руководство.

**Новый контент**

- Руководство по восстановлению безопасности. Пошаговые стратегии для различных ситуаций, направленные на незамедлительное решение возникшей проблемы, в том числе срочные меры и альтернативные способы поиска статей на определенную тематику.
- Руководство по личной безопасности. Пошаговые стратегии для различных ситуаций, направленные на предотвращение возникновения проблем в будущем.
- В разделе Настройки сторонних приложений можно узнать о дополнительных мерах обеспечения безопасности в приложениях сторонних разработчиков (не Apple).
- В разделе Дополнительная информация по безопасности можно узнать о возможных последствиях изменений перед их внесением.

**Улучшения**

- Обновлены главная страница и оглавление руководства: теперь можно быстро перейти к инструкциям по решению проблем.
- Изменена структура страницы «Проверка безопасности»: теперь она объединяет разделы «Что делает функция "Проверка безопасности" на iPhone для Вашей безопасности» и «Закрытие доступа к личной информации и защита учетной записи с помощью функции "Проверка безопасности"».
- Контрольные списки теперь включают дополнительные шаги, а также ссылки на страницы с подробной информацией, с помощью которых можно самостоятельно настроить то, что нужно именно Вам. Кроме того, в названия списков добавлены номера (1, 2, 3) для упрощения их запоминания, поиска и добавления ссылок.
- Раздел «Дополнительные соображения при использовании функции "Проверка безопасности"» теперь называется «Дополнительные шаги по обеспечению безопасности», т.к. он содержит информацию, которая может помочь всем пользователям.

# Стратегии и решения

## Руководство по восстановлению безопасности

Если Вы или знакомый Вам человек полагаете, что Вы могли стать жертвой преследования или домогательств посредством технологий в продуктах, связанных с Apple, или хотите оборвать цифровые взаимосвязи с кем-либо, Вам могут помочь нижеперечисленные стратегии. Чтобы связаться с организацией, защищающей интересы и оказывающей поддержку жертвам домогательств, домашнего насилия, преследования или других форм недопустимого поведения, обратитесь к веб-странице Here to Help (Помощь рядом) (https://learn.appleservices.apple/here-to-help).

Если Вы ищете способы предотвратить возможные проблемы, связанные с технологиями, изучите Руководство по личной безопасности далее в этом руководстве.

## Стратегии восстановления безопасности

Шаги, перечисленные далее, помогут Вам контролировать информацию, которой Вы делитесь, и защитить Вами устройства и учетные записи.

**Шаг 1. Безопасность превыше всего**

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность.

Вы можете загрузить или напечатать копию этого Руководства по восстановлению безопасности, чтобы обращаться к нему в будущем: для этого нажмите его при нажатой клавише Control и выберите вариант «Сохранить страницу как» или «Напечатать страницу».

**Шаг 2. Обновление программного обеспечения Apple**

Чтобы Ваше устройство было защищено, на всех Ваших устройствах Apple должна быть установлена новейшая версия операционной системы с новейшими обновлениями системы безопасности и конфиденциальности. Подробнее см. в разделе Обновление программного обеспечения Apple.

*Примечание.* Для обновления устройств может понадобиться время, а аккумуляторы устройств должны быть заряжены. В срочной или экстренной ситуации Вы можете сразу перейти к следующему шагу.

### Шаг 3. Воспользуйтесь пошаговыми инструкциями

Большинство проблем личной безопасности, связанных с технологиями, относятся к предоставлению или получению доступа. Пошаговые инструкции по этим темам доступны в любом из указанных разделов.

- *Проверка безопасности.* Самый быстрый и простой способ просматривать и контролировать настройки доступа прямо на iPhone. Инструкции см. в разделе Проверка безопасности далее в этом руководстве.

  Эта функция доступна на iPhone с iOS 16 или новее. Откройте «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности». (Возможно, потребуется прокрутить вниз.)

- *Контрольные списки.* В iOS 15 или более ранней версии, а также на других устройствах Apple воспользуйтесь инструкциями из указанных разделов далее в этом руководстве.

  - Ограничение доступа
  - Закрытие доступа
  - Управление доступом к геопозиции

### Шаг 4. Дальнейшие действия

Некоторые настройки невозможно просмотреть или изменить с помощью пошаговых инструкций. Изучите эти важные дополнительные шаги.

Это руководство содержит десятки статей по личной безопасности, относящихся к различным устройствам, функциям и настройкам. Если Вам нужна помощь по определенной функции или проблеме, воспользуйтесь указанными вариантами.

- Поле поиска (слева вверху).
- Оглавление этого руководства (слева вверху).
- Указатели статей по темам (далее).

## Принятие срочных мер

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.

### Краткая справка

- Экстренный сброс для быстрого прекращения любого доступа
- Совершение экстренного вызова или отправка экстренного текстового сообщения на iPhone или Apple Watch
- Блокировка вызовов и сообщений от определенных абонентов
- Блокировка чужих попыток входа
- Получение предупреждений о нецензурных или неприемлемых фото и видео
- Безопасное управление аксессуарами в приложении «Дом»
- Управление отпечатками пальцев для Touch ID

### Сбор доказательств

- Запись подозрительной активности
- Получение доказательств, связанных с Аккаунтом Apple другого человека

### Восстановление заводских настроек устройства

Если Вы хотите стереть всю информацию и настройки, в том числе любые приложения, установленные без Вашего ведома, и сбросить настройки конфиденциальности, чтобы закрыть доступ всем людям и приложениям, см. раздел Восстановление заводских настроек устройства.

### Режим блокировки

Если Вы считаете, что могли подвергнуться высокотехнологичной кибератаке, например со стороны частной компании, которая разрабатывает спонсируемое государством узконацеленное шпионское ПО, см. раздел Защита устройств с помощью режима блокировки.

## Помощь в конкретных ситуациях

Рекомендуется всегда начинать с шагов 1–4, приведенных выше, но в дальнейших разделах Вы можете быстро найти статьи, которые могут быть полезны в конкретной ситуации.

### Другой человек всегда знает, где я нахожусь

Это может быть одна из следующих ситуаций: другой человек имеет доступ к Вашему Аккаунту Apple; Вы состоите в группе Семейного доступа; Вы предоставили общий доступ к геопозиции или контенту (например, общим календарям или фото, опубликованным в социальных сетях или общих календарях).

Начните с шагов 1–4, приведенных выше. Если на шаге 3 Вы используете контрольные списки, начните с пунктов Ограничение доступа и Управление доступом к геопозиции.

### Мне не удается войти в свой Аккаунт Apple

Чтобы восстановить доступ к своему Аккаунту Apple, изучите статьи службы поддержки Apple, перечисленные далее.

- Если вы считаете, что ваша учетная запись Apple скомпрометирована
- Аккаунт Apple заблокирован, неактивен или отключен
- Если вы забыли пароль от Аккаунта Apple
- Восстановление учетной записи в случае, если сбросить пароль учетной записи Apple не удается

После восстановления доступа изучите указанный ресурс.

- Изменение Аккаунта Apple — статья службы поддержки Apple
- Обеспечение надежности паролей Вашего устройства, приложений и сайтов
- Как избежать потери доступа к Аккаунту Apple и устройству
- Способы предотвратить возможные проблемы в будущем: Руководство по личной безопасности

### Кто-то заблокировал мое устройство, или я не могу его разблокировать

Чтобы восстановить доступ, см. статью службы поддержки Apple Если вы забыли код-пароль для iPhone или ваш iPhone заблокирован.

После восстановления доступа изучите указанные ресурсы, чтобы защитить свое устройство в будущем.

- Контрольный список 1. Ограничение доступа к устройству и учетной записи
- Установка уникального код-пароля или пароля устройства
- Используйте Touch ID для защиты своих устройств и удалите неизвестные отпечатки пальцев.
- Защитите свои устройства с помощью Face ID (для iPhone или iPad).
- Добавьте контакт для восстановления доступа к учетной записи.
- Примите меры предосторожности, указанные в Руководстве по личной безопасности.

### Я хочу уйти из дома или прекратить отношения, в которых я ощущаю себя в опасности

Чтобы связаться с организацией, защищающей интересы и оказывающей поддержку жертвам домогательств, домашнего насилия, преследования или других форм недопустимого поведения, обратитесь к веб-странице Here to Help (Помощь рядом) (https://learn.appleservices.apple/here-to-help).

1. Используя пошаговые инструкции, приведенные выше, проверьте настройки доступа и внесите необходимые изменения, если Вы считаете, что это будет безопасно для Вас.
2. Изучите список срочных мер, чтобы узнать о блокировке, сборе доказательств и других аспектах.
3. Изучите дополнительные шаги по обеспечению безопасности: в этом разделе описаны нежелательные уведомления об отслеживании, сторонние учетные записи, тарифные планы сотовой связи и другие аспекты.

### Мне нужно защитить другого человека

## Доступ к Вашим устройствам

Изучите Контрольный список 1. Ограничение доступа к устройству и учетной записи

Также изучите эти разделы:

- Установка уникального код-пароля или пароля
- Как предотвратить потерю доступа к своему устройству
- Использование режима блокировки

Чтобы изучить другие статьи о защите устройств и учетных записей, откройте раздел оглавления (в левом верхнем углу) «Ограничение доступа к устройству и учетной записи — статьи».

## Ваша геопозиция

Изучите Контрольный список 2. Управление данными о геопозиции.

Также изучите эти разделы:

- Сохранение конфиденциальности истории просмотра в Safari и Картах

## Ваш контент

Изучите Контрольный список 3. Управление контентом.

Также изучите эти разделы:

- Безопасно управляйте перенаправлением контента: почты, текстовых сообщений и вызовов
- Предупреждения о неприемлемых изображениях и видео
- Управление настройками общего доступа к данным Фото
- Управление доступом к метаданным о геопозиции в приложении «Фото»

### Ваши приложения и веб-браузер

- Безопасность паролей
- Управление общими паролями и ключами входа
- Функции конфиденциальности приложений
- Проверка и удаление приложений
- Настройки сторонних приложений
- Конфиденциальность истории просмотра в Safari
- Сообщения
  - Настройки безопасности
  - Блокировка вызовов и сообщений от определенных абонентов
  - Использование функции «На связи»
- Фото
  - Управление настройками общего доступа к данным Фото
  - Управление доступом к метаданным

### Ваша семья и Ваш дом

- Семейный доступ
- Домашние аксессуары

### Какими устройствами Вы пользуетесь?

**iPhone, iPad и Mac**

Почти все содержимое Руководства по личной безопасности пользователя относится к iPhone, iPad и Mac.

- О том, как просмотреть, ограничить или запретить доступ других людей к Вашим устройствам, учетным записям или личной информации, см. в разделе Стратегии восстановления безопасности ранее в этом руководстве.
- Если Вы хотите заранее предотвратить доступ других людей, см. раздел Руководство по личной безопасности.
- Дополнительные способы получения разнообразной информации из этого руководства описаны в обзоре.

Другие темы, относящиеся к этим устройствам, описаны в Руководстве пользователя iPhone, Руководстве пользователя iPad и Руководстве пользователя Mac.

### Apple Watch

Информация о личной безопасности, относящаяся к Apple Watch, приведена в этих разделах:

- Управление отправкой данных об активности на Apple Watch
- Управление доступом к геопозиции с помощью Локатора
- Совершение экстренного вызова
- Безопасность NameDrop (меры предосторожности)
- Использование функции «На связи» для Сообщений (меры предосторожности)

Другие темы описаны в Руководстве пользователя Apple Watch.

### Домашние аксессуары

Информация о личной безопасности, относящаяся к приложению «Дом», приведена в разделе Безопасное управление аксессуарами в приложении «Дом».

Другие темы описаны в Руководстве пользователя приложения «Дом».

### AirTag

Информация о личной безопасности, относящаяся к AirTag, приведена в разделе Обнаружение нежелательного отслеживания.

Чтобы получить информацию на другие темы, введите «AirTag» в поле поиска на сайте службы поддержки Apple.

Дата публикации: 28 октября 2024 г.

# Руководство по личной безопасности

Эта страница предназначена для всех, кто хочет заранее защитить себя от возможного преследования, домогательств или травли с применением технологий. Если Вы уже столкнулись с такими проблемами, изучите Руководство по восстановлению безопасности ранее в этом документе. Другие способы поддержки, доступные для продуктов и сервисов Apple, перечислены в разделе Другие ресурсы поддержки далее в этом документе.

## Стратегии обеспечения безопасности

Apple предлагает множество функций, помогающих обеспечить Вашу безопасность и конфиденциальность. Далее приведены некоторые способы задействовать их.

**Уровень 1. Минимальная защита**

В качестве первой линии защиты все пользователи должны принять следующие меры по защите своих устройств и Аккаунта Apple.

- Обновите программное обеспечение Apple на всех своих устройствах Apple, чтобы у Вас были установлены новейшие обновления систем безопасности и конфиденциальности. См. раздел «Обновите программное обеспечение Apple». Подробнее см. в разделе Обновление программного обеспечения Apple.
- Защита доступа к Вашим устройствам:
  - Установка уникального код-пароля или пароля.
  - Защита iPhone или iPad с помощью Face ID.
  - Управление отпечатками пальцев для Touch ID.
  - Управление общими паролями и ключами входа.

Защита Вашего Аккаунта Apple:

- Поддержание безопасности Аккаунта Apple.
- Использование двухфакторной аутентификации.
- Назначение контакта для восстановления доступа к учетной записи.

**Уровень 2. Улучшенная защита**

В дополнение к уровню 1 примите меры для защиты Ваших приложений и связанных с ними паролей, а также настройте доступ приложений к Вашим данным.

- Повышение надежности паролей Вашего устройства, приложений и сайтов.
- Конкретные настройки доступа:
  - Используйте «Управление доступом» в функции «Проверка безопасности» на iPhone с iOS 16 или новее.
  - Контрольный список 3. Управление контентом (на других устройствах либо в iOS 15 или более ранней версии).
  - Безопасность AirDrop.
  - Безопасность NameDrop.
  - Управление общими группами вкладок в Safari
  - Управление настройками функции «Отправлено Вам».

- Управление конфиденциальностью приложений:
  - Функции конфиденциальности приложений.
  - Проверка и удаление приложений.
  - Настройки сторонних приложений.
  - Safari и Карты: Сохранение конфиденциальности истории просмотра.

**Уровень 3. Наилучшая защита**

В дополнение к уровням 1 и 2 изучите инструменты Apple для обеспечения личной безопасности и выработайте привычку поддерживать наивысший уровень безопасности.

- Будьте готовы
  - Включите уведомления об отслеживании
  - Борьба с мошенническими запросами данных.
  - Блокировка чужих попыток входа.
  - Как заблокировать определенных людей.
  - Сообщения, AirDrop, FaceTime: Настройте предупреждения об откровенном контенте.
  - Используйте функцию «На связи» для Сообщений, чтобы автоматически сообщать другу о том, что Вы добрались домой.
  - Узнайте, как совершить экстренный вызов или отправить экстренное сообщение (доступно на iPhone или Apple Watch; зависит от страны или региона).
- Сделайте безопасность своей привычкой
  - Примите дополнительные меры, чтобы защитить свои учетные записи помимо Аккаунта Apple, сторонние приложения, пароли и социальные сети, а также приложение «Дом», Apple Wallet и Семейный доступ.
  - Регулярно выполняйте Проверку безопасности на iPhone с iOS 16 или новее, чтобы проверять, какими данными Вы делитесь.

Дополнительные действия

- Управление отпечатками пальцев для Touch ID.
- Защита устройств с помощью режима блокировки.
- Управление настройками безопасности в приложении «Сообщения».
- Получение доказательств, связанных с Аккаунтом Apple другого человека.

Дата публикации: 28 октября 2024 г.

# Проверка безопасности

## Проверка безопасности на iPhone с iOS 16 или новее

Функция «Проверка безопасности», доступная в приложении «Настройки» на iPhone с iOS 16 или новее, позволяет Вам быстро просматривать и обновлять настройки доступа, а также закрывать доступ к данным для отдельных людей и приложений. Функция «Проверка безопасности» предлагает две возможности.

- Вы можете просматривать параметры доступа, управлять ими и вносить конкретные изменения.
- Выполнив Экстренный сброс, Вы можете немедленно закрыть доступ к любым своим данным.

Чтобы открыть функцию «Проверка безопасности», на iPhone выберите «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.

### Необходимые условия

- У Вас должен быть iPhone с iOS 16 или новее.
  - Чтобы узнать, какая версия iOS у Вас установлена, выберите «Настройки» > «Основные» > «Об этом устройстве».
  - Чтобы обновить iOS 15.8.3 или более ранней версии, выберите «Настройки» > «Основные» > «Обновление ПО». Дополнительные варианты описаны в разделе Обновление программного обеспечения Apple.
- Для Вашего Аккаунта Apple должна быть включена двухфакторная аутентификация.
- Вы должны выполнить вход в разделе «Настройки» > [*Ваше имя*] на iPhone.

*Примечание.* Если на Вашем iPhone включена функция «Защита украденного устройства», функция «Проверка безопасности» может работать немного иначе. Подробнее см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone.

### Альтернативный вариант. Контрольные списки

Если Вы пользуетесь другим устройством (iPad, Mac) или при использовании функции «Проверка безопасности» возникли проблемы, можно настроить параметры доступа вручную по контрольным спискам, указанным далее.

- Контрольный список 1. Ограничение доступа к устройству и учетной записи
- Контрольный список 2. Управление данными о геопозиции
- Контрольный список 3. Управление контентом

## Обзор

С помощью функции «Проверка безопасности» на iPhone Вы можете быстро закрыть доступ к своим данным, а также просматривать и обновлять настройки доступа для отдельных людей и приложений. Вы можете выполнить любые из указанных действий:

- Проверить, с кем Вы делитесь информацией.
- Просмотреть и удалить устройства, подключенные к Вашему Аккаунту Apple.
- Сбросить системные права доступа для приложений.
- Сменить код-пароль своего iPhone.
- Сменить пароль своего Аккаунта Apple.
- Внести другие изменения.


## Меры предосторожности перед началом

**ВАЖНО!** Планируйте свои действия заранее.

- Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.
- Функция «Выйти сейчас» помогает Вам быстро защитить свою конфиденциальность. Чтобы немедленно закрыть приложение «Настройки» и вернуться на экран «Домой», коснитесь «Выйти сейчас» (в правом верхнем углу всех экранов функции «Проверка безопасности». Любые изменения, которые Вы внесли до использования кнопки «Выйти сейчас», сохраняются.
- Чтобы снова предоставить кому-либо доступ после использования функции «Проверка безопасности», просто откройте приложение или сервис, в которых находится контент, и снова поделитесь этим контентом. Некоторые приложения и сервисы могут уведомлять Вас, если Вы снова начали делиться информацией.

С помощью функции «Проверка безопасности» можно посмотреть, с кем Вы делитесь информацией, разрешить использование Сообщений и FaceTime только на Вашем iPhone, сбросить системные права доступа для приложений, сменить код-пароль, сменить пароль Аккаунта Apple и выполнить другие действия.

Чтобы снова предоставить кому-либо доступ после использования функции «Проверка безопасности», откройте приложение или сервис, в которых находится контент, и снова поделитесь этим контентом.

Если у Вас включена функция «Защита украденного устройства», функция «Проверка безопасности» может работать немного иначе. Подробнее о защите украденного устройства см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone (https://support.apple.com/HT212510).

*Примечание.* Если на Вашем iPhone включены ограничения Экранного времени или установлен профиль управления мобильными устройствами (MDM), Вы можете использовать функцию «Проверка безопасности», но некоторые возможности могут быть недоступны.

## Что требуется для использования функции «Проверка безопасности»?

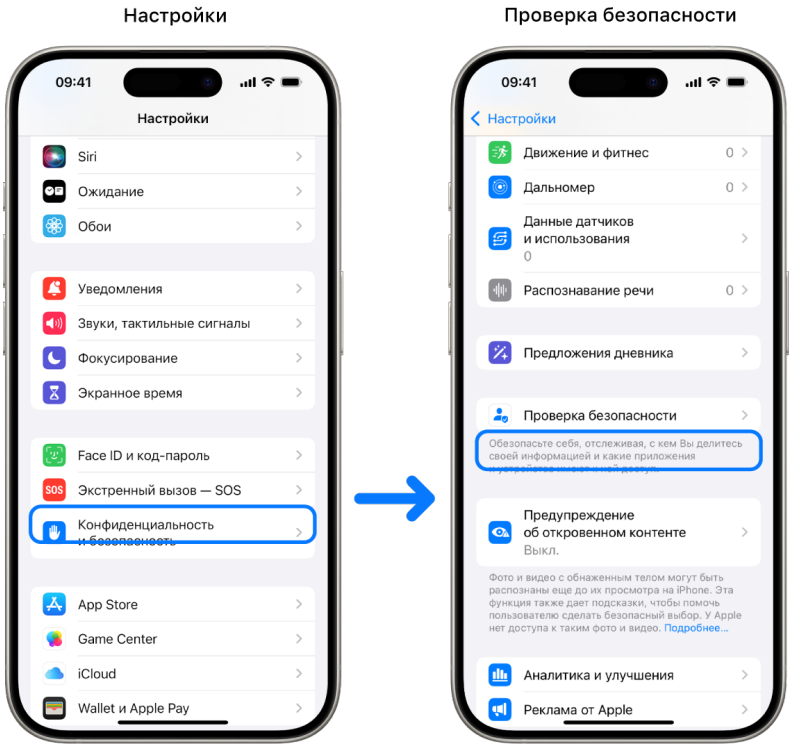
Функция «Проверка безопасности» доступна только на iPhone с iOS 16 или новее. Для использования функции «Проверка безопасности» требуется Аккаунт Apple с включенной двухфакторной аутентификацией. Вы также должны выполнить вход в меню «Настройки» > [*Ваше имя*] на iPhone. (Чтобы узнать, какая версия ПО установлена на Вашем устройстве, выберите «Настройки» > «Основные», затем коснитесь «Об устройстве».)

Чтобы открыть функцию «Проверка безопасности», выберите «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности». (Возможно, потребуется прокрутить вниз.)

*Примечание.* Если у Вас нет доступа к функции «Проверка безопасности» или возникли проблемы с ее использованием, Вы можете вручную изменить настройки доступа к информации, Вашему устройству и учетным записям. См. раздел Контрольный список 3. Управление контентом далее в этом руководстве.

### Шаг 1. Откройте Проверку безопасности

На iPhone выберите «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности». (Возможно, потребуется прокрутить вниз.)

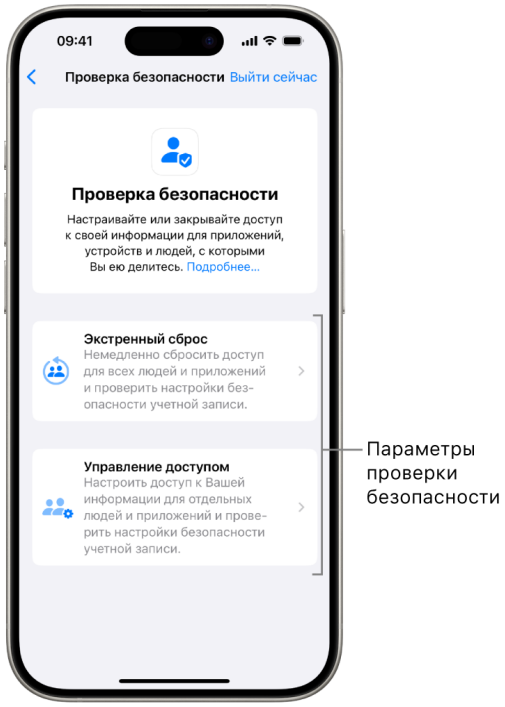


### Шаг 2. Выберите действие

Функция «Проверка безопасности» предлагает две возможности управлять доступом и безопасностью учетной записи.

- *Экстренный сброс*. Немедленное полное закрытие доступа для всех людей и приложений.
- *Управление доступом*. Просмотр и настройка параметров доступа для отдельных людей и приложений.

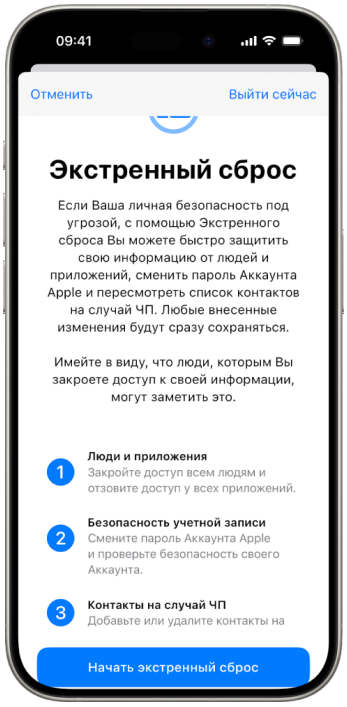
Описания параметров, которые можно изменить с помощью функции «Проверка безопасности», см. в разделе Часто задаваемые вопросы о функции «Проверка безопасности» далее в этом руководстве.



### Экстренный сброс

С помощью функции «Экстренный сброс» можно выполнить указанные действия.

- Быстро закрыть доступ для всех людей и приложений (подробнее см. в разделе «Часто задаваемые вопросы о функции "Проверка безопасности"»).
- Просмотреть контакты на случай ЧП.
- Просмотреть устройства, подключенные к Вашему Аккаунту Apple.
- Просмотреть номера телефонов, которые используются для подтверждения Вашей личности.
- Сменить пароль Аккаунта Apple и просмотреть настройки безопасности устройства и учетной записи.



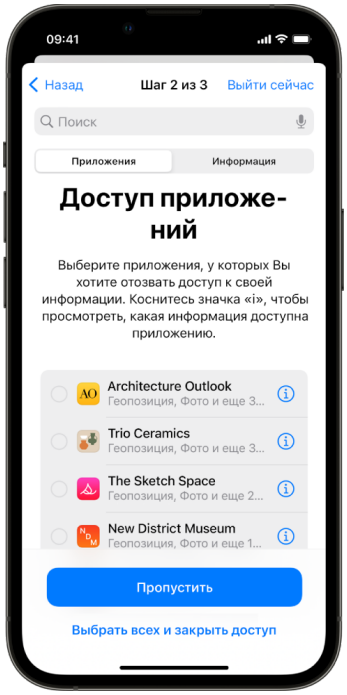

- Коснитесь «Экстренный сброс», затем следуйте инструкциям на экране. Внесенные Вами изменения сохраняются сразу.

  *Примечание.* Если у Вас включена функция «Защита украденного устройства», функция «Проверка безопасности» может работать немного иначе. Подробнее о защите украденного устройства см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone (https://support.apple.com/HT212510).

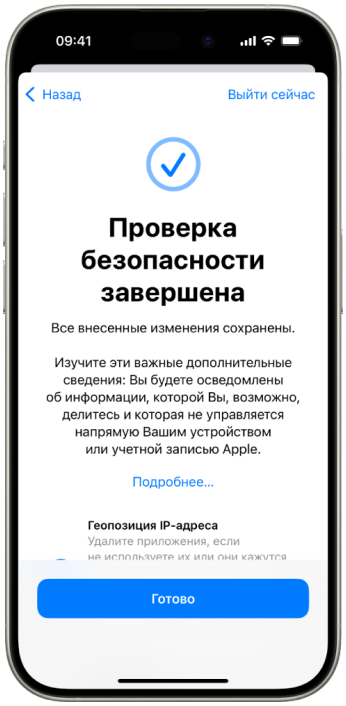
### Управление доступом

В разделе «Управление доступом» Вы можете просмотреть, какой информацией Вы делитесь с людьми и к какой информации имеют доступ приложения, а также изменить настройки доступа к своим данным и параметры безопасности устройства и Аккаунта Apple. Выполните указанные 5 шагов.

1. Коснитесь «Управление доступом». (Изменения сохраняются по мере их внесения.)
2. Чтобы просмотреть настройки доступа или закрыть доступ к информации другим людям, выполните одно из двух указанных действий.
   - *Коснитесь «Люди».* Выберите людей в списке, просмотрите информацию, которой Вы делитесь с людьми, затем выберите информацию, которой Вы больше не хотите делиться с выбранными людьми.
   - *Коснитесь «Информация»* Выберите приложения в списке, просмотрите информацию, которой Вы делитесь с людьми, затем выберите информацию, которой Вы больше не хотите делиться с выбранными людьми.
3. Чтобы просмотреть настройки доступа или закрыть доступ к информации другим приложениям, выполните одно из двух указанных действий.
   - *Коснитесь «Приложения».* Выберите приложения в списке, просмотрите информацию, которой Вы делитесь с ними, затем выберите информацию, которой Вы больше не хотите делиться с выбранными приложениями.
   - *Коснитесь «Информация»* Выберите тип информации в списке, просмотрите информацию, которой Вы делитесь с приложениями, затем выберите информацию, которой Вы больше не хотите делиться с выбранными приложениями.



4. Коснитесь «Продолжить», затем выполните одно из указанных действий.
   - Просмотрите и удалите устройства, подключенные к Вашему Аккаунту Apple.
   - Просмотрите и обновите номера телефонов, которые используются для подтверждения Вашей личности.
   - Обновите пароль своего Аккаунта Apple.
   - Добавьте или обновите контакты на случай ЧП.
   - Измените код-пароль устройства или информацию Face ID или Touch ID.
   - Просмотрите и удалите компьютеры, синхронизированные с устройством (только в iOS 17 или новее).
   - Если у Вас есть iCloud+ и Вы еще не включили Частный узел, включите эту функцию (только в iOS 17 или новее).
5. Коснитесь «Готово».



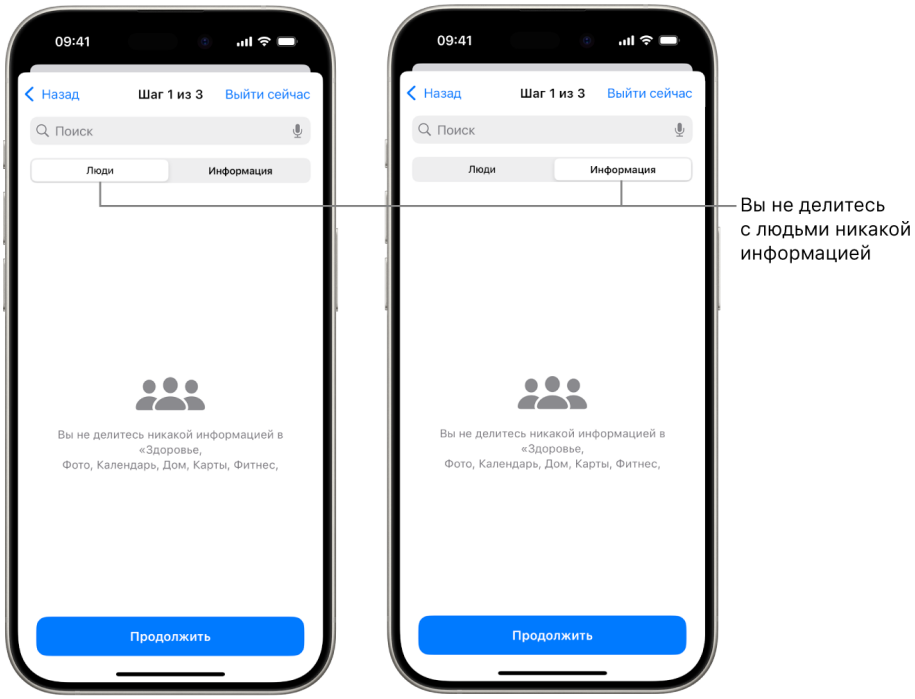

6. По завершении перейдите к следующему разделу и убедитесь, что доступ закрыт.

   **ВАЖНО!** Изучите дополнительные шаги далее в этом руководстве, чтобы узнать, какими еще способами можно защитить Вашу конфиденциальную информацию.

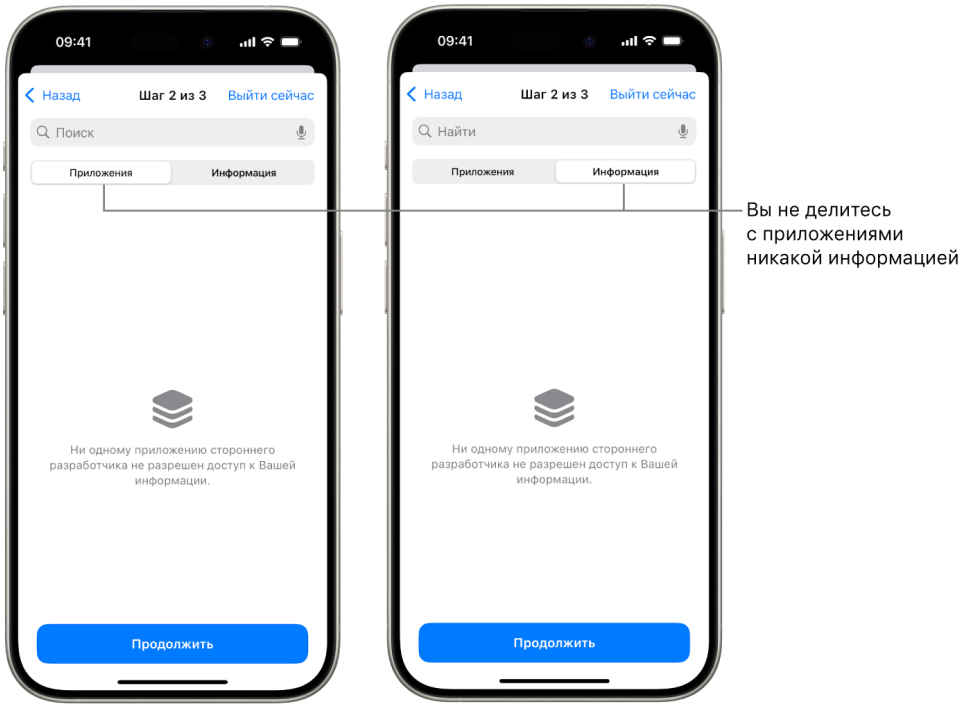
### Шаг 3. Проверьте внесенные изменения

После использования функции «Проверка безопасности» Вы можете проверить все изменения параметров доступа, внесенные в ходе этих 4 шагов.

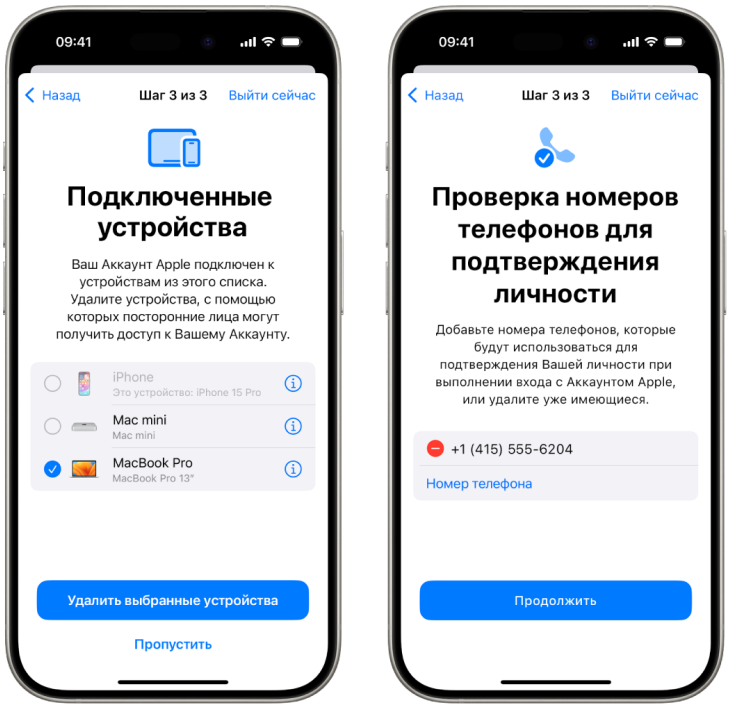
1. Коснитесь кнопки «Назад» (либо завершите и снова откройте функцию «Проверка безопасности»).
2. Убедитесь, что параметры доступа к информации, которой Вы делитесь с людьми, теперь соответствуют желаемым Вами.



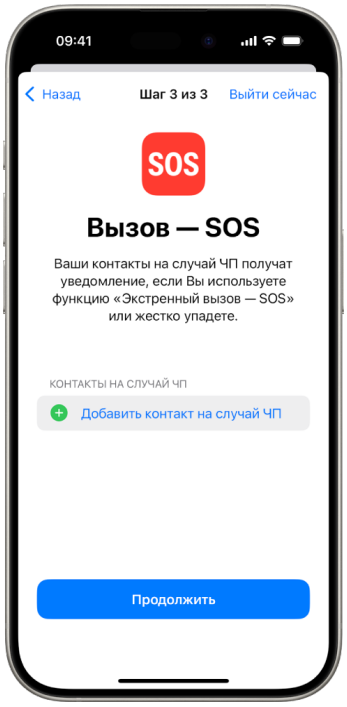
3. Убедитесь, что параметры доступа к информации, которой Вы делитесь с приложениями, теперь соответствуют желаемым Вами.



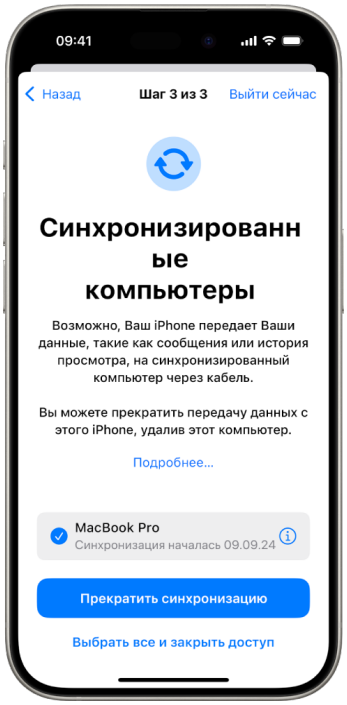

4. Убедитесь, что сохранены перечисленные ниже изменения, внесенные в учетную запись.
   - Устройства, подключенные к Вашему Аккаунту Apple.
   - Номера телефонов, которые используются для подтверждения Вашей личности.



- Добавленные или измененные контакты на случай ЧП.




- Удаленные компьютеры, синхронизированные с устройством.



### Где не действует Проверка безопасности

С помощью функции «Проверка безопасности» невозможно просмотреть или изменить параметры доступа к некоторым типам информации, указанным далее.

- Учетные записи и пароли, не относящиеся к Apple.
- Параметры доступа к социальным сетям.
- Устройства, на которых Вы вошли в другую учетную запись iCloud.
- Параметры доступа, предоставленного для других приложений на iPad или Mac.

## Часто задаваемые вопросы о функции «Проверка безопасности»

### Для каких приложений и функций Apple можно просмотреть или изменить параметры доступа с помощью функции «Проверка безопасности»?

Далее указаны приложения Apple, для которых можно просмотреть параметры доступа или закрыть доступ к данным для других людей с помощью функции «Проверка безопасности».

| Приложение | Информация, доступом к которой можно управлять |
|---|---|
|  | Активность |
|  | Дом |
|  | Здоровье |
|  | На связи |
|  | Общая геопозиция в Локаторе |
|  | Общие вещи в Локаторе |
|  | Общие заметки |
|  | Общие календари |
|  | Общие пароли |
|  | Общие фото (в том числе общая медиатека и общие альбомы) |
|  | Сообщения о прибытии в Картах |

## Для каких сторонних приложений можно просмотреть или изменить параметры доступа с помощью функции «Проверка безопасности»?

Далее указаны типы данных, к которым можно закрыть доступ для сторонних приложений с помощью функции «Проверка безопасности».

| | |
|---|---|
|  | Bluetooth® |
|  | Календари |
|  | Камера |
|  | Контакты |
|  | Файлы и папки |
|  | Здоровье |
|  | Локальная сеть |
|  | Службы геолокации |
|  | Медиафайлы и Apple Music |
|  | Микрофон |
|  | Движение и фитнес |
|  | Фото |
|  | Напоминания |
|  | Исследование |
|  | Распознавание речи |

### Какие изменения можно внести в Аккаунт Apple с помощью функции «Проверка безопасности»?

С помощью функции «Проверка безопасности» Вы можете изменить информацию, связанную с Вашим Аккаунтом Apple. Например:

- Просмотреть и удалить устройства, на которых выполнен вход в Вашу учетную запись.
- Просмотреть и изменить доверенные телефонные номера.
- Сменить пароль своего Аккаунта Apple.
- Изменить контакты на случай ЧП.
- Изменить код-пароль устройства и информацию Face ID или Touch ID.

Если у Вас включена функция «Защита украденного устройства», функция «Проверка безопасности» может работать немного иначе. Подробнее о защите украденного устройства см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone (https://support.apple.com/HT212510).

### Для чего предназначена кнопка «Выйти сейчас»?

Человеку, ставшему жертвой агрессивного поведения, может быть необходимо быстро скрыть факт использования функции «Проверка безопасности». Кнопка «Выйти сейчас» позволяет сделать это мгновенно.

## Дополнительные шаги по обеспечению безопасности

Большинство таких проблем личной безопасности относятся к предоставлению или получению доступа. Пошаговые инструкции по этим темам доступны в указанных разделах.

- *Проверка безопасности.* На iPhone с iOS 16 или новее выберите «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности» либо изучите раздел Проверка безопасности.
- *Контрольные списки.* Для более ранних версий iOS или других устройств см. контрольные списки: Ограничение доступа, Закрытие доступа или Управление доступом к геопозиции.

Некоторые настройки невозможно просмотреть или изменить с помощью функции «Проверка безопасности» или контрольных списков. Чтобы дополнительно ограничить доступ, выполните шаги, указанные далее.

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.

### Шаги, не связанные с технологиями Apple

#### Приложения сторонних разработчиков

Установленные на устройстве приложения могут собирать информацию о Вашей приблизительной геопозиции. Учитывая возможное влияние этих факторов на Вашу безопасность, Вы можете просмотреть список установленных приложений и удалить те приложения, которые Вы не используете или не узнаете. См. разделы Проверка и удаление приложений и Настройки сторонних приложений.

#### Учетные записи и пароли, не относящиеся к Apple.

Защитите важную личную информацию в своих учетных записях, например для банкинга, покупок, электронной почты, социальных сетей и учебы:

- Смените пароли своих учетных записей.
- Просмотрите настройки безопасности и конфиденциальности.
- Просмотрите учетные записи, которые Вы используете для общения (электронной почты, телефонных вызовов, сообщений) и убедитесь, что никакие данные не передаются без Вашего разрешения.

### Учетные записи для социальных сетей, интернет-магазинов и других задач

При публикации фото и другой личной информации в социальных сетях, в интернет-магазинах и на других сайтах Вы можете случайно раскрыть сведения о своей геопозиции и личной жизни. Выполните указанные действия.

- Проверьте настройки конфиденциальности и безопасности в своих учетных записях социальных сетей, интернет-магазинов и онлайн-сервисов.
- Проверьте списки своих контактов и подписчиков
- Внимательно следите за тем, что Вы публикуете, чтобы сохранить необходимый Вам уровень конфиденциальности.
- Управление доступом к метаданным о геопозиции в приложении «Фото»

  См. раздел Управление доступом к метаданным о геопозиции в приложении «Фото далее в этом руководстве.

### Другие устройства, которыми Вы владеете или которые Вы используете

Проверьте настройки общего доступа на любых других устройствах, которые Вы используете, чтобы обеспечить безопасность своей информации. Инструкции приведены в контрольном списке Ограничение доступа к устройству и учетной записи. Если рядом с Вами есть кто-то еще, например ребенок или друг, помните, что их устройства также могут передавать информацию.

### Сотовый тариф

Если у Вас совместный сотовый тариф, возможно, другие пользователи этого тарифа могут просматривать Вашу геопозицию, а также детали вызовов, сообщений и расходов на связь. Обратитесь к оператору, чтобы узнать подробнее о своем тарифе, а также о дополнительных мерах безопасности, которые можно использовать для Вашей учетной записи, например требовании ввода PIN-кода или кода безопасности для внесения изменений.

Если у Вас не совместный сотовый тариф, но у другого человека есть онлайн-доступ к Вашей учетной записи сотовой связи, он также может просматривать Вашу геопозицию, а также детали вызовов, сообщений и расходов на связь. Учитывая возможное влияние этих факторов на Вашу безопасность, Вы можете сменить свои пароли, PIN-коды и другие параметры безопасности, связанные с Вашим тарифным планом сотовой связи.

## Шаги, связанные с технологиями Apple

### Нежелательное отслеживание

Включите уведомления, чтобы обнаруживать источники нежелательного отслеживания (например, AirTag и аксессуары в сети Локатора). Чтобы получать оповещения, если такой аксессуар перемещается вместе с Вами, включите:

- Bluetooth
- Службы геолокации
- Уведомления об отслеживании (откройте приложение «Локатор», коснитесь «Я», прокрутите до раздела «Настроить уведомления об отслеживании», затем включите «Допуск уведомлений»)

  См. раздел Обнаружение нежелательного отслеживания далее в этом руководстве.

### Дом и HomeKit

Если Вы добавлены в дом, управляемый приложением Apple «Дом», и решили удалить себя, помните, что человек, управляющий домом, по-прежнему может использовать аксессуары HomeKit, например камеры, что может влиять на Вашу личную безопасность.

См. раздел Безопасное управление аксессуарами в приложении «Дом» далее в этом руководстве.

### Apple Wallet

Если Вы используете платежные карты или ключи доступа в Apple Wallet совместно с другим человеком, этот человек может просматривать историю Ваших покупок или время, когда Вы отпирали двери.

Сведения о финансовых транзакциях также могут быть доступны через общие банковские счета и общие кредитные карты, а также в том случае если у другого человека есть онлайн-доступ к Вашим финансовым учетным записям. Чтобы просмотреть свои недавние транзакции и журналы, откройте приложение Apple Wallet. Учитывая возможное влияние этих факторов на Вашу безопасность, Вы можете сменить пароли, связанные с Вашими банковскими и кредитными картами.

### Семейный доступ

Если Вы входите в группу Семейного доступа Apple, организатор Семейного доступа может просматривать Ваши покупки и изменять настройки на устройстве ребенка. Чтобы выйти из группы Семейного доступа, перейдите в Настройки, коснитесь своего имени и откройте настройки Семейного доступа. Детскую учетную запись нельзя удалить из группы Семейного доступа, но можно переместить ее в другую группу Семейного доступа или просто удалить связанный с ней Аккаунт Apple.

См. раздел Управление настройками Семейного доступа далее в этом руководстве.

*Примечание.* Чтобы проверить, состоите ли Вы в группе Семейного доступа, выберите «Настройки» > [*Ваше имя*] > вкладку «Семейный доступ». Если отобразятся имена членов Вашей семьи, то Вы состоите в группе Семейного доступа.

# Контрольные списки для устройств с iOS 15 или более ранней версии

## Контрольный список 1. Ограничение доступа к устройству и учетной записи

Защита доступа к Вашим устройствам и Аккаунту Apple исключительно важна для обеспечения технологических аспектов Вашей личной безопасности. В этом контрольном списке перечислены настройки, которые Вы можете просмотреть и изменить, чтобы Ваше устройство передавало данные только тем людям, которым Вы хотите предоставлять доступ.

**ВАЖНО!** На iPhone с iOS 16 или новее можно использовать функцию «Проверка безопасности».

**ВАЖНО!** На iPhone с iOS 16 или новее можно использовать функцию «Проверка безопасности», описанную ранее в этом руководстве.


### Ограничение доступа к Вашим устройствам

1. Проверьте, на каких устройствах выполнен вход в Ваш Аккаунт Apple. Для этого выберите «Настройки» > [*Ваше имя*] > «Устройства». Если какое-то из устройств Вам незнакомо, коснитесь его имени и выберите «Удалить из учетной записи». Подробнее см. в разделе Поддержание безопасности Аккаунта Apple далее в этом руководстве.
2. Убедитесь, что на устройство добавлены только нужные Вам данные о внешности для Face ID или отпечатки пальцев для Touch ID. См. информацию о Face ID и Touch ID далее в этом руководстве.

3. Проверьте личную информацию и параметры безопасности своего Аккаунта Apple на сайте Аккаунта Apple. Подробнее см. в разделе Поддержание безопасности Аккаунта Apple далее в этом руководстве.
4. Если Вы используете двухфакторную аутентификацию, проверьте свой список доверенных устройств и убедитесь,что в нем нет незнакомых Вам устройств. См. раздел о двухфакторной аутентификации далее в этом руководстве.
5. Просмотрите приложения, установленные на устройстве, и убедитесь, что в списке нет незнакомых Вам приложений или приложений, об установке которых Вы не помните. Инструкции см. в разделе Проверка и удаление приложений далее в этом руководстве.
6. Убедитесь, что на устройстве не установлен неизвестный Вам профиль конфигурации для управления мобильными устройствами (MDM). Профили MDM обычно устанавливаются работодателями, учебными заведениями или другими официальными организациями. Инструкции см. в разделе Просмотр и удаление профилей конфигурации далее в этом руководстве.
7. Проверьте и настройте параметры доступа к своим данным, используя Контрольный список 3. Управление контентом далее в этом руководстве.

# Контрольный список 2. Управление данными о геопозиции


Для iPhone с iOS 15 или более ранней версии используйте этот контрольный список, чтобы ограничить список тех, кто имеет право просматривать Вашу геопозицию, или полностью закрыть к ней доступ. Для iPhone с iOS 16 или новее см. раздел Проверка безопасности.

1. Если Вы не используете новейшую версию iOS, iPadOS или macOS и считаете, что кто-то мог получить доступ к Вашему устройству, Вы можете восстановить заводские настройки на устройстве. При восстановлении заводских настроек стираются все данные и настройки на устройстве. В том числе стираются любые приложения, установленные без Вашего ведома, и сбрасываются настройки конфиденциальности, чтобы у людей и приложений не было доступа к Вашей геопозиции. При восстановлении заводских настроек также устанавливается новейшая версия операционной системы. Чтобы восстановить заводские настройки, обратитесь к разделу Восстановление заводских настроек устройства.

2. Чтобы закрыть доступ к геопозиции для всех приложений, служб и сервисов (даже на короткое время), выберите «Настройки» > «Конфиденциальность» > «Службы геолокации» и выключите доступ к геопозиции. После этого все приложения на Вашем устройстве, даже Карты, не смогут использовать Вашу геопозицию. Никто не узнает, что Вы выключили Службы геолокации, но без доступа к Вашей геопозиции некоторые функции могут начать работать не так, как ожидалось.

   *Примечание.* Вы также можете временно выключить функцию «Найти iPhone» в той же вкладке, если полагаете, что кто-то мог получить доступ к Вашей учетной записи iCloud. В списке приложений с доступом к геопозиции коснитесь Локатора, затем выберите «Никогда».

3. Чтобы прекратить делиться своей геопозицией с определенными приложениями и сервисами, выберите «Настройки» > «Конфиденциальность» > «Службы геолокации», затем выберите приложения и сервисы, которым Вы хотите закрыть доступ. Коснитесь названия приложения, затем для параметра «Разрешать доступ к геопозиции» выберите «Никогда».

4. Чтобы перестать делиться своей геопозицией с определенным человеком, в приложении Локатор коснитесь «Люди», выберите человека, затем коснитесь «Не делиться геопозицией» внизу экрана.

   Если Вы сначала предоставили, а потом закрыли доступ к своей геопозиции в Локаторе, то другой человек не получит уведомление о закрытии доступа и не увидит Вас в своем списке друзей. Если Вы возобновите доступ, другой человек получит уведомление о том, что Вы делитесь с ним своей геопозицией.

5. Чтобы перестать делиться своим примерным временем прибытия в Картах, откройте «Карты», выберите «Избранное», чтобы открыть окно со всеми геопозициями, которые Вы отметили как избранные. Коснитесь ⓘ рядом с каждой геопозицией, для которой хотите изменить настройки автоматической отправки примерного времени прибытия, затем прокрутите вниз к разделу «Уведомление контактов о прибытии» и удалите пользователей, которым нужно закрыть доступ.

6. Чтобы проверить, геопозиции каких Ваших устройств и аксессуаров в данный момент доступны через сеть Локатора людям, имеющим доступ к Вашему Аккаунту Apple, откройте «Локатор» > «Устройства» и просмотрите список. Если в списке есть незнакомое устройство и Вы хотите удалить его, коснитесь названия этого устройства, затем коснитесь «Удалить это устройство».

   *Примечание.* Если Вы участник группы Семейного доступа, Вы увидите список ее участников, предоставивших Вам доступ к геопозициям своих устройств, вместе с именем владельца группы.

7. Когда Вы делитесь фото и видео с метаданными о геопозиции, пользователи, с которыми Вы поделились, могут просмотреть эти метаданные и узнать место съемки. Если Вы не хотите делиться метаданными о геопозиции своих фото и видео, Вы можете удалить имеющиеся метаданные и запретить их сбор в дальнейшем.

## Контрольный список 3. Управление контентом

В этом контрольном списке указано, как закрыть ранее предоставленный доступ на iPhone с iOS 15 или более ранней версии. Если Вы пользуетесь iPhone с iOS 16 или новее, обратитесь к разделу Проверка безопасности на iPhone с iOS 16 или новее ранее в этом руководстве.


1. Проверьте, состоите ли Вы в группе Семейного доступа. Для этого выберите «Настройки» > [*Ваше имя*] и найдите вкладку «Семейный доступ». Если Вы в группе Семейного доступа, отобразятся имена участников этой группы.
2. Если Вы участник группы Семейного доступа и больше не хотите делиться информацией, Вы можете выйти из группы (при условии, что Вам уже исполнилось 13 лет). Если Вы организатор группы Семейного доступа (под Вашим именем отображается слово *организатор*), Вы можете удалить из этой группы любых участников старше 13 лет.
3. В приложении «Локатор» выберите вкладку «Люди», чтобы просмотреть, с кем Вы делитесь своей геопозицией. Чтобы закрыть доступ определенному человеку, выберите его, затем выберите «Не делиться геопозицией». Чтобы закрыть доступ для всех, выберите «Я» и выключите параметр «Делиться геопозицией».
4. В приложении «Фото» коснитесь вкладки «Альбомы», затем перейдите в раздел «Общие альбомы». Выберите общий альбом и коснитесь «Люди», чтобы узнать, кто владелец общего альбома и кто имеет к нему доступ.
   - Если Вы владелец альбома и хотите закрыть доступ кому-либо из подписчиков, коснитесь имени этого подписчика и выберите соответствующий параметр.
   - Если Вы подписчик, коснитесь кнопки «Отписаться» внизу экрана. Вы также можете удалить любые фото, которыми поделились.

5. В приложении «Календарь» коснитесь вкладки «Календари». Выберите общий календарь и коснитесь, чтобы узнать, кто имеет к нему доступ.
   - Если альбомом владеете Вы и хотите закрыть доступ для кого-то из подписчиков, коснитесь его имени и выберите этот параметр.
   - Если Вы подписчик, коснитесь «Удалить календарь» внизу экрана.
6. Если у Вас есть часы Apple Watch и Вы делитесь с кем-то своим прогрессом заполнения колец Активности, Вы можете закрыть доступ. На iPhone откройте приложение «Активность», затем коснитесь «Поделиться». Коснитесь того, с кем Вы делитесь, коснитесь имени этого человека, затем выберите «Удалить друга» или «Скрыть мою активность».
7. Вы также можете делиться информацией с другими людьми в сторонних приложениях. Просмотрите приложения, установленные на устройстве, и проверьте, делятся ли они данными. См. раздел Управление настройками общего доступа к данным Фото

# Ограничение доступа к устройству и учетной записи

## Доступ к Аккаунту Apple

### Поддержание безопасности Аккаунта Apple

Аккаунт Apple — это личная учетная запись, с помощью которой можно выполнять вход на устройствах и получать доступ к таким сервисам Apple, как App Store, iCloud, Сообщения, FaceTime и Локатор. В этой учетной записи также есть личная информация, которую Вы храните с помощью Apple и которая передается между устройствами. К такой информации относятся данные контактов, платежная информация, фото, резервные копии устройств и многое другое. Человек, получивший доступ к Вашему Аккаунту Apple, может просматривать информацию, синхронизируемую между устройствами и в том числе к сообщениям и геопозициям. Здесь Вы узнаете, как защитить Аккаунт Apple на iPad, iPhone и Mac.


Далее перечислены важные правила, которые помогут Вам защитить свой Аккаунт Apple и конфиденциальность.

### Защита Вашего Аккаунта Apple

1. Не делитесь своим Аккаунтом Apple ни с кем, даже с членами семьи, партнерами и близкими друзьями. Поделившись Аккаунтом Apple, Вы даете другому человеку доступ к своим личным данным и своему контенту. Если другой человек настроил Ваш Аккаунт Apple и задал его пароль либо получил доступ к Вашему паролю, смените такой пароль.
2. Для доступа к своему Аккаунту Apple используйте двухфакторную аутентификацию. Благодаря двухфакторной аутентификации доступ к Вашей учетной записи можете получить только Вы, даже если Ваш пароль известен кому-то еще. С двухфакторной аутентификацией потребуется ввести пароль и шестизначный код проверки, который автоматически отобразится на доверенных устройствах при первом входе на новом устройстве.

   Чтобы включить двухфакторную аутентификацию, Вам необходимо иметь хотя бы один проверенный номер телефона. На этот номер будут приходить коды проверки в виде текстовых сообщений или автоматических телефонных вызовов.
3. Внимательно читайте уведомления о своем Аккаунте Apple. Apple уведомляет Вас в электронном письме, текстовом сообщении или push-уведомлении, если Ваша учетная запись была изменена. Например, Вы будете уведомлены о первом входе на новом устройстве или изменении пароля. Именно поэтому важно, чтобы Ваша контактная информация была актуальной.

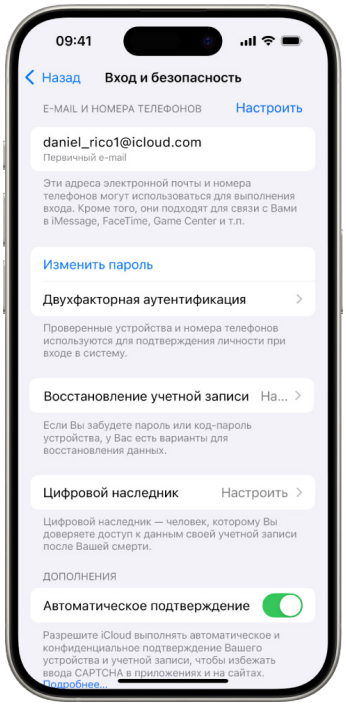
   См. раздел Блокировка чужих попыток входа ранее в этом руководстве.
4. Если Вы получили уведомление о попытке входа или изменении учетной записи, но Вы этих действий не совершали, это может означать, что кто-то получил или пытается получить доступ к Вашей учетной записи.

### Проверка и обновление информации о безопасности Аккаунта Apple

Следуйте инструкциям далее, чтобы убедиться в том, что личная информация, связанная с Вашим Аккаунтом Apple, принадлежит Вам.

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Откройте «Настройки» > [*Ваше имя*].
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки», затем нажмите «Аккаунт Apple».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки», затем нажмите «Аккаунт Apple».
   - *В веб-браузере на Mac или устройстве с Windows.* Перейдите на сайт Аккаунта Apple (https://appleid.apple.com).

2. Обновите информацию в полях имени, номеров телефонов и адресов электронной почты, если внесенные сведения неверны или если Вы не знаете, чьи они, затем введите свое имя, номера телефонов и адреса электронной почты, чтобы с Вами можно было связаться.




3. Выполните одно из описанных ниже действий.

   - Если двухфакторная аутентификация включена, просмотрите свои доверенные устройства. Если в списке есть устройства, которые нужно удалить из учетной записи, выполните инструкции в следующем разделе.
   - Если двухфакторная аутентификация не настроена, см. раздел Использование двухфакторной аутентификации далее в этом руководстве.

### Защита учетной записи и удаление неизвестных устройств

Если Вам незнакомы какие-либо устройства, подключенные к Вашему Аккаунту Apple, или Вы не разрешали использовать свой Аккаунт Apple, его можно защитить, удалив устройства по инструкции далее. После удаления неизвестного устройства на нем больше не будут отображаться коды проверки, а доступ к iCloud (а также к другим сервисам Apple на устройстве) будет заблокирован, пока Вы снова не выполните вход с использованием двухфакторной аутентификации.

Возможно, будет полезно создать снимок экрана, запечатлев все устройства, перед тем как принимать меры для защиты учетной записи.

Следуйте приведенным далее инструкциям, чтобы просмотреть информацию в своей учетной записи и защитить ее.

1. Изменение пароля.
   - *На iPhone или iPad.* Выберите «Настройки» > [*Ваше имя*] > «Вход и безопасность» > «Изменить пароль». Создайте надежный пароль (он должен содержать не менее восьми символов, включая строчные и прописные буквы и как минимум одну цифру).
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки», затем вверху бокового меню нажмите свое имя. Нажмите «Пароль и безопасность», затем нажмите «Сменить пароль».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки», затем нажмите *[Ваше имя]* > «Пароль и безопасность» > «Сменить пароль». Создайте надежный пароль (он должен содержать не менее восьми символов, включая строчные и прописные буквы и как минимум одну цифру).
2. Чтобы в качестве меры предосторожности изменить адрес электронной почты, связанный с Вашим Аккаунтом Apple, откройте Safari и войдите в свою учетную запись на сайте Аккаунта Apple (https://account.apple.com). Выберите «Учетная запись», под своим текущим Аккаунтом Apple выберите «Сменить Аккаунт Apple», затем введите новый адрес электронной почты, который хотите использовать.
3. Удаление устройств, которые подключены к учетной записи.
   - *На iPhone или iPad.* Откройте «Настройки» > [*Ваше имя*], прокрутите вниз до списка устройств, коснитесь устройства, которое нужно удалить, затем коснитесь «Удалить из учетной записи».
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки», затем нажмите [*Ваше имя*]. Прокрутите вниз до списка устройств, нажмите устройство, которое нужно удалить, затем нажмите «Удалить из учетной записи».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки», нажмите «Apple ID», прокрутите вниз до списка устройств, выберите устройство, которое нужно удалить, затем нажмите «Удалить из учетной записи».

## Использование двухфакторной аутентификации

Двухфакторная аутентификация — это дополнительный уровень защиты Вашего Аккаунта Apple. Благодаря двухфакторной аутентификации доступ к Вашей учетной записи можете получить только Вы, даже если Ваш пароль известен кому-то еще. Можно настроить двухфакторную аутентификацию на iPhone, iPad и Mac.


### Настройка двухфакторной аутентификации на iPhone или iPad

1. Выберите «Настройки» > *[Ваше имя]* > «Вход и безопасность».
2. Касанием включите двухфакторную аутентификацию, затем коснитесь «Продолжить».
3. Введите проверенный номер телефона. На этот номер будут приходить коды проверки для двухфакторной аутентификации (это может быть номер телефона Вашего iPhone).

   Вы можете выбрать способ получения этих кодов — в виде текстового сообщения или вызова.
4. Коснитесь «Далее».
5. Введите код проверки, отправленный на проверенный номер телефона.

   Чтобы отправить код проверки или получить новый код, коснитесь «Не получили код проверки?».

   Вам не придется снова вводить код проверки на своем iPhone, кроме случаев, указанных далее.

   - Полный выход из учетной записи
   - Стирание iPhone
   - Вход в Аккаунт Apple с веб-страницы Аккаунта Apple
   - Необходимость сменить пароль Аккаунта Apple в целях безопасности

После включения двухфакторной аутентификации у Вас будет две недели на то, чтобы выключить ее, если Вы передумаете. После этого выключить двухфакторную аутентификацию будет невозможно. Чтобы выключить двухфакторную аутентификацию, откройте электронное письмо с подтверждением и нажмите ссылку для возврата к предыдущим настройкам безопасности. Учтите, что без двухфакторной аутентификации Ваша учетная запись более уязвима. По этой причине Вы не сможете использовать функции, требующие более высокого уровня безопасности.

### Настройка двухфакторной аутентификации на компьютере Mac

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Выберите меню Apple  > «Системные настройки», нажмите [*Ваше имя*], затем в боковом меню выберите «Вход и безопасность».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки», нажмите «Apple ID» , затем выберите «Вход и безопасность».
2. Нажатием включите настройку двухфакторной аутентификации, затем нажмите «Продолжить».
3. Ответьте на проверочные вопросы, затем нажмите кнопку проверки.
4. Введите номер телефона для проверки, выберите способ проверки, затем нажмите «Продолжить».
5. Когда появится запрос, подтвердите свою личность, введя шестизначный код проверки, отправленный на Ваш проверенный номер телефона. Вам придется снова ввести код проверки на своем Mac, только если Вы полностью выйдете из своего Аккаунта Apple, сотрете все данные с Mac или смените пароль в целях безопасности.

### Ключи безопасности для Аккаунта Apple

Ключ безопасности — это небольшое внешнее устройство, которое выглядит как флеш-накопитель или тег и которое можно использовать для подтверждения входа с Вашим Аккаунтом Apple при использовании двухфакторной аутентификации. Ключи безопасности для Аккаунта Apple — это дополнительная функция безопасности. Она предназначена специально для пользователей, которым необходима более надежная защита от преступных действий в их адрес, в том числе от фишинга и мошенничества с использованием социальной инженерии. Использование физического ключа вместо шестизначного кода усиливает безопасность процесса двухфакторной аутентификации и помогает защитить второй фактор аутентификации от перехвата или запроса информации мошенниками.

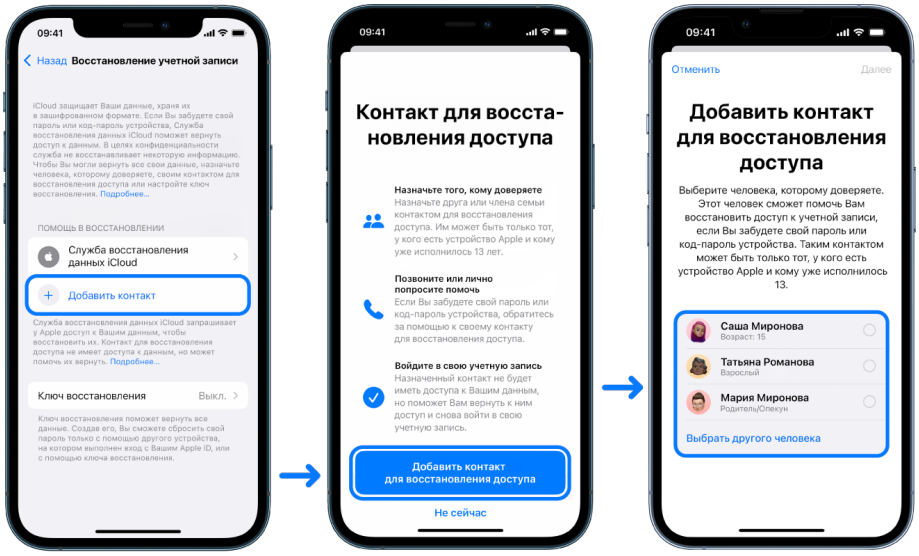
Подробнее о ключах безопасности см. в статье службы поддержки Apple Сведения о ключах безопасности для Аккаунта Apple (https://support.apple.com/HT213154).

## Как избежать потери доступа к Аккаунту Apple и устройству

Контакты для восстановления доступа — это те, кому Вы доверяете и кто сможет помочь Вам восстановить доступ к Вашей учетной записи, если Вы забудете пароль или код-пароль устройства или если кто-то изменит Ваш пароль или код-пароль без Вашего разрешения. Контакты для восстановления доступа не получают доступ к Вашей учетной записи. Они могут только отправить Вам код для восстановления доступа к учетной записи, если потребуется. Вы можете назначить контакт для восстановления доступа, который поможет Вам восстановить доступ к данным на Вашем iPhone, iPad или Mac.


*Примечание.* Помимо контакта для восстановления доступа, Вы можете назначить *цифрового наследника* — это самый простой и надежный способ передать доступ к данным Вашему Аккаунту Apple после Вашей смерти. См. статью службы поддержки Apple Как добавить цифрового наследника для Вашего Аккаунта Apple (https://support.apple.com/102631).

Чтобы стать контактом для восстановления доступа, необходимо быть старше 13 лет, иметь устройство с iOS 15, iPadOS 15 или macOS 12 или новее и использовать двухфакторную аутентификацию в своем Аккаунте Apple и код-пароль на своем устройстве.




### Назначение контакта для восстановления доступа к учетной записи

Если Вы беспокоитесь, что кто-то может получить доступ к Вашей учетной записи с целью изменить Ваш пароль и заблокировать для Вас доступ, Вы можете назначить контакт для восстановления доступа, который поможет Вам восстановить доступ.

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Выберите «Настройки» > [*Ваше имя*], затем коснитесь «Вход и безопасность».
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки», нажмите «Аккаунт Apple», затем в боковом меню выберите «Вход и безопасность».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки», нажмите «Аккаунт Apple», затем выберите «Вход и безопасность».
2. Выберите «Восстановление учетной записи», добавьте контакт для восстановления доступа, затем выполните аутентификацию с помощью Face ID, Touch ID, код-пароля или пароля.
3. Если Вы в группе Семейного доступа, в рекомендациях отобразятся имена участников этой группы. Или Вы можете выбрать одного из своих контактов.
4. Если выбрать члена семьи, этот человек будет добавлен автоматически. Если выбрать контакт, то ему сначала потребуется принять запрос.
5. Если Ваш запрос будет принят, Вы увидите сообщение о том, что теперь этот человек является Вашим контактом для восстановления доступа.

### Просмотр и удаление контакта для восстановления доступа

Вы можете просмотреть или удалить контакт для восстановления доступа.

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad*. Выберите «Настройки» > [*Ваше имя*], затем коснитесь «Вход и безопасность».
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки», нажмите «Аккаунт Apple», затем в боковом меню выберите «Вход и безопасность».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки», нажмите «Аккаунт Apple», затем выберите «Вход и безопасность».
2. В разделе «Помощь в восстановлении» отображается список Ваших контактов для восстановления.
3. Выберите контакт для восстановления доступа, который нужно удалить, затем удалите этот контакт.

# Доступ к устройству

## Управление отпечатками пальцев для Touch ID

Используйте Touch ID, чтобы безопасно и удобно разблокировать iPhone, iPad или Mac, разрешать покупки и платежи и входить во многие сторонние приложения, нажимая пальцем кнопку «Домой».

Для использования Touch ID сначала нужно задать код-пароль на iPhone, iPad или Mac.

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.


### Защита устройств с помощью Touch ID

Для использования Touch ID сначала нужно задать код-пароль на iPhone или iPad.

#### Настройка Touch ID на iPhone или iPad

1. Если Вы не включили распознавание отпечатка пальца при первой настройке iPhone или iPad, откройте «Настройки» > «Touch ID и код-пароль».
2. Включите нужные параметры, затем следуйте инструкциям на экране.

   Если Вы не можете вспомнить некоторые из зарегистрированных отпечатков, обратитесь к разделу Управление отпечатками пальцев для Touch ID далее в этом руководстве.

*Примечание.* Если Вам не удается добавить отпечаток пальца или разблокировать iPhone или iPad с помощью Touch ID, см. статью службы поддержки Apple Если Touch ID не работает на iPhone или iPad (https://support.apple.com/101612).

### Настройка Touch ID на Mac или клавиатуре Magic Keyboard

Для использования Touch ID сначала нужно задать пароль на компьютере Mac.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Выберите меню Apple  > «Системные настройки», затем нажмите «Touch ID» .
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки», затем нажмите «Touch ID» .
2. Нажмите «Добавить отпечаток», введите пароль, затем следуйте инструкциям на экране.

   Если на компьютере Mac или клавиатуре Magic Keyboard есть сенсор Touch ID, то он расположен вверху справа на клавиатуре. В учетную запись можно добавить до трех отпечатков пальцев (и сохранить на компьютере Mac до пяти отпечатков пальцев).
3. Поставьте флажки, чтобы выбрать те функции Touch ID, которые Вы хотите использовать.
   - *Разблокировка компьютера Mac*. Используйте Touch ID, чтобы разблокировать компьютер Mac при выходе из режима сна.
   - *Apple Pay*. Используйте Touch ID, чтобы подтверждать покупки, совершаемые на компьютере Mac с использованием Apple Pay.
   - *iTunes Store, App Store и Apple Books*. Используйте Touch ID, чтобы подтверждать покупки, совершаемые на компьютере Mac в интернет-магазинах Apple.
   - *Автозаполнение пароля*. Используйте Touch ID, чтобы автоматически заполнять имена пользователей и пароли, а также данные кредитных карт при их запросе в Safari и других приложениях.
   - Использовать сенсор Touch ID для быстрого переключения пользователей. Используйте Touch ID, чтобы переключаться между учетными записями пользователя на компьютере Mac.

### Удаление неизвестных отпечатков, зарегистрированных для Touch ID на iPhone или iPad

Если на Вашем iPhone или iPad зарегистрировано несколько отпечатков для Touch ID, Вы можете удалить их, чтобы доступ к устройству остался только у Вас.

1. Откройте «Настройки»  > «Touch ID и код-пароль».
2. Если на устройство добавлено несколько отпечатков без подписей, поместите палец на кнопку «Домой», чтобы определить, какой из отпечатков Ваш. Подпишите свой отпечаток, чтобы узнавать его впоследствии.
3. При необходимости коснитесь отпечатка, затем коснитесь «Удалить отпечаток».

   *Примечание*. Если не удается добавить отпечаток пальца или разблокировать iPhone или iPad с помощью Touch ID, см. статью службы поддержки Apple Если Touch ID не работает на iPhone или iPad.

**Удаление неизвестных отпечатков, зарегистрированных для Touch ID на Mac или клавиатуре Magic Keyboard.**

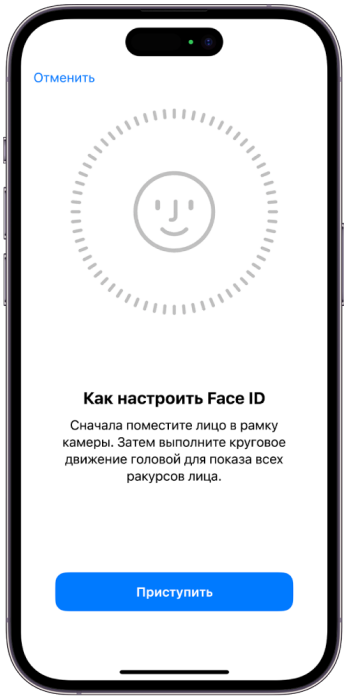
Если на Вашем Mac или клавиатуре Magic Keyboard зарегистрировано несколько отпечатков для Touch ID, Вы можете удалить их, чтобы доступ к устройству остался только у Вас.

1. Откройте настройки Touch ID.
   - На Mac с macOS 13 или новее. Выберите меню Apple  > «Системные настройки», затем нажмите «Touch ID и пароль» .
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки», затем нажмите «Touch ID» .
2. Выполните одно из перечисленных ниже действий.
   - *Удаление отпечатка.* Выберите отпечаток, введите пароль, нажмите «OK», затем нажмите «Удалить».
   - *Добавление отпечатка.* Нажмите «Добавить отпечаток», чтобы добавить новый отпечаток, затем выберите функции, которые хотите использовать с Touch ID.

## Защита iPhone или iPad с помощью Face ID

Face ID создан для тех, кто хочет обеспечить дополнительный уровень защиты своего iPhone или iPad. Эта функция помогает гарантировать, что никто другой не сможет получить доступ к информации, хранящейся на Вашем устройстве. Для использования Face ID сначала нужно задать код-пароль на iPhone или iPad.

Список поддерживаемых устройств см. в статье службы поддержки Apple Модели iPhone и iPad с поддержкой Face ID (https://support.apple.com/102854).

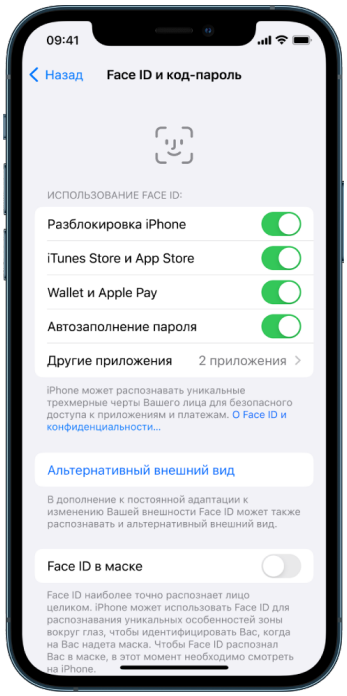


### Защита iPhone или iPad с помощью Face ID

- Если Вы не настроили Face ID при первой настройке iPhone или iPad, откройте «Настройки» > «Face ID и код-пароль» > «Настройка Face ID», затем следуйте инструкциям на экране.

Если у Вас есть особые физические потребности, во время настройки Face ID Вы можете коснуться «Параметры Универсального доступа». После этого при настройке распознавания лица не придется выполнять полный диапазон движений головой. Пользоваться Face ID будет по-прежнему безопасно, но потребуется определенным образом смотреть на iPhone или iPad.

В Face ID также есть поддержка функции Универсального доступа для слабовидящих и слепых. Чтобы функция Face ID не требовала взгляда на экран iPhone или iPad с открытыми глазами, выберите «Настройки» > «Универсальный доступ», затем выключите функцию «Требование внимания для Face ID». Эта функция выключается автоматически, если при первой настройке iPhone или iPad была включена функция VoiceOver.




См. раздел Изменение настроек Face ID и функции распознавания внимания на iPhone (https://support.apple.com/guide/iphone/iph646624222) в Руководстве пользователя iPhone или Изменение настроек Face ID и функции распознавания внимания на iPad в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipad058b4a31).

### Сброс Face ID для удаления альтернативных вариантов внешности

Если Вы больше не хотите использовать альтернативный вариант внешности для Face ID или считаете, что кто-то мог добавить такой вариант на Вашем устройстве без Вашего разрешения, Вы можете сбросить Face ID, а затем настроить эту функцию снова.

1. Откройте «Настройки» > «Face ID и код-пароль», затем коснитесь «Сбросить Face ID».
2. Обратитесь к инструкции выше, чтобы настроить Face ID снова.

## Блокировка чужих попыток входа

Если у Вас включена двухфакторная аутентификация, то при попытке входа на новом устройстве Вы получаете уведомление на других доверенных устройствах. Это уведомление включает карту с геопозицией нового устройства. Уведомление может отобразиться на любом доверенном iPhone, iPad или Mac.

Геопозиция новой попытки входа определяется приблизительно — на основе IP-адреса или сети, которые в данный момент использует устройство. Это не точная геопозиция устройства.


Если Вы получили уведомление о том, что Ваш Аккаунт Apple сейчас используется для входа на новом устройстве, которое Вам неизвестно, выберите «Не разрешать», чтобы заблокировать попытку входа.

**ВАЖНО!** Прежде чем закрывать уведомление, Вы можете сделать снимок экрана с ним. См. раздел Запись подозрительной активности далее в этом руководстве.


Если Вы считаете, что Ваш Аккаунт Apple мог быть скомпрометирован, обратитесь к разделу Поддержание безопасности Аккаунта Apple (далее в этом руководстве) и удалите неизвестные устройства.

# Обновление программного обеспечения Apple

Для защиты устройства и контроля доступа к личной информации на устройстве должна быть установлена новейшая операционная система со всеми актуальными обновлениями системы безопасности и конфиденциальности. Если Ваши устройства обновлены, изучите, как управлять Аккаунтом Apple. Обновления программного обеспечения идут на пользу всем устройствам Apple.


Обновление программного обеспечения операционной системы — один из важнейших аспектов защиты устройства и данных на нем. Благодаря Apple Вы можете с легкостью загружать и устанавливать эти обновления.

Список обновлений системы безопасности устройств Apple см. в статье службы поддержки Apple Обновления системы безопасности Apple (https://support.apple.com/HT201222#update).

### Автоматическое обновление iPhone и iPad

Если Вы не включили автоматическое обновление при первоначальной настройке устройства, Вы можете сделать это сейчас.

1. Откройте «Настройки» > «Основные» > «Обновление ПО» > «Автообновление».
2. Включите все три указанных параметра: «Автоматически устанавливать обновления [*iOS или iPadOS*], «Ответы на угрозы и системные файлы» и «Автоматически загружать обновления [*iOS или iPadOS*]».

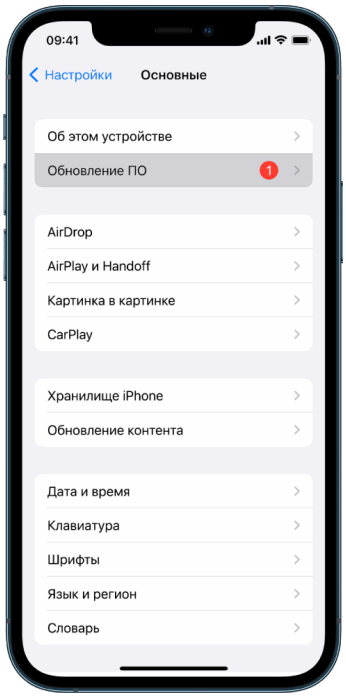
Как только обновление станет доступно, устройство загрузит и установит обновление ночью при наличии подключения к источнику питания и сети Wi-Fi. Перед установкой обновления Вы получите уведомление.

Чтобы выключить автообновление, откройте «Настройки» > «Основные» > «Обновление ПО» > «Автообновление», затем выключите параметры «Автоматически устанавливать обновления [*iOS или iPadOS*]» и «Ответы на угрозы и системные файлы».

### Обновление iPhone или iPad вручную

Вы можете в любой момент проверить наличие обновлений ПО и установить их.

- Откройте «Настройки» > «Основные» > «Обновление ПО».




На экране отобразится текущая установленная версия iOS, а Вы будете уведомлены, если выйдет обновление.

### Обновление iPhone или iPad с помощью компьютера

1. Вам понадобится что-то одно из списка ниже.
   - Компьютер Mac с разъемом USB и OS X 10.9 или новее.
   - Устройство с Windows, оснащенное разъемом USB, с Windows 7 или новее.
2. Выполните одно из описанных ниже действий.
   - Подключите устройство к компьютеру с помощью прилагаемого кабеля Lightning — USB. Если Ваш компьютер оснащен разъемом USB-C, используйте адаптер USB-C — USB или кабель USB-C — Lightning (адаптер и кабель продаются отдельно).
   - Если к устройству прилагается кабель USB-C — Lightning, а компьютер оснащен разъемом USB, используйте кабель Lightning — USB (продается отдельно).
   - Если к iPad прилагается зарядный кабель USB-C, а компьютер оснащен разъемом USB, используйте адаптер USB-C — USB и кабель USB-A (адаптер и кабель продаются отдельно).
   - Если к iPad прилагается зарядный кабель Thunderbolt 4 — USB-4, а компьютер оснащен разъемом USB, используйте адаптер USB-C — USB и кабель USB-A (адаптер и кабель продаются отдельно). Кроме того, можно использовать кабели Thunderbolt или USB с устройствами с разъемом Thunderbolt, такими как 12,9-дюймовый iPad Pro (5-го поколения) и 11-дюймовый iPad Pro (3-го поколения).

3. Подключив устройство к компьютеру, выполните одно из описанных ниже действий.
   - *В боковом меню Finder на Mac.* Выберите устройство, затем нажмите «Основные» вверху окна.

     Чтобы использовать Finder для обновления устройства до iOS 15 или iPadOS 15, требуется macOS 10.15 или новее. Если у Вас более ранняя версия macOS, используйте iTunes, чтобы обновить устройство. См. раздел «Обновление ПО устройств iOS в iTunes» (https://support.apple.com/guide/itunes/itns3235/12.9/mac/10.14).
   - *В приложении iTunes на устройстве с Windows.* Нажмите кнопку iPhone в левом верхнем углу окна iTunes, затем нажмите «Обзор».
4. Нажмите «Проверить наличие обновлений».
5. Чтобы установить доступное обновление, нажмите «Обновить».

**Автоматическое обновление компьютера Mac**

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Выберите меню Apple  > «Системные настройки», нажмите «Основные» , затем нажмите «Обновление ПО».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки», затем нажмите «Обновление ПО» .
2. Чтобы обновления macOS устанавливались автоматически, установите флажок «Автоматически устанавливать обновления ПО Mac».
3. Чтобы задать дополнительные параметры обновления, нажмите «Дополнительно», затем выполните любое из указанных действий.
   - *Чтобы Mac автоматически проверял наличие обновлений,* установите флажок «Проверять наличие обновлений».
   - *Чтобы Mac загружал обновления, не спрашивая об этом,* установите флажок «Загружать обновления, если они доступны».
   - *Чтобы Mac автоматически устанавливал обновления macOS,* установите флажок «Устанавливать обновления macOS».
   - *Чтобы Mac автоматически устанавливал обновления из App Store,* установите флажок «Устанавливать обновления приложений из App Store».
   - *Чтобы Mac автоматически устанавливал системные файлы и обновления системы безопасности,* Выберите «Устанавливать ответы на угрозы и системные файлы».
4. Нажмите «OK».

Чтобы получать новейшие обновления автоматически, рекомендуется установить флажки «Проверять наличие обновлений», «Загружать обновления, если они доступны» и «Устанавливать системные файлы и обновления системы безопасности».

*Примечание.* MacBook, MacBook Pro и MacBook Air должны быть подключены к источнику питания с помощью адаптера, чтобы обновления загружались автоматически.

### Обновление компьютера Mac вручную

Операционную систему Mac и любое программное обеспечение из App Store можно обновлять вручную.

- Выполните одно из описанных ниже действий.
  - На Mac с macOS 13 или новее. Выберите меню Apple  > «Системные настройки», нажмите «Основные» , затем нажмите «Обновление ПО».
  - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки», затем нажмите «Обновление ПО» .
- Чтобы обновить программное обеспечение, загруженное из App Store, нажмите меню Apple. Количество обновлений, если они доступны, отобразится рядом в App Store. Выберите App Store, чтобы продолжить работу в приложении App Store .

## Просмотр и удаление профилей конфигурации

Организации (такие как учебные заведения и компании) могут использовать профили конфигурации устройств, инструменты управления мобильными устройствами (MDM) и собственные приложения, чтобы управлять устройствами, контролировать их и получать с помощью этих средств доступ к данным или информации о геопозиции на устройстве.

Профиль конфигурации может управлять различными настройками учетных записей пользователей, а также другими функциями устройства. Профили конфигурации могут работать на iPhone, iPad, Mac, Apple TV и Apple Watch.

Если на Вашем устройстве установлен профиль конфигурации, но его быть не должно, Вы можете удалить этот профиль. Однако возможность удаления зависит от того, кто установил профиль. В случае удаления удаляются все настройки, приложения и данные, связанные с профилем конфигурации.

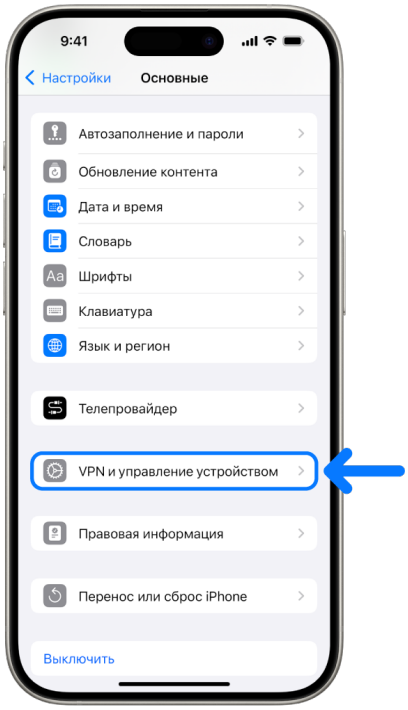
**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.


### Просмотр профилей конфигурации

**Важно!** Если устройство принадлежит учебному заведению или компании, обратитесь к системному администратору перед тем, как удалять приложения или профили.

### Удаление неизвестных профилей конфигурации с iPhone или iPad

При удалении профиля также удаляются все его настройки и связанная с ним информация. Например, если в профиле предоставлялось разрешение подключаться к частной школьной сети через протокол VPN (виртуальных частных сетей), то после удаления профиля подключение к такой сети через VPN станет недоступно.




1. Откройте «Настройки» > «Основные» > «VPN и управление устройством».

   Если профилей нет, значит, на Вашем устройстве не установлены профили управления устройством.

2. Выберите профиль, коснитесь «Удалить профиль» и следуйте инструкциям на экране.

3. Перезагрузите устройство.

### Удаление неизвестных профилей конфигурации с компьютера Mac

При удалении профиля также удаляются все его настройки и связанная с ним информация. Например, если с помощью профиля была настроена учетная запись электронной почты, то после удаления профиля с Вашего компьютера Mac удалятся данные учетной записи электронной почты.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Выберите меню Apple  > «Системные настройки» > «Конфиденциальность и безопасность», затем нажмите «Профили» .
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки», затем нажмите «Профили» .

   Если панели настроек «Профили» нет, значит, на Вашем устройстве не установлены профили управления устройством.
2. Выберите профиль в списке «Профили», затем нажмите —.
3. Перезагрузите Mac.

## Защита устройств с помощью режима блокировки

Режим блокировки — это необязательное средство экстренной защиты для iPhone, iPad и Mac с iOS 16, iPadOS 16.1 и macOS 13 или новее. Используйте его, только если считаете, что Вы могли подвергнуться высокотехнологичной кибератаке, например с помощью узконацеленного шпионского ПО, разработанного по заказу государства.

*Примечание.* Большинство людей никогда не становятся целью таких атак.


Работа устройства в режиме блокировки отличается от его работы в обычном режиме. Работа приложений, веб-сайтов и функций строго ограничена в целях безопасности, а некоторые возможности полностью недоступны. Режим блокировки включает перечисленные ниже средства защиты.

- *Сообщения.* Блокируется большинство типов вложений в сообщениях, кроме изображений. Некоторые функции, такие как предварительный просмотр ссылок, недоступны.
- *Просмотр веб-страниц.* Некоторые сложные веб-технологии, такие как динамическая компиляция JavaScript, не работают, если только пользователь не исключил доверенный сайт из режима блокировки.
- *Сервисы Apple.* Входящие приглашения и запросы от сервисов, включая вызовы FaceTime, блокируются, если пользователь ранее не отправлял отправителю вызов или запрос.
- *Подключения через провод.* Для подключения устройства к компьютеру или аксессуару необходимо разблокировать устройство.
- *Профили конфигурации.* В режиме блокировки профили конфигурации не могут быть установлены, а устройство не может быть зарегистрировано в системе управления мобильными устройствами (MDM). Однако профили MDM, включенные до запуска режима блокировки, останутся на устройстве.

### Включение и выключение режима блокировки

Режим блокировки должен быть отдельно включен на iPhone, iPad и Mac. При включении режима блокировки на iPhone этот режим также активируется на объединенных с ним в пару Apple Watch с watchOS 10 или новее. Включить или выключить режим блокировки непосредственно на Apple Watch невозможно.

- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Откройте «Настройки» > «Конфиденциальность и безопасность» > «Режим блокировки», коснитесь «Включить режим блокировки», коснитесь «Включить и перезагрузить», затем введите код-пароль устройства.
  - *На Mac.* Выберите меню Apple > «Системные настройки» > «Конфиденциальность и безопасность», затем выберите «Режим блокировки». Коснитесь «Включить», затем введите пароль (если появится запрос) и коснитесь «Включить и перезагрузить».

## Безопасное управление аксессуарами в приложении «Дом»

Если Вы добавлены как житель в приложении «Дом», Вы можете легко и безопасно управлять аксессуарами в своем доме через приложение «Дом» на iPhone, iPad, или Mac либо через HomePod.

*Примечание.* Аксессуарами в приложении «Дом» могут быть устройства Apple или сторонних производителей. Список аксессуаров, совместимых с приложением «Дом» и устройствами Apple, приведен на веб-странице Аксессуары для умного дома (https://www.apple.com/home-app/accessories/).

### Закрытие доступа к дому для определенного человека

1. Выберите приложение «Дом», затем выберите «Настройки дома». Если отображаются несколько домов, выберите тот, из которого нужно выйти, затем выберите «Настройки дома».
2. В разделе «Люди» выберите пользователя, которого хотите удалить из дома, затем выберите «Удалить человека».

### Выход из группы жителей дома, в который Вы были приглашены

Если Вы покинете дом, то не сможете просматривать аксессуары в нем.

1. В приложении «Дом» выберите значок приложения «Дом», затем выберите «Настройки дома». Если отображаются несколько домов, выберите тот, из которого нужно выйти, затем выберите «Настройки дома».
2. Прокрутите вниз и выберите «Покинуть дом». Выберите «Покинуть».

### Сброс настроек дома

В iOS 16, iPadOS 16.1 и macOS 13 или новее при удалении дома из приложения «Дом» все устройства HomeKit необходимо добавить в новый дом. Перед удалением дома убедитесь, что на всех аксессуарах в доме установлены новейшие версии программного обеспечения.

Если операционные системы еще не обновлены, выполните шаг 4 ниже.

1. В приложении «Дом» выберите значок приложения «Дом», затем выберите «Настройки дома».
2. Внизу диалогового окна выберите «Удалить дом», затем выберите «Удалить».
3. Выберите приложение «Дом».
4. Найдите все аксессуары в доме, затем восстановите заводские настройки на каждом из них.
5. Снова откройте приложение «Дом» и создайте новый дом.
6. Добавьте аксессуары в новый дом.

# Пароли, ключи входа, код-пароли

## Обеспечение надежности паролей Вашего устройства, приложений и сайтов

На iPhone или iPad с iOS 17 либо iPadOS 17 или более ранней версии для управления паролями можно использовать Настройки, поиск Spotlight или Siri. Также можно использовать функцию «Рекомендации по безопасности паролей» для выявления слабых или уязвимых паролей. Сохраненные пароли отображаются в алфавитном порядке и упорядочены по сайту или платформе, на которых они сохранены.

На iPhone или iPad с iOS 18 либо iPadOS 18 или новее можно управлять паролями в приложении «Пароли», где собраны все Ваши пароли, ключи входа и коды проверки. Их также можно использовать на всех Ваших устройствах, на которых выполнен вход в iCloud с одним и тем же Аккаунтом Apple, а в настройках iCloud выбран параметр «Пароли и связка ключей». Если Вы используете Автозаполнение для входа в приложения и на сайты, пароли автоматически отобразятся в разделе «Пароли».


**Управление паролями в iOS 18, iPadOS 18 или новее**

1. На iPhone откройте приложение «Пароли».
2. Коснитесь «Все», затем коснитесь учетной записи, которой хотите управлять.
3. Коснитесь «Правка».
4. Смените или удалите пароль, затем коснитесь для подтверждения.

### Управление паролями в iOS 17, iPadOS 17 или более ранней версии

Для управления паролями можно использовать Настройки, поиск Spotlight или Siri.

1. Откройте «Настройки» > «Пароли», затем выполните одно из описанных ниже действий.
   - Чтобы добавить новый пароль вручную, коснитесь «Добавить» в правом верхнем углу.
   - Чтобы отредактировать или удалить пароль, коснитесь «Изменить» в правом верхнем углу, коснитесь «Выбрать сохраненные пароли», затем коснитесь «Изменить» или «Удалить».

     **Важно!** Удаленный пароль нельзя восстановить.
2. Если Вы добавили новый пароль, проверьте его, чтобы убедиться в правильности ввода.

### Использовании функции «Рекомендации по безопасности паролей» в iOS 17, iPadOS 17 или более ранней версии

Если Вы придумываете и сохраняете собственные пароли для сайтов и приложений, функция «Рекомендации по безопасности паролей» поможет выявлять слабые или уязвимые пароли (например, которые легко угадать или которые используются несколько раз). Также эта функция может безопасным образом следить за Вашими паролями и предупреждать Вас, если какие-либо из них были скомпрометированы в результате известной утечки данных.

1. Откройте «Настройки» > «Пароли» > «Рекомендации по безопасности».
2. Включите параметр «Выявление украденных паролей», чтобы iPhone безопасным образом следил за Вашими паролями и предупреждал Вас, если какие-либо из них были обнаружены в известных утечках данных.
3. Просмотрите рекомендации по созданным Вами паролям.
   - Пароли, помеченные как *используемые повторно*, используются в разных доменах. Использование одного и того же пароля в нескольких службах может сделать Вашу учетную запись уязвимой для злоумышленника, завладевшего Вашими учетными данными.
   - Пароли, помеченные как *слабые*, могут быть легко угаданы злоумышленником.
   - Пароли помечаются как *украденные*, если функция «Мониторинг паролей» обнаружила их в известной утечке данных.
4. Чтобы изменить используемый повторно, слабый или украденный пароль, коснитесь объекта и следуйте инструкциям на экране.

### Автоматические удаление одноразовых кодов проверки

В iOS 17, iPadOS 17 и macOS 14 или новее одноразовые коды проверки заполняются автоматически, поэтому Вам не нужно покидать приложение или сайт, где Вы выполняете вход. Вы можете выбрать, нужно ли автоматически удалять коды проверки после их ввода с помощью автозаполнения или сохранять их.

- Выполните одно из описанных ниже действий.
  - На iPhone или iPad с iOS 18 либо iPadOS 18 или новее. Выберите «Настройки» > «Основные» > «Автозаполнение и пароли». В разделе «Коды проверки» коснитесь «Удаление после использования», затем включите этот параметр.
  - На iPhone или iPad с iOS 17 либо iPadOS 17 или более ранней версии. Откройте «Настройки» > «Пароли», выберите «Параметры паролей» и включите параметр «Автоматическая очистка».
  - На Mac с macOS 15. Выберите меню Apple > «Системные настройки», нажмите «Основные» , затем нажмите «Автозаполнение и пароли». В разделе «Коды проверки» нажмите «Удаление после использования», затем включите этот параметр.
  - На Mac с macOS 14 или macOS 13. Выберите меню Apple > «Системные настройки», в боковом меню выберите «Пароли», выберите «Параметры паролей» и включите параметр «Автоматическая очистка».

## Установка уникального код-пароля или пароля устройства

Чтобы никто, кроме Вас, не мог использовать Ваши устройства и получать доступ к Вашей информации, установите уникальный код-пароль или пароль, известный только Вам. Если Вы используете устройство совместно с другими пользователями или другие люди знают Ваш код-пароль или пароль, они могут просматривать и изменять информацию на Вашем устройстве и в связанном с ним Аккаунте Apple. Если Вы считаете, что кому-то известен код-пароль или пароль Вашего устройства, и Вы хотите задать новый код-пароль или пароль, известный только Вам, то его можно сбросить в Настройках или Системных настройках в зависимости от типа устройства (см. инструкции далее).


### Установка код-пароля на iPhone или iPad

Для повышения безопасности установите код-пароль, который потребуется вводить для разблокировки iPhone или iPad при его включении или выводе из режима сна. При установке код-пароля также включается функция защиты данных, которая шифрует данные на iPhone или iPad, чтобы они были доступны только тем, кому известен код-пароль.

*Примечание. Код-пароль* устройства не совпадает с *паролем* Аккаунта Apple, который дает доступ к iTunes Store, App Store, Apple Books, iCloud и другим сервисам Apple.

- Откройте «Настройки», затем выполните одно из описанных ниже действий.
  - На iPhone или iPad с Face ID. Коснитесь «Face ID и код-пароль», затем — «Включить код-пароль» или «Сменить код-пароль».
  - *На iPhone или iPad с кнопкой «Домой».* Коснитесь «Touch ID и код-пароль», затем — «Включить код-пароль» или «Сменить код-пароль».

  Чтобы просмотреть варианты создания пароля, коснитесь «Параметры код-пароля». По умолчанию код-пароли состоят из шести цифр, но в параметрах можно выбрать, например, наименее надежный — четырехзначный — пароль или самый надежный, то есть буквенно-цифровой.

### Смена код-пароля и аннулирование предыдущего код-пароля на iPhone или iPad

Если Вы предполагаете, что кто-то получил доступ к Вашему код-паролю, и хотите защитить свой iPhone, можно сменить код-пароль для защиты Ваших данных и аннулировать предыдущий код-пароль. Чтобы сменить код-пароль, выполните указанные ниже действия.

1. Откройте «Настройки», затем выполните одно из описанных ниже действий.
   - На iPhone или iPad с Face ID. Коснитесь «Face ID и код-пароль», затем введите свой код-пароль.
   - *На iPhone или iPad с кнопкой «Домой»*. Коснитесь «Touch ID и код-пароль», затем введите свой код-пароль.
2. Коснитесь «Сменить код-пароль» и введите свой текущий код-пароль.
3. Если Вы хотите повысить безопасность, коснитесь «Параметры код-пароля» и выберите формат будущего код-пароля.

   Доступны следующие форматы: числовой код из 4 цифр, числовой код из 6 цифр, произвольный код из цифр и букв либо произвольный код из цифр.
4. Дважды введите новый код-пароль.

   **ВАЖНО!** После смены код-пароля в iOS 17 или iPadOS 17 можно использовать старый код-пароль для сброса нового в течение 72 часов. Это может быть полезно, если Вы случайно забудете новый код-пароль. Если Вы хотите полностью деактивировать старый код-пароль после его смены на новый, коснитесь «Аннулировать старый код-пароль» в разделе Настроек «[Face ID][Touch ID] и код-пароль».

### Изменение пароля для входа на компьютере Mac

Если Вы предполагаете, что кто-то получил доступ к Вашему паролю, и хотите защитить свой Mac, можно сменить пароль пользователя для защиты Ваших данных.

*Примечание.* Пароль для входа — это пароль, который вводится для того, чтобы разблокировать компьютер Mac при его включении или выводе из режима сна. Поскольку этот пароль создан Вами, он может совпадать с паролем Вашего Аккаунта Apple, который дает доступ к iTunes Store, App Store, Apple Books, iCloud и другим сервисам Apple.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Пользователи и группы», затем нажмите ⓘ.
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Пользователи и группы», затем нажмите «Сменить пароль».
2. Нажмите «Сменить пароль».
3. Введите текущий пароль в поле «Старый пароль».
4. Введите новый пароль в поле «Новый пароль», затем введите его еще раз в поле «Подтверждение».

   Чтобы получить помощь в создании надежного пароля, рядом с полем «Новый пароль» нажмите .

5. Введите подсказку, чтобы было проще вспомнить пароль.

   Подсказка появится, если ввести неправильный пароль три раза подряд или если нажать знак вопроса у поля пароля в окне входа.

6. Нажмите «Сменить пароль».

### Автоматическая блокировка устройств

Для более надежной защиты данных Вы можете настроить устройство таким образом, чтобы оно автоматически блокировалось в определенных условиях.

- *На iPhone или iPad.* Выберите «Настройки» > «Экран и яркость» > «Автоблокировка», затем укажите временной интервал.
- *Mac.* Выберите меню Apple  > «Системные настройки», затем в боковом меню нажмите «Экран блокировки» (возможно, потребуется прокрутить вниз).

  Подробнее см. в разделе Изменение параметров настроек «Экран блокировки» на Mac в Руководстве пользователя Mac. (https://support.apple.com/guide/mac-help/mh11784)

- На Apple Watch. Откройте приложение «Настройки», коснитесь «Код-пароль», затем включите или выключите «Распознавание запястья».

  Подробнее см. в разделе Автоматическая блокировка в Руководстве пользователя Apple Watch. (https://support.apple.com/guide/watch/apd0e1e73b6f#apd6771615db)

## Управление общими паролями и ключами входа

В iOS 17, iPadOS 17 и macOS 14 или новее можно создать группу доверенных контактов или присоединиться к такой группе, чтобы совместно пользоваться паролями и ключами входа на определенных устройствах. В группах с общими паролями есть две различные роли пользователей: владелец группы и участник группы. Каждая из ролей определяет типы задач, доступных пользователю.

- *Владелец группы.* Владелец группы — это участник, создавший группу. Только владелец может добавлять и удалять других участников.
- *Участник группы.* Каждый пользователь, получивший и принявший приглашение от владельца, становится участником группы. Все участники группы могут добавлять, просматривать, изменять и удалять пароли в любое время. Участники могут покинуть группу в любое время.


*Примечание.* Если Вы удалили пароль или ключ входа, которым Вы делились с группой, Вы можете восстановить его в течение 30 дней. Если Вы удалили пароль или ключ входа, которым делился с группой другой пользователь, этот пользователь получает уведомление о возможности восстановить его в течение 30 дней. См. раздел Восстановление ранее удаленного пароля или ключа входа на Mac (https://support.apple.com/guide/mac-help/mchlee73013a) в Руководстве пользователя Mac.

### Как определить свою роль в группе с общими паролями

- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Откройте «Настройки» > «Пароли», найдите группу с общими паролями, выберите эту группу и посмотрите, являетесь ли Вы ее владельцем или участником.
  - На Mac с macOS 14 или более ранней версии. Выберите меню Apple > «Системные настройки», в боковом меню выберите «Пароли», найдите группу с общими паролями, выберите эту группу, нажмите «Управлять» и посмотрите, являетесь ли Вы *владельцем* или *участником* этой группы.

### Удаление участников из группы с общими паролями, владельцем которой Вы являетесь

Участник, которого Вы удалили из группы с общими паролями, сохраняет доступ к учетным записям и паролям, которыми Вы поделились, пока этот участник состоял в группе. После удаления участника Вам необходимо сменить пароли своих учетных записей, к которым Вы больше не хотите предоставлять доступ этому пользователю.

- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Откройте «Настройки» > «Пароли», найдите группу с общими паролями, выберите эту группу и удалите участника.
  - На Mac с macOS 14 или более ранней версии. Выберите меню Apple > «Системные настройки», в боковом меню выберите «Пароли», найдите группу с общими паролями, выберите эту группу, нажмите «Управлять» и удалите участника.

### Выход из группы с общими паролями, в которой Вы являетесь участником

Если Вы удалили себя из группы с общими паролями, состоящие в ней пользователи сохраняют доступ к учетным записям, паролям и ключам входа, которыми Вы поделились, пока Вы состояли в группе. После выхода из группы Вам необходимо сменить пароли и ключи входа для своих учетных записей, к которым Вы больше не хотите предоставлять доступ участникам группы.

- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Выберите «Настройки» > «Пароли», найдите группу с общими паролями, выберите эту группу и удалите себя из нее.
  - На Mac с macOS 14 или более ранней версии. Выберите меню Apple > «Системные настройки», в боковом меню выберите «Пароли», найдите группу с общими паролями, выберите эту группу, нажмите «Управлять» и удалите себя из группы.

### Удаление пароля или ключа входа из группы с общими паролями

Если Вы решили удалить пароли или ключи входа из группы с общими паролями, состоящие в ней пользователи сохраняют доступ к учетным записям, паролям и ключам входа, которыми Вы поделились с группой. После их удаления Вам необходимо сменить пароли и ключи входа для своих учетных записей, к которым Вы больше не хотите предоставлять доступ участникам группы.

*Примечание.* Если Вы удалили пароль или ключ входа, которым Вы делились с группой, Вы можете восстановить его в течение 30 дней. Если Вы удалили пароль или ключ входа, которым делился с группой другой пользователь, этот пользователь получает уведомление о возможности восстановить его в течение 30 дней. См. раздел Восстановление ранее удаленного пароля или ключа входа на Mac в Руководстве пользователя Mac (https://support.apple.com/guide/mac-help/mchlee73013a).

- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Откройте «Настройки» > «Пароли» в боковом меню, найдите группу с общими паролями, выберите эту группу и посмотрите, являетесь ли Вы ее владельцем или участником.
  - На Mac с macOS 14 или более ранней версии. Выберите меню Apple > «Системные настройки», в боковом меню нажмите «Пароли», нажмите рядом с учетной записью, для которой нужно удалить пароль или ключ входа, нажмите «Удалить пароль» или «Удалить ключ входа», затем снова нажмите «Удалить пароль» или «Удалить ключ входа».

# Управление данными о геопозиции

## Использование функции «На связи» для Сообщений

Можно использовать функцию «На связи» на iPhone, чтобы автоматически уведомлять друзей, когда iPhone прибывает в заданную геопозицию. Можно также выбрать, какую информацию получат друзья, если Вам не удастся успешно завершить поездку.

Точно так же, если Ваш друг воспользуется функцией «На связи», но его iPhone не прибудет в заданную геопозицию, как планировалось, Вы сможете просмотреть информацию о геопозиции друга, уровне заряда аккумулятора его устройства, наличии сотовой связи и многом другом.

*Примечание.* Для использования функции «На связи» необходимо, чтобы и у отправителя, и у получателя уведомлений была установлена операционная система iOS 17 или новее. Доступ к геопозиции не поддерживается в Южной Корее и может быть недоступен в других странах в связи с требованиями местного законодательства.

Когда Вы начинаете сеанс «На связи» *в поездке*, Ваш контакт получает следующую информацию:

- Ваше место назначения и приблизительное время прибытия;
- Ваши предполагаемые действия в тех случаях, если Вы не отвечаете на запросы, Вы воспользовались функцией «Экстренный вызов — SOS» во время сеанса «На связи» или Ваш телефон не прибыл в ожидаемое место назначения.

Когда Вы начинаете сеанс «На связи» *с таймером*, Ваш контакт получает следующую информацию:

- время, когда Вы запустили таймер;
- время окончания таймера;
- Ваши предполагаемые действия в тех случаях, если Вы не отвечаете на запросы в связи с таймером или Вы воспользовались функцией «Экстренный вызов — SOS» во время сеанса «На связи».

## Какая информация отправляется, и когда она отправляется?

При настройке сеанса «На связи» Вы можете выбрать, какая информация будет отправлена Вашему контакту в том случае, если сеанс «На связи» не завершится так, как ожидается. После настройки сеанса «На связи» Вы можете изменить тип отправляемых данных, открыв «Настройки» > «Сообщения» > «На связи» > «Данные».

Вы можете выбрать один из двух вариантов объема данных.

- *Ограниченный объем данных*. Включает Вашу текущую геопозицию и сведения об уровне заряда аккумулятора и уровне сетевого сигнала Вашего iPhone и Apple Watch.
- *Полный объем данных*. Включает все данные, входящие в ограниченный объем, а также проделанный Вами маршрут и геопозицию последней разблокировки Вашего iPhone и снятия Apple Watch.

Вашему контакту автоматически отправляется ссылка для просмотра выбранной Вами информации в любом из следующих случаев:

- Ваш телефон не прибыл в место назначения;
- Вы значительно задержались в дороге и не отвечаете на запрос о добавлении времени к поездке;
- Вы воспользовались функцией «Экстренный вызов — SOS» и не отвечаете на последующий запрос функции «На связи»;
- Вы не отвечаете на запрос в конце сеанса «На связи» с таймером.

**Важно!** Если Вы потеряете телефон во время сеанса «На связи», Ваш контакт будет получать уведомления так же, как если бы Вы не отвечали.

## Во время сеанса «На связи»

Во время сеанса «На связи» в поездке на заблокированном экране отображается следующее сообщение: «Разблокируйте для просмотра сведений». Если Вы коснетесь этого сообщения и разблокируете устройство, отобразится заданное Вами место назначения, ожидаемое в данный момент время прибытия (оно обновляется автоматически в зависимости от дорожной ситуации) и объем данных (ограниченный или полный), которые получит Ваш контакт, если сеанс «На связи» не будет успешно завершен. Вы также можете отменить сеанс «На связи».

### Запуск сеанса «На связи» с таймером

Если Вы не ощущаете себя в безопасности там, где Вы находитесь, и хотите получить поддержку от доверенного человека, Вы можете запустить сеанс «На связи» с таймером. Во время сеанса «На связи» с таймером Ваш доверенный контакт получит уведомление, если Вы не ответите на запрос по истечении срока таймера.

Во время сеанса «На связи» с таймером на заблокированном экране отображается следующее сообщение: «На связи: Разблокируйте для просмотра сведений». Если Вы коснетесь этого сообщения и разблокируете устройство, отобразится следующая информация:

- оставшееся время сеанса «На связи»;
- контакт, выбранный Вами для сеанса «На связи»;
- объем данных, которыми Вы делитесь с контактом
  - (ограниченный или полный).

Запуск сеанса «На связи» с таймером

1. Откройте приложение «Сообщения» и выберите человека, которого Вы хотите уведомлять.
2. Коснитесь «Новое сообщение» вверху экрана и добавьте получателя, либо выберите существующий разговор.
3. Коснитесь ＋, коснитесь «На связи», затем коснитесь «Изменить».

   Для отображения пункта «На связи» Вам может потребоваться коснуться «Еще».
4. Выберите «После таймера».
5. Выберите время до срабатывания таймера.

Когда сеанс «На связи» с таймером завершится, Вам будет предложено коснуться одного из двух вариантов: «Завершить сеанс „На связи“» или «Продлить». При успешном завершении сеанса «На связи» Ваш контакт получит уведомление об этом. Вы также можете выбрать вариант «Продлить», добавив 15, 30 или 60 минут к текущему сеансу «На связи». Ваш контакт получит уведомление о новом времени сеанса.

### Запуск сеанса «На связи» в поездке

Перемещаясь на автомобиле, общественным транспортом или пешком, Вы можете запустить сеанс «На связи», чтобы уведомить своего друга об успешном прибытии в место назначения.

Во время сеанса «На связи» в поездке на заблокированном экране отображается следующее сообщение: «Разблокируйте для просмотра сведений». Если Вы коснетесь этого сообщения и разблокируете устройство, отобразится заданное Вами место назначения, ожидаемое в данный момент время прибытия (оно обновляется автоматически в зависимости от дорожной ситуации) и объем данных, которые получит Ваш контакт, если сеанс «На связи» не будет успешно завершен. Вы также можете отменить сеанс «На связи».

1. Откройте приложение «Сообщения» и выберите человека, которого Вы хотите уведомлять.
2. Коснитесь «Новое сообщение» вверху экрана и добавьте получателя, либо выберите существующий разговор.
3. Коснитесь ＋, коснитесь «На связи», затем коснитесь «Изменить».

   Для отображения пункта «На связи» Вам может потребоваться коснуться «Еще».
4. Выберите «Когда я прибуду».
5. Коснитесь «Изменить» и введите свое место назначения в поле поиска.
6. Чтобы задать радиус места прибытия, коснитесь «Малый», «Средний» или «Большой» внизу экрана. Когда Вы окажетесь внутри этого радиуса, Ваш друг получит уведомление о Вашем прибытии.
7. Коснитесь «Готово».
8. Коснитесь «За рулем» «В транспорте» или «Пешком», затем при необходимости коснитесь «Продлить».

   Если Ваше устройство не движется в направлении Вашего места назначения, Вы получите запрос, и у Вас будет 15 минут для ответа. При отсутствии ответа Ваш доверенный человек автоматически получит уведомление.

Когда Ваш iPhone прибудет в место назначения, заданное для сеанса «На связи» в поездке, сеанс «На связи» завершится, а Ваш контакт получит уведомление о том, что Вы прибыли.

# Обнаружение нежелательного отслеживания

Компания Apple разработала AirTag и сеть Локатора, чтобы помочь пользователям следить за местонахождением своих вещей и в то же время предотвратить нежелательное отслеживание. Следующим шагом по защите пользователей от нежелательного отслеживания стало создание отраслевого стандарта совместными усилиями Apple и Google. Благодаря ему пользователи iPhone, iPad и Android могут получать предупреждения, если их геопозиция отслеживается.


Если Вам угрожает опасность, обратитесь в местные правоохранительные органы. Если вещь относится к продуктам Apple, правоохранительные органы могут связаться с Apple и запросить информацию об этой вещи (https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf). Возможно, Вам потребуется предоставить AirTag, AirPods или аксессуар с поддержкой сети «Локатор», а также серийный номер устройства.

### Уведомления о нежелательном отслеживании

Доступность ПО для уведомлений о нежелательном отслеживании.

- Уведомления о нежелательном отслеживании для AirTag и других аксессуаров с поддержкой сети Локатора доступны на iPhone или iPad с iOS 14.5 либо iPadOS 14.5 или новее.
- Уведомления о нежелательном отслеживании для неизвестных отслеживающих устройств Bluetooth, совместимых со спецификацией об обнаружении нежелательных трекеров, отслеживающих геопозицию, доступны на iPhone с iOS 17.5 или новее.
- Google обеспечивает обнаружение нежелательного отслеживания на устройствах с Android 6.0 или новее. Пользователи более ранних версий операционных систем могут обновить или использовать приложение «Детектор трекеров».

### Включение уведомлений о нежелательном отслеживании

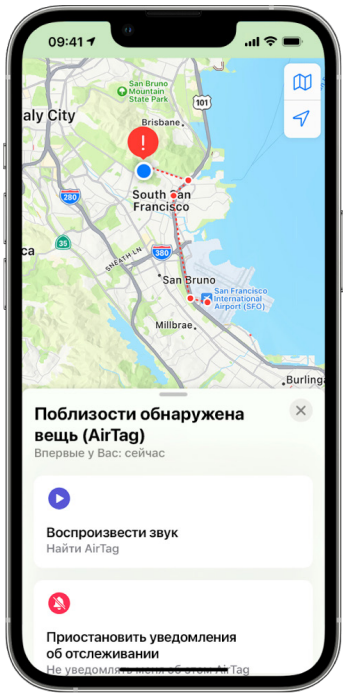
Чтобы получать уведомления о нежелательном отслеживании на iPhone или iPad с iOS 14.5 либо iPadOS 14.5 или новее, выполните указанные действия.

- Выберите «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации» и включите параметр «Службы геолокации».
- Выберите «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации» > «Системные службы» и включите параметр «Найти iPhone».
- Выберите «Настройки» > «Bluetooth» и включите параметр «Bluetooth».
- Выберите «Настройки» > «Уведомления», прокрутите вниз до пункта «Уведомления об отслеживании» и включите параметр «Допуск уведомлений».
- Выключите Авиарежим. Когда устройство находится в Авиарежиме, Вы не получаете уведомления об отслеживании.

### Если Вы получили уведомление о нежелательном отслеживании

Выполните перечисленные ниже действия для обнаружения вещи.

1. Коснитесь уведомления.
2. Коснитесь «Продолжить», затем коснитесь «Воспроизвести звук». Либо, если это доступно, коснитесь «Поиск поблизости», чтобы использовать функцию «Точное местонахождение» для обнаружения неизвестной вещи.



Если воспроизведение звука недоступно или Вам не удается обнаружить вещь с помощью функции «Точное местонахождение», возможно, эта вещь больше не находится рядом с Вами. Если Вы считаете, что она все еще поблизости, обыщите свои вещи, чтобы обнаружить ее. Отслеживающее устройство может находиться на Вас или в Ваших вещах. Оно может быть спрятано в местах, которые Вы редко проверяете, например, в кармане куртки, внешнем кармане сумки или в автомобиле. Если Вы не можете найти устройство и считаете, что Вам угрожает опасность, доберитесь до безопасного места и свяжитесь с правоохранительными органами.

**Если ранее Вы получили уведомление о нежелательном отслеживании и хотите снова проверить эту информацию, выполните одного из указанных действий.**

- *На iPhone или iPad.* Откройте приложение «Локатор», коснитесь «Вещи», а затем — «Обнаруженные с Вами вещи».
- *На Mac.* Откройте приложение «Локатор», нажмите «Вещи», а затем — «Обнаруженные с Вами вещи».

### Если Вы обнаружили AirTag, аксессуар с поддержкой сети «Локатор» или совместимое отслеживающее устройство Bluetooth

Выполните указанные ниже действия для получения информации об устройстве.

1. Поднесите верхнюю часть iPhone к вещи и дождитесь получения уведомления.
2. Коснитесь уведомления. Откроется сайт, содержащий следующую информацию о вещи:
   - серийный номер или идентификатор устройства;
   - последние четыре цифры телефонного номера или частично скрытый адрес электронной почты пользователя, зарегистрировавшего вещь. Эта информация может помочь Вам опознать владельца вещи, если Вы с ним знакомы.
3. Если владелец пометил вещь как потерянную, может отобразиться сообщение с информацией о том, как с ним связаться.


### Если Вы считаете, что вещь используется для отслеживания Вашей геопозиции

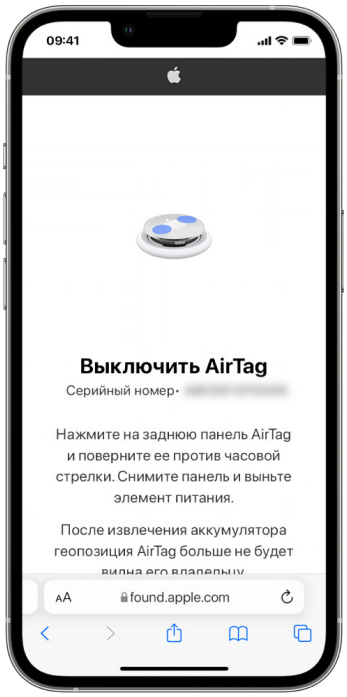
**ВАЖНО!** Прежде чем вносить изменения, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность. Если Вам угрожает опасность, обратитесь в местные правоохранительные органы. Если вещь относится к продуктам Apple, правоохранительные органы могут связаться с Apple и запросить информацию об этой вещи (https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf). Возможно, Вам потребуется предоставить AirTag, AirPods или аксессуар с поддержкой сети Локатора, а также серийный номер устройства.

1. Сделайте снимок экрана с информацией о вещи и ее владельце.
2. Выключите устройство и остановите отправку его геопозиции: коснитесь параметра «Инструкция по выключению» и следуйте инструкциям на экране.

3. Если Вам угрожает опасность, обратитесь в местные правоохранительные органы. Если вещь относится к продуктам Apple, правоохранительные органы могут связаться с Apple и запросить информацию об этой вещи. Возможно, Вам потребуется предоставить AirTag, AirPods или аксессуар с поддержкой сети «Локатор», а также серийный номер устройства.

   См. документ https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (на английском языке).

После выключения устройства владелец больше не сможет видеть его текущее местоположение. Вы также перестанете получать уведомления о нежелательном отслеживании для этой вещи.




### Обнаружение AirTag или аксессуара с поддержкой сети «Локатор» с помощью устройства Android

Подробнее об обнаружении нежелательного отслеживания на устройствах Android см. в статье службы поддержки Как обнаруживать неизвестные трекеры. (https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&)

### Если звучит сигнал AirTag

Если AirTag в течение определенного времени не находится рядом с владельцем, при перемещении он издает сигнал, слышный окружающим людям. Если Вы нашли AirTag после того, как прозвучал сигнал, Вы можете использовать любое устройство с модулем NFC (связь ближнего поля), такое как iPhone или телефон Android, чтобы проверить, отметил ли его владелец как пропажу, а затем вернуть потерянное.

**ВАЖНО!** Если Вам угрожает опасность, обратитесь в местные правоохранительные органы, которые могут обратиться в Apple за помощью (https://www.apple.com/legal/transparency/government-information.html). Возможно, Вам потребуется предоставить AirTag или его серийный номер.

### Устройства, подключенные к другому Аккаунту Apple

Если при попытке настроить AirPods, AirTag или другой аксессуар в сети Локатора Вы видите сообщение о том, что этот аксессуар подключен к другому Аккаунту Apple, то сначала необходимо удалить этот аксессуар из другого Аккаунта Apple. Подробнее о том, как удалить вещь или устройство из другого Аккаунта Apple или разорвать пару с ним, см. в статье службы поддержки Apple Если объект или устройство подключены к другому Аккаунту Apple (https://support.apple.com/102620).

### Общий доступ к AirTag

Общий доступ к вещам дает владельцам трекера AirTag возможность использовать его совместно с пятью другими пользователями одновременно. Люди, одолжившие вещь с трекером, могут:

- просматривать геопозицию AirTag в Локаторе;
- находить AirTag с помощью функции «Точное местонахождение»;
- воспроизводить звук в случае потери AirTag;
- получать уведомление в случае присоединения нового участника к группе общего доступа;
- просматривать Аккаунт Apple каждого участника группы общего доступа или контактную информацию участников группы, сохраненных в Контактах.

*Примечание.* Участники группы общего доступа не видят, у какого пользователя в данный момент находится AirTag.

Поскольку все участники группы общего доступа могут видеть геопозицию AirTag, уведомления о нежелательном отслеживании этого AirTag выключены для всех участников группы. Когда участник покидает группу общего доступа или владелец вещи удаляет участника из группы, этот участник перестает видеть геопозицию AirTag, а уведомления о его нежелательном отслеживании снова включаются.

Подробные сведения приводятся в разделе Открытие доступа к AirTag или другой вещи в приложении «Локатор» на iPhone в Руководстве пользователя iPhone. (https://support.apple.com/guide/iphone/iph419cc5f28)

### Выход из группы общего доступа

Если Вы хотите удалить себя из группы общего доступа, Вы можете воспользоваться Локатором или функцией «Проверка безопасности».

**ВНИМАНИЕ!** После выхода из группы Вы не сможете видеть геопозицию AirTag, а уведомления о его нежелательном отслеживании снова включатся. Перед выходом из группы общего доступа Вы можете проверить, находится ли этот AirTag рядом с Вами.

1. Откройте «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».
2. Коснитесь «Управление доступом».
3. Коснитесь «Вещи» > «Закрыть доступ».

### Использование Локатора

Выход из группы с помощью Локатора.

1. Откройте приложение «Локатор».
2. Коснитесь «Вещи», затем коснитесь вещи, из группы которой хотите выйти.
3. Коснитесь «Удалить».

### Использование функции «Проверка безопасности»

Выход из группы с помощью функции «Проверка безопасности».

1. Коснитесь «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».
2. Коснитесь «Управление доступом».
3. Коснитесь «Вещи» > «Закрыть доступ».

### Удаление других участников из группы общего доступа с помощью Локатора

Вы как владелец группы можете удалять других участников из группы общего доступа с помощью Локатора.

1. Откройте приложение «Локатор».
2. Коснитесь «Вещи», затем коснитесь имени вещи.
3. Коснитесь имени участника, которого хотите удалить.
4. Коснитесь «Удалить» > «Закрыть доступ».

### Удаление других участников из группы общего доступа с помощью функции «Проверка безопасности»

Вы как владелец группы можете удалять других участников из группы общего доступа с помощью функции «Проверка безопасности».

1. Коснитесь «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».
2. Коснитесь «Управление доступом» > «Продолжить».
3. Коснитесь имени человека, которому хотите закрыть доступ, затем коснитесь «Проверить доступ».
4. Коснитесь «Вещи» > «Закрыть доступ».

# Локатор и доступ к геопозиции

Приложение «Локатор» для iPhone, iPad, Mac и Apple Watch помогает Вам находить свои устройства и дает возможность делиться геопозицией с другими пользователями.


Если Вы настроили Семейный доступ и используете общий доступ к геопозиции, члены Вашей семьи автоматически появятся на вкладке «Люди», но им по-прежнему нужно будет делиться своей геопозицией с Вами. См. раздел Управление настройками Семейного доступа далее в этом руководстве.

### Сведения о доступе к геопозиции и возможностях ее просмотра

Когда Вы делитесь своей геопозицией с помощью Локатора, пользователи, с которыми Вы делитесь, могут просматривать ее в приложениях, перечисленных в таблице ниже.

Если Вы и человек, с которым Вы делитесь геопозицией, используете iPhone с iOS 15 или новее, Вы также делитесь своей геопозицией в реальном времени во всех приложениях, перечисленных ниже. Когда Вы движетесь, человек, с которым Вы делитесь, может просматривать направление Вашего движения и Вашу скорость.


| Приложение | Описание |
|---|---|
| Локатор | В приложении Локатор другие пользователи могут просмотреть Вашу геопозицию, перейдя на вкладку «Люди» и коснувшись Вашего имени. |
| Локатор | Если Вы и другой человек делитесь геопозициями друг с другом, используете iPhone 15 и находитесь поблизости друг от друга, Вы можете определить точные геопозиции друг друга с помощью функции «Точное местонахождение». Когда Вы находитесь поблизости от этого человека, функция «Точное местонахождение» помогает этому человеку найти Вас, пока Вы не окажетесь в нескольких метрах друг от друга. Если кто-либо пытается найти Вас с помощью функции «Точное местонахождение», Вы получаете уведомление об этом.<br>Подробные сведения приводятся в разделе Использование функции «Точное местонахождение» на iPhone 15 для встречи с другом в Руководстве пользователя iPhone. (https://support.apple.com/guide/iphone/iph3effd0ed6) |

| Приложение | Описание |
| --- | --- |
| Локатор | Если Вы настроили Семейный доступ и используете общий доступ к геопозиции, члены Вашей семьи автоматически отображаются на вкладке «Люди», но сеанс общего доступа к геопозиции не начнется, пока Вы не поделитесь своими геопозициями друг с другом. См. раздел Управление настройками Семейного доступа далее в этом руководстве. |
| Сообщения | Когда пользователи, с которыми Вы делитесь своей геопозицией, касаются значка Вашего контакта в Сообщениях, они переходят на экран «Подробнее», где показана Ваша текущая геопозиция, отправляемая с помощью Локатора. |
| Сообщения | В Сообщениях в iOS 17 либо iPadOS 17 и новее пользователи, с которыми Вы делитесь своей геопозицией, также могут видеть Ваше приблизительное местонахождение вверху экрана разговора. |
| Карты | Когда пользователи, с которыми Вы делитесь своей геопозицией, выполняют поиск по Вашему имени в Картах, они видят на карте Вашу текущую геопозицию, отправляемую с помощью Локатора. |

### Уведомления об изменении геопозиции

С помощью приложения «Локатор» Вы можете уведомить друга об изменении Вашей геопозиции (https://support.apple.com/guide/iphone/iph9bfec93b1). Люди, с которыми Вы делитесь своей геопозицией, также могут настроить уведомления о ее изменении.

Вы можете выключить любые уведомления об изменении своей геопозиции. В том числе уведомления, установленные Вами, и уведомления, созданные Вашими друзьями.

1. Чтобы просмотреть все уведомления о себе, выполните одно из указанных действий.
   - *На iPhone или iPad.* Откройте приложение «Локатор», затем коснитесь «Я».
   - *На Mac.* Откройте приложение «Локатор», нажмите «Я», затем нажмите ⓘ.
2. Перейдите к разделу «Уведомления о Вас».
   - Если раздел «Уведомления о Вас» *отображается*, выберите имя для просмотра подробной информации.
   - Если раздел «Уведомления о Вас» *не отображается*, то Ваши друзья не получают уведомлений об изменениях Вашей геопозиции.
3. Если Вы видите уведомление, которое хотите удалить, выберите имя, затем выберите уведомление.
4. Удалите уведомление, затем подтвердите, что Вы хотите его удалить.

### Закрытие доступа к Вашей геопозиции в Локаторе на iPhone или iPad

Когда Вы закрываете другому пользователю доступ к своей геопозиции любым из способов, перечисленных ниже, Ваша геопозиция перестает отображаться у этого пользователя в приложениях «Локатор», «Карты», «Контакты» и «Сообщения».

**ВАЖНО!** Когда Вы закрываете другому пользователю доступ к своей геопозиции, пользователь может это заметить. В более ранних версиях операционных систем пользователь может получить уведомление в Сообщениях о том, что Вы больше не делитесь своей геопозицией.

1. Откройте приложение «Локатор».
2. Выполните одно из описанных ниже действий.
   - *Закрытие доступа для одного пользователя.* Выберите вкладку «Люди», найдите человека, с которым Вы не хотите делиться своей геопозицией, коснитесь имени этого человека, прокрутите вниз и коснитесь «Не делиться геопозицией».
   - *Закрытие доступа для всех пользователей.* Выберите вкладку «Я» и выключите параметр «Делиться геопозицией».

   *Примечание.* Если приложение «Локатор» удалено с Вашего устройства, Вы можете выключить Службы геолокации (выберите «Настройки» > > «Конфиденциальность и безопасность» > «Службы геолокации»), чтобы гарантировать, что Ваша геопозиция никому не передается. Затем снова загрузите приложение «Локатор» из App Store.

### Закрытие доступа к Вашей геопозиции в Сообщениях на iPhone или iPad

Когда Вы прекращаете делиться своей геопозицией любым из способов, перечисленных ниже, Ваша геопозиция перестает отображаться в приложении «Сообщения» на устройствах других пользователей.

1. Откройте приложение «Сообщения».
2. Выполните одно из описанных ниже действий.
   - *Закрытие доступа к геопозиции в разговоре.* Выберите разговор с человеком, с которым Вы не хотите делиться своей геопозицией, коснитесь имени собеседника вверху разговора, затем коснитесь «Закрыть доступ».
   - *Закрытие доступа путем удаления разговора.* В списке разговоров в Сообщениях смахните влево по разговору, коснитесь , затем коснитесь «Да», чтобы подтвердить, что Вы не хотите делиться своей геопозицией с участниками этого разговора.

### Закрытие доступа к Вашей геопозиции в Контактах на iPhone или iPad

Когда Вы прекращаете делиться своей геопозицией любым из способов, перечисленных ниже, Ваша геопозиция перестает отображаться в приложении «Контакты» на устройствах других пользователей.

1. Откройте приложение «Контакты».
2. Коснитесь имени человека.
3. Коснитесь «Не делиться геопозицией».

### Когда следует выключить функцию «Найти iPhone» в случае потери или кражи устройства

С помощью функции «Найти iPhone» (в разделе «Настройки» > «Локатор») Вы можете найти свой телефон в случае его потери или кражи.

Когда функция «Найти iPhone» включена, Ваше устройство можно найти в сети Локатора в течение 24 часов с момента его выключения или отключения от интернета. Геопозиция устройства отображается в Локаторе на вкладке «Устройства» на других Ваших устройствах, а также для участников Семейного доступа, с которыми Вы делитесь своей геопозицией.

Если Вам нужно добраться до безопасного места и Вы хотите выключить устройство, но переживаете, что эту функцию могут использовать, чтобы найти Вас, при выключении устройства Вы можете временно отключить сеть Локатора. Для этого коснитесь параметра «iPhone можно найти даже после выключения» в разделе выключения смахиванием и следуйте инструкциям на экране. Обратитесь к инструкции ниже, чтобы выключить эту функцию.

**ВНИМАНИЕ!** Выключив приложение «Найти [*название устройства*]» и сеть Локатора, Вы не сможете найти и заблокировать потерянное или украденное устройство, а также стереть с него все данные.

- *На iPhone или iPad*. Откройте «Настройки» > [*Ваше имя*] > «Локатор» > «Найти iPhone» > «Сеть Локатора».

  После выключения этой функции Вы не сможете ею воспользоваться, если потерянное или украденное устройство выключено.

- На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Аккаунт Apple» > «iCloud», затем рядом с пунктом «Найти Mac» нажмите «Параметры».

- На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Аккаунт Apple» > «iCloud», затем рядом с пунктом «Найти Mac» нажмите «Параметры».

# Управление настройками Служб геолокации

Службы геолокации дают Вам возможность выбирать приложения (такие как Карты, Камера или Погода) и сайты, которым Вы хотите предоставить доступ к своей геопозиции. Когда Службы геолокации включены, они используют информацию от сетей различных типов, чтобы определять Вашу приблизительную или точную геопозицию. Службы геолокации доступны на iPhone, iPad, Mac и Apple Watch.


Когда какое-либо приложение использует Службы геолокации, в меню статуса вверху экрана iPhone и iPad и в строке меню на Mac отображается значок Служб геолокации.

Даже если выключить Службы геолокации, приложения и сайты сторонних разработчиков могут по-прежнему использовать другие способы определения Вашей геопозиции. В целях безопасности информация о геопозиции Вашего устройства может быть отправлена во время экстренного вызова независимо от того, включены ли Службы геолокации.

**Включите или выключите параметр «Службы геолокации».**

При настройке устройства отображается запрос, нужно ли включить Службы геолокации. После настройки можно в любой момент включить или выключить Службы геолокации.

- *На iPhone или iPad.* Выберите «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации», затем включите или выключите доступ к геопозиции.
- На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Конфиденциальность и безопасность» > «Службы геолокации», включите или выключите параметр «Службы геолокации», при необходимости введите пароль, затем нажмите «Снять защиту».
- На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Защита и безопасность», затем нажмите «Конфиденциальность». Нажмите «Службы геолокации». Если замок в левом нижнем углу закрыт, нажмите его, чтобы снять защиту с панели настроек. Включите или выключите Службы геолокации.
- *На Apple Watch.* Выберите «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации».

### Включение Служб геолокации

При настройке устройства отображается запрос, нужно ли включить Службы геолокации. После настройки можно в любой момент включить или выключить Службы геолокации.

Если Службы геолокации не были включены во время настройки.

- *На iPhone или iPad.* Откройте «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации» и включите параметр «Службы геолокации».
- На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Защита и безопасность» > «Службы геолокации», включите параметр «Службы геолокации», введите пароль, затем нажмите «Снять защиту».
- На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Защита и безопасность», затем нажмите «Конфиденциальность». Нажмите «Службы геолокации». Если замок в левом нижнем углу закрыт, нажмите его, чтобы снять защиту с панели настроек, затем выберите «Включить Службы геолокации».

### Выбор приложений, которые могут использовать Службы геолокации на iPhone или iPad

Некоторые приложения могут не работать, когда Службы геолокации не включены. Когда приложению впервые понадобится доступ к Службам геолокации, Вы получите уведомление с запросом на разрешение доступа. Выберите один из перечисленых ниже вариантов.

- Однократно
- При использовании
- Запретить

Вы также можете просмотреть или изменить доступ к своей геопозиции и указать, как часто может использоваться Ваша геопозиция. Далее приведены инструкции для iPhone или iPad.

1. Выберите «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации», затем просмотрите или измените настройки доступа для приложения.

   Чтобы узнать, зачем приложение хочет использовать Службы геолокации, коснитесь приложения.

2. Укажите, насколько точную геопозицию Вы хотите сообщать приложению.

   - Чтобы разрешить приложению использовать Вашу точную геопозицию, оставьте параметр «Точная геопозиция» включенным.
   - Чтобы делиться только приблизительной геопозицией (этого может быть достаточно, если приложению не требуется точное местоположение), выключите параметр «Точная геопозиция».

   *Примечание.* Если для доступа приложения установлено значение «Спросить в следующий раз», при следующей попытке приложения использовать Вашу геопозицию Вы снова получите запрос на включение Служб геолокации.

### Выбор приложений, которые могут использовать Службы геолокации на Mac

1. Выполните одно из описанных ниже действий.

   - На Mac с macOS 13 или новее. Откройте меню Apple , нажмите «Системные настройки», нажмите «Конфиденциальность и безопасность» , нажмите «Службы геолокации», выключите параметр «Службы геолокации», введите пароль, затем нажмите «Снять защиту».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple  > «Системные настройки» > «Конфиденциальность и безопасность» , нажмите «Службы геолокации» и снимите флажок «Включить Службы геолокации». Возможно, чтобы внести изменения, сначала потребуется снять защиту в Системных настройках. Для этого в левом нижнем углу нажмите , затем введите пароль.

2. Установите флажок рядом с приложением, чтобы разрешить ему использовать Службы геолокации. Снимите флажок, чтобы выключить Службы геолокации для этого приложения.

   Если выключить Службы геолокации для определенного приложения, при следующей попытке приложения использовать Вашу геопозицию Вы снова получите запрос на включение Служб геолокации.

3. Прокрутите вниз списка приложений до Системных служб, затем нажмите кнопку «Подробнее», чтобы отобразились системные службы, которые используют Вашу геопозицию.

   Чтобы разрешить компьютеру Mac использовать геопозицию в Предложениях Siri и Предложениях Safari, установите флажок «Геолокационные предложения».

   Чтобы разрешить компьютеру Mac запоминать значимые для Вас геопозиции и предоставлять полезную и релевантную информацию в приложении «Карты», «Календарь», «Напоминания», а также многих других, установите флажок «Важные геопозиции». Важные геопозиции защищены сквозным шифрованием, и Apple не может ознакомиться с ними. Нажмите кнопку «Подробнее», чтобы просмотреть список распознанных геопозиций. Чтобы удалить геопозицию из списка, выберите ее и нажмите —. Чтобы удалить все геопозиции, нажмите , затем нажмите «Очистить журнал».

# Управление автоматической отправкой примерного времени прибытия в приложении «Карты»

В приложении «Карты» на iPhone и iPad (модели Wi-Fi + Cellular) можно автоматически сообщать примерное время прибытия в избранную геопозицию любому пользователю из Ваших контактов. Если Вы настроили эту функцию, то при начале движения к избранной геопозиции Ваши контакты будут видеть примерное время Вашего прибытия. После начала движения по маршруту внизу Вашего экрана будет показано, что примерное время Вашего прибытия отображается у других людей.


**Управление сообщением о примерном времени прибытия на iPhone или iPad**

1. В приложении «Карты» на iPhone или iPad (модели Wi-Fi + Cellular) коснитесь значка профиля справа от поля поиска.
2. Выберите «Избранное», чтобы открыть окно со всеми геопозициями, которые Вы отметили как избранные.
3. Коснитесь ⓘ рядом с избранным пунктом интереса.
4. Прокрутите вниз до раздела «Сообщить о прибытии», чтобы просмотреть имена людей, которым автоматически сообщается примерное время Вашего прибытия.
5. Чтобы удалить человека, коснитесь «Не делиться» рядом с именем человека, которого Вы хотите удалить.
6. Чтобы добавить человека, коснитесь «Добавить человека», затем в приложении «Контакты» выберите человека, которому хотите автоматически сообщать примерное время Вашего прибытия в этот пункт интереса.
7. Повторите шаги 3–6 для дополнительных пунктов интереса в Избранном.

### Прекращение автоматической отправки примерного времени прибытия после начала движения по маршруту

Можно прекратить автоматическую отправку примерного времени прибытия даже после того, как Вы начали движение к избранной геопозиции. Если Вы прекратите отправку примерного времени прибытия этим способом, человек больше не сможет видеть примерное время Вашего прибытия или информацию о маршруте, однако он уже получил на своем устройстве уведомление о том, что Вы двигаетесь в сторону избранной геопозиции.

**ВАЖНО!** Этот способ не означает полного выключения автоматической отправки этому человеку. В следующий раз, когда Вы направитесь в эту избранную геопозицию, снова будет запущена автоматическая отправка примерного времени прибытия. Чтобы предотвратить отправку, Вам необходимо удалить контакт из списка «Сообщить о прибытии» для избранной геопозиции.

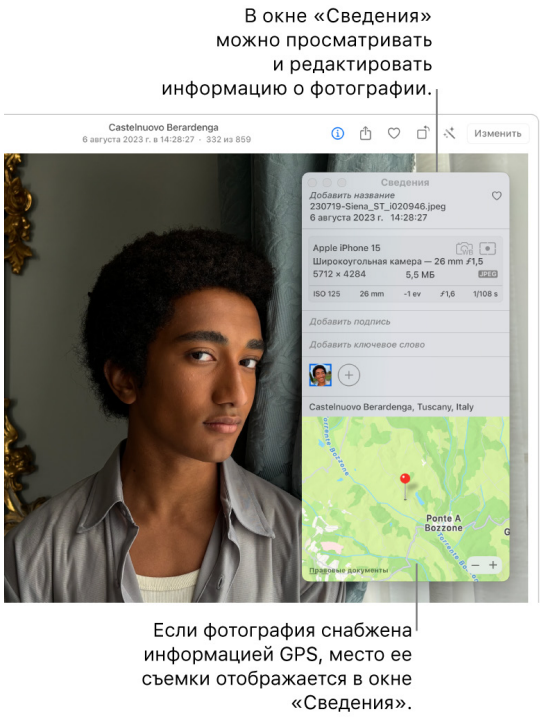
1. В приложении «Карты» на iPhone или iPad (модели Wi-Fi + Cellular) коснитесь «Делюсь с [*имя контакта*]» внизу экрана.
2. Найдите в списке человека, которому больше не хотите сообщать о прибытии.
3. Выберите «Закрыть доступ» под именем этого человека.

# Управление доступом к метаданным о геопозиции в приложении «Фото»

Когда в приложении «Камера» включены Службы геолокации, приложение определяет геопозицию снятых фото и видео на основе сведений (называемых метаданными), полученных от сотовых сетей, Wi-Fi, GPS и Bluetooth. Эти координаты, встроенные в каждое фото и видео, помогают Вам находить фото и видео в приложении «Фото» по месту съемки и просматривать коллекции по местам съемки в альбоме «Места».

Когда Вы делитесь фото и видео с метаданными о геопозиции, пользователи, с которыми Вы поделились, могут просмотреть эти метаданные и узнать место съемки. Если Вы не хотите делиться метаданными о геопозиции своих фото и видео, Вы можете удалить имеющиеся метаданные и запретить их сбор в дальнейшем.

### Просмотр фото с метаданными о геопозиции на iPhone и iPad




В альбоме «Места» в приложении «Фото» можно легко просматривать в Вашей медиатеке фотографии, в которые встроены метаданные геопозиций.

1. Откройте приложение «Фото», затем коснитесь «Альбомы».
2. Коснитесь альбома «Места» и выполните одно из указанных действий.
   - Чтобы просмотреть фото, снятые в определенный период времени, коснитесь варианта «Сетка» для отображения объектов в хронологическом порядке.
   - Чтобы просмотреть фото, снятые в определенных местах, коснитесь варианта «Карта» для отображения объектов по месту съемки.

### Просмотр фото с метаданными о геопозиции на Mac

В альбоме «Места» в приложении «Фото» можно легко просматривать в Вашей медиатеке фотографии, в которые встроены метаданные геопозиций.

1. В приложении «Фото» на Mac выберите фото для просмотра.
2. Нажмите ⓘ и просмотрите информацию о месте съемки.

### Удаление метаданных о геопозиции в приложении «Фото» на iPhone или iPad

Удаление метаданных о геопозиции определенного фото.

1. Откройте приложение «Фото», затем коснитесь «Альбомы».
2. Коснитесь альбома «Места» и выполните одно из указанных действий.
   - Чтобы просмотреть фото, снятые в определенный период времени, коснитесь варианта «Сетка» для отображения объектов в хронологическом порядке.
   - Чтобы просмотреть фото, снятые в определенных местах, коснитесь варианта «Карта» для отображения объектов по месту съемки.
3. Откройте фото, для которого Вы хотите удалить метаданные о геопозиции, затем коснитесь ⓘ или смахните вверх.

   В приложении «Карты» появится изображение, показывающее место съемки фото.
4. Чтобы удалить метаданные о геопозиции, коснитесь «Изменить», затем коснитесь «Удалить геопозицию».

### Удаление метаданных о геопозиции в приложении «Фото» на Mac

Удаление метаданных о геопозиции фото.

1. В приложении «Фото» на Mac выберите фото, которые Вы хотите изменить.
2. Выберите меню «Изображение» > «Геопозиция», затем выберите «Скрыть геопозицию» или «Вернуть исходную геопозицию».

### Прекращение сбора метаданных о геопозиции в приложении «Камера» на iPhone или iPad

Сбор метаданных геопозиций для фото и видео может выполняться только в том случае, если приложение «Камера» имеет доступ к Службам геолокации.

- Откройте «Настройки», коснитесь параметра «Конфиденциальность и безопасность» > «Службы геолокации» > «Камера», затем коснитесь «Никогда».

  Если Вы не хотите полностью прекращать сбор метаданных о геопозиции, вместо выбора варианта «Никогда» выключите параметр «Точная геопозиция». Это позволит приложению «Камера» собирать данные о Вашей приблизительной, а не точной геопозиции.

### Скрытие метаданных о геопозиции при предоставлении доступа к фото в приложении «Фото» на iPhone или iPad

Можно делиться фото с другими пользователями, не предоставляя им информацию о месте съемки.

1. Выполните одно из перечисленных ниже действий.
   - Откройте приложение «Камера», выберите фотопленку, затем выберите одно или несколько фото, которыми Вы хотите поделиться.
   - Откройте приложение «Фото», затем выберите одно или несколько фото, которыми Вы хотите поделиться.
2. Коснитесь, затем коснитесь «Параметры».
3. Выключите параметр «Геопозиция» и коснитесь «Готово».
4. Поделитесь фото любым из способов, предлагаемых на странице экспорта.

# Управление контентом

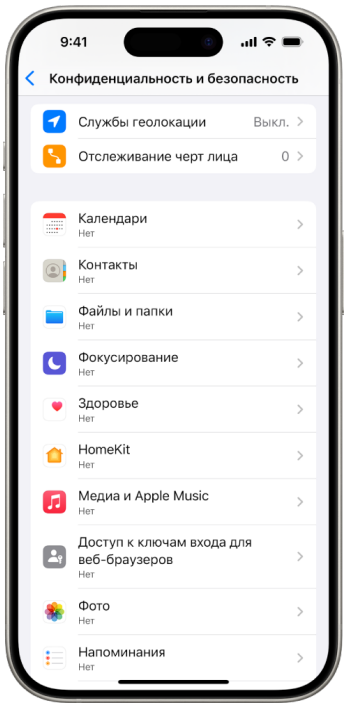
## Основные

### Функции конфиденциальности приложений в продуктах Apple

В продуктах Apple есть настройки, функции и элементы управления, помогающие Вам контролировать данные, которыми Вы делитесь с приложениями.

### Просмотр и изменение настроек конфиденциальности приложений на устройствах Apple

Настройки конфиденциальности на Вашем устройстве были тщательно разработаны таким образом, чтобы Ваши данные были у Вас под контролем. Например, Вы можете разрешить приложению социальной сети использовать Вашу камеру, чтобы Вы могли делать снимки и выгружать их в это приложение. Однако, если кто-то настраивал Ваше устройство или мог получить к нему доступ, зная Ваш код-пароль, Вам стоит пересмотреть настройки конфиденциальности. Вам следует проверить, не изменил ли этот человек заданные Вами настройки.




1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Откройте «Настройки» > «Конфиденциальность и безопасность».
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки», затем в боковом меню выберите «Конфиденциальность и безопасность».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Вход и безопасность», затем нажмите «Конфиденциальность».
2. Просмотрите список типов данных (календари, контакты, фото, напоминания и т. д.).

3. Выберите любой тип данных из списка, чтобы посмотреть, какие приложения на устройстве имеют доступ к этим данным.

   Приложения не будет в списке, пока оно не запросит разрешение. Вы можете дать разрешение или отозвать его у любого приложения, которое запросило доступ. Для фото также можно изменить тип доступа, предоставленного приложениям. Приложение сможет использовать данные того типа, который указан в настройке, только если Вы дадите свое разрешение этому приложению.

   *Примечание.* Изменение настроек конфиденциальности на устройстве Apple влияет только на то, каким образом приложения могут получать доступ к Вашим данным. Чтобы изменить настройки конфиденциальности и безопасности для стороннего приложения (разработанного кем-либо помимо Apple), необходимо войти в учетную запись этого приложения (в самом приложении или в браузере) и обновить настройки там.

### Включение функции «Прозрачность отслеживания в приложениях»

С помощью функции «Прозрачность отслеживания в приложениях» Вы можете разрешать или запрещать определенным приложениям отслеживать Вашу активность в приложениях и на сайтах других компаний. Вы можете отозвать разрешения на отслеживание своей активности в любое время. Если выключить параметр «Запрос приложений на трекинг», Вы не будете получать запросы от приложений, желающих отслеживать Вашу активность. Когда этот параметр выключен, вариант «Попросить не отслеживать» выбирается для всех приложений, запрашивающих разрешение на отслеживание.

- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Откройте «Настройки» > «Конфиденциальность и безопасность» > «Отслеживание» и выключите параметр «Запрос приложений на трекинг».
  - На Apple TV. Откройте «Настройки» > «Основные» > «Конфиденциальность и безопасность» > «Отслеживание» и выключите параметр «Запрос приложений на трекинг».

### Проверка того, как приложения получают доступ к данным, в отчете о конфиденциальности приложений

Если Вы полагаете, что близкий Вам человек установил приложения на Ваш iPhone или iPad без Вашего разрешения либо изменил настройки установленных Вами приложений, Вы можете включить ведение отчета о конфиденциальности приложений.

В этом отчете собраны сведения о том, как часто каждое приложение получает доступ к данным, например к Вашей геопозиции, камере и микрофону.

1. Откройте «Настройки» > «Конфиденциальность и безопасность».
2. Прокрутите вниз и коснитесь «Отчет о конфиденциальности приложений».
3. Включите «Отчет о конфиденциальности приложений».

   Ведение отчета о конфиденциальности приложений можно выключить в любое время. Для этого откройте «Настройки» > «Конфиденциальность и безопасность» > «Отчет о конфиденциальности приложений». После этого с Вашего устройства будут удалены все данные, содержащиеся в отчете.

   *Примечание.* Отчет о конфиденциальности приложений начинает собирать информацию только после включения его ведения, поэтому данные могут появиться только через какое-то время. Информация будет пополняться по мере использования приложений на устройстве. Данные в отчете о конфиденциальности приложений зашифрованы и хранятся только на Вашем устройстве. Отчет содержит сведения о том, как часто и когда какое-либо приложение получало доступ к конфиденциальным данным или датчикам устройства за прошедшие 7 дней. Касайтесь каждого приложения и типа данных, чтобы узнать больше.

## Проверка и удаление приложений

Если Вы предполагаете, что на Ваше устройство было установлено приложение без Вашего разрешения, Вы можете проверить список приложений и убедиться, что в нем отсутствуют нежелательные приложения (инструкции приведены в следующем разделе).

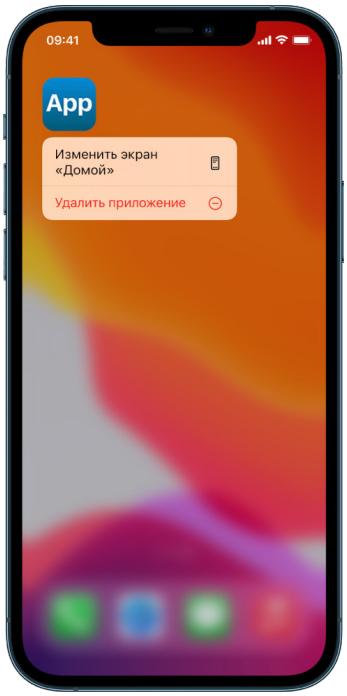
Если Вы не уверены, для чего предназначено определенное приложение, можно попробовать найти его в App Store.

Вы можете проверить и изменить доступ каждого приложения к определенным типам данных (геопозиции, фото и т. д.) с помощью функции «Проверка безопасности» в iOS 16 или новее.

Вы также можете просмотреть настройки сторонних приложений, доступные только внутри этих приложений и недоступные для Apple.

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.

### Удаление приложения из библиотеки приложений на iPhone или iPad




1. Перейдите на экран «Домой», затем смахните влево через все страницы экрана «Домой», пока не откроется библиотека приложений.
2. Коснитесь в поле поиска. Отобразится список всех приложений на устройстве, упорядоченный по алфавиту.
3. Если Вы видите приложение, которое нужно удалить, коснитесь значка этого приложения и удерживайте его, пока не отобразится меню.
4. Коснитесь «Удалить приложение», чтобы его удалить.

   Подробнее см. в разделе Удаление приложений с iPhone в Руководстве пользователя iPhone. (https://support.apple.com/guide/iphone/iph248b543ca)

### Удаление приложения с экрана «Домой»

1. На экране «Домой» коснитесь значка нужного приложения и удерживайте его.
2. Коснитесь «Удалить приложение», затем снова коснитесь «Удалить приложение».

   Подробнее см. в разделе Удаление приложений с iPhone в Руководстве пользователя iPhone. (https://support.apple.com/guide/iphone/iph248b543ca)

### Удаление приложения с Mac

Можно удалять установленные приложения, загруженные из интернета или с внешнего устройства, например с USB-устройства.

1. Нажмите значок Finder в Dock, затем нажмите «Программы» в боковом меню Finder.
2. Выполните одно из описанных ниже действий.
   - *Если приложение в папке.* Откройте папку приложения и найдите ассистент удаления. Если отображается параметр «Удалить [*приложение*]» или ассистент удаления [*приложения*], дважды его нажмите, затем следуйте инструкциям на экране.
   - *Если приложение не в папке или у него нет ассистента удаления.* Если приложение не в папке или у него нет ассистента удаления. Перетяните приложение из папки «Программы» в Корзину (в конце панели Dock).

     **ПРЕДУПРЕЖДЕНИЕ.** Приложение будет навсегда удалено с компьютера Mac, когда Finder очистит Корзину. Если в этом приложении были созданы файлы, возможно, их больше не удастся открыть. Если Вы решите оставить приложение, его можно будет вернуть до очистки Корзины. Выберите приложение в Корзине, затем выберите «Файл» > «Восстановить».

Чтобы удалять приложения, загруженные из App Store, используйте Launchpad.

## Настройки сторонних приложений

### Основные сведения о сторонних приложениях

В экосистеме Apple доступны два типа приложений.

- *Приложения Apple.* Приложения, разработанные компанией Apple, например Сообщения, Календарь, Safari и FaceTime.
- *Сторонние приложения.* Приложения, разработанные не Apple, а другими компаниями и организациями, например Instagram, YouTube, Threads или Google.

Сторонние приложения доступны в App Store и других магазинах приложений. Настройки учетных записей и элементы управления ими в сторонних приложениях могут отличаться от аналогичных элементов в приложениях Apple, а некоторые элементы управления могут быть доступны только внутри приложения или на сайте разработчика. Это различие особенно важно, так как в сторонних приложениях обычно требуются дополнительные действия для управления настройками конфиденциальности и доступа к данным.

### Настройки Apple для сторонних приложений

Некоторыми настройками сторонних приложений можно управлять в приложении «Настройки». Здесь можно выбрать функции устройства Apple, к которым может получать доступ каждое из сторонних приложений. Например, можно разрешить или запретить доступ к геопозиции, контактам и фото, а также возможность отправки уведомлений.

Чтобы задать эти настройки, откройте приложение «Настройки», прокрутите вниз и коснитесь значка приложения, которое Вы хотите настроить.

## Настройки сторонних приложений, доступные только внутри приложения

Некоторые настройки сторонних приложений недоступны для Apple; ими можно управлять только непосредственно в приложении. Чтобы управлять доступом стороннего приложения к передаче информации, откройте соответствующее приложение и перейдите к настройкам учетной записи. Эти настройки могут быть указаны под другим названием, а некоторые настройки могут находиться в разных разделах настроек учетной записи. Проверьте любые настройки, связанные с безопасностью, конфиденциальностью, передачей данных и возможностью обнаружения устройства. Для некоторых приложений может быть необходимо изучить статьи их служб поддержки или часто задаваемые вопросы, чтобы найти все настройки, доступные для изменения.

*Примечание.* В некоторых случаях определенные действия, например удаление учетной записи или запрос копии Ваших данных, могут быть доступны только на сайте разработчика стороннего приложения. Чтобы изменить настройки учетной записи, Вам придется выполнить вход на сайте разработчика стороннего приложения.

### Блокировка, выключение уведомлений и удаление из друзей

Взаимоотношения с пользователями в экосистеме Apple не распространяются на сторонние приложения. Например, те пользователи, которых Вы заблокировали в Сообщениях, Телефоне и FaceTime, не блокируются в Instagram автоматически. Такими взаимоотношениями необходимо управлять непосредственно в стороннем приложении. Подробнее о временной или постоянной блокировке, выключении уведомлений и удалении из друзей можно узнать на сайте поддержки стороннего приложения.

## Проверка настроек перенаправления

Вы можете просматривать и регулировать способы автоматического перенаправления контента и решать, кому Вы его отправляете.

**ВАЖНО!** Прежде чем вносить изменения или удалять информацию, оцените возможное влияние этих действий на Вашу безопасность и конфиденциальность.


### Управление перенаправлением Почты iCloud

В приложении «Почта iCloud» Вы можете просмотреть, перенаправляются ли письма на другой адрес, и выключить эту возможность.

1. Войдите в iCloud на сайте https://www.icloud.com, используя имя пользователя и пароль своего Аккаунта Apple. При необходимости введите код двухфакторной аутентификации.
2. Откройте приложение «Почта», над списком почтовых ящиков нажмите, затем выберите «Настройки».
3. На вкладке «Основные» проверьте, выбран ли параметр «Пересылать мои письма», и просмотрите, на какие адреса пересылаются Ваши письма. При необходимости удалите адрес для перенаправления и остановите пересылку электронных писем.
4. Во вкладке «Правила» просмотрите все правила, в которых для параметра «Далее» выбран вариант «Переслать» или «Переслать на почтовый адрес и отметить прочитанным», и при необходимости измените это правило.
5. Выйдите из iCloud.

### Управление пересылкой текстовых сообщений на iPhone

Когда Вы отправляете сообщение на телефон, отличный от iPhone, оно отправляется в формате текстового сообщения. Вы можете настроить iPhone таким образом, чтобы при отправке или получении текстового сообщения оно отображалось и на других устройствах, где выполнен вход в Ваш Аккаунт Apple. С этих устройств также можно отправлять новые текстовые сообщения. Если Вы беспокоитесь о том, что Ваши сообщения перенаправляются на другие устройства, Вы можете проверить список таких устройств и выключить пересылку текстовых сообщений.

1. На iPhone откройте «Настройки» > «Приложения» > «Сообщения».
2. Коснитесь параметра «Переадресация», чтобы увидеть, какие устройства могут отправлять и получать текстовые сообщения с Вашего устройства.
3. Отмените выбор всех устройств, на которых Вы не хотите получать или отправлять текстовые сообщения.

### Управление переадресацией вызовов и вызовами с других устройств на iPhone

В зависимости от оператора сотовой связи Ваш iPhone может перенаправлять входящие звонки на другой номер телефона. Вы можете проверить, перенаправляются ли входящие звонки на другой номер, и при необходимости выключить этот параметр.

1. На iPhone откройте «Настройки» > «Приложения» > «Телефон» > «Переадресация».

   Если бегунок зеленого цвета, это означает, что переадресация вызовов выключена. Вам также виден номер, на который они перенаправляются.

   *Примечание.* Если такой вариант не отображается, функция переадресации недоступна на Вашем iPhone. Подробности можно узнать у Вашего оператора сотовой связи.

2. При необходимости выключите переадресацию вызовов.

   При выключении переадресации вызовов уведомление на номер телефона, на который она осуществлялась, отправлено не будет.

# Скрытие фото и видео на устройствах Apple

В приложении «Фото» на Mac можно скрывать фото, которые Вы не хотите отображать. Скрытые фото остаются в медиатеке, и при желании Вы можете отобразить их снова.

Открыть приложение «Фото»

### Временное скрытие фото

1. На Mac откройте приложение «Фото».
2. В боковом меню нажмите «Медиатека», затем выберите фото, которые Вы хотите скрыть.
3. Выберите «Изображение» > «Скрыть [*количество*] фото», затем нажмите «Скрыть».

   Выбранные фото будут скрыты, но не будут удалены.

### Отображение скрытых фото

1. На Mac откройте приложение «Фото».
2. В боковом меню нажмите «Медиатека», затем выберите меню «Вид» > «Показать фотоальбом "Скрытые"».

   Альбом «Скрытые» появится в боковом меню в разделе «Другое». Если альбом «Скрытые» защищен паролем, для его разблокировки используйте Touch ID или введите свой пароль. Чтобы скрыть альбом «Скрытые», выберите меню «Вид» > «Скрыть фотоальбом "Скрытые"».
3. Выберите фото, которые Вы хотите отобразить, затем выберите меню «Вид» > «Показать [*количество*] фото».

### Отображение или скрытие коллекции «Скрытые»

По умолчанию альбом «Скрытые» защищен паролем и скрыт. Вы можете разрешить отображать его в коллекции «Другое» и скрыть его в любое время.

1. На Mac откройте приложение «Фото».
2. В боковом меню коснитесь «Медиатека», затем выполните любое из указанных действий.
   - *Отображение альбома «Скрытые» в разделе «Другое»*. Выберите меню «Вид» > «Показать фотоальбом "Скрытые"».
   - *Скрытие альбома «Скрытые»*. Выберите меню «Вид» > «Скрыть фотоальбом "Скрытые"».

Для разблокировки альбома «Скрытые» требуется пароль или Touch ID. Это можно изменить в настройках приложения «Фото».

## Предупреждения о неприемлемых изображениях и видео

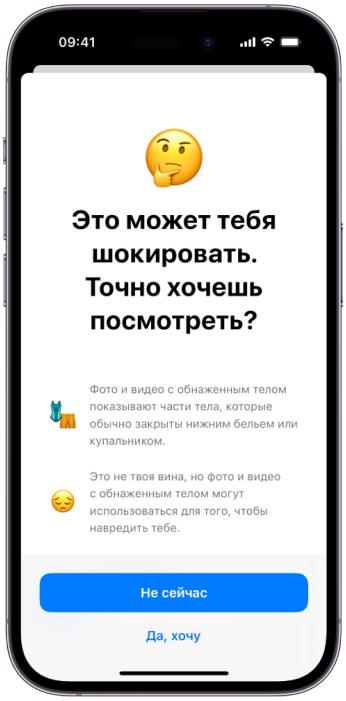
Функция «Предупреждение о нецензурном или неприемлемом контенте» помогает взрослым пользователям избегать просмотра нежелательных изображений и видео с обнаженным телом, полученных в Сообщениях, по AirDrop, в видеосообщениях FaceTime и в постерах контактов через приложение «Телефон». Эта функция задействует ту же технологию защиты конфиденциальности, что и функция «Безопасность общения». Эта функция не является обязательной. Ее можно включить в разделе настроек «Конфиденциальность и безопасность».

Вы (или члены Вашей семьи) будете получать предупреждения перед получением и отправкой откровенных фото. При настройке Экранного времени можно также заблокировать неприемлемый контент и включить ограничения на покупки. См. раздел Как настроить «Экранное время» для члена семьи на iPhone в Руководстве пользователя iPhone.


**Настройка предупреждения об откровенном контенте на iPhone, iPad или Mac**

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Откройте «Настройки» > «Конфиденциальность и безопасность», затем коснитесь «Предупреждение об откровенном контенте».
   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Конфиденциальность и безопасность», затем нажмите «Предупреждение об откровенном контенте».

- На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки» > «Защита и безопасность» , затем нажмите «Предупреждение об откровенном контенте».




2. Прокрутите вниз и коснитесь «Предупреждение о нецензурном или неприемлемом контенте», затем включите «Предупреждение о нецензурном или неприемлемом контенте».
3. Выключите или включите разрешение на обнаружение неприемлемого контента перед его просмотром и на получение рекомендаций, которые помогут сделать безопасный выбор в такой ситуации.

## Получение доказательств, связанных с Аккаунтом Apple другого человека

Компания Apple привержена своей цели обеспечивать безопасность и конфиденциальность наших пользователей. Если Вы столкнулись с преследованием, домогательством или иными противоправными действиями, совершаемыми с использованием технологий, и хотите запросить доказательства, связанные с учетной записью другого человека, для подачи запроса Вам следует обратиться в местные правоохранительные органы или суд. Мы понимаем, что у правоохранительных органов регулярно возникает потребность в получении цифровых доказательств. В нашем юридическом отделе есть специальная команда специалистов, которые отвечают на все запросы от правоохранительных органов по всему миру.

Все другие запросы о получении информации относительно клиентов Apple, включая вопросы клиентов о раскрытии информации, следует направлять по адресу https://www.apple.com/ru/privacy/contact/.

### Руководство Apple по работе с запросами правоохранительных органов

В перечисленных ниже руководствах приведена информация по работе с запросами правоохранительных органов в США и за их пределами.

- *В США:* Руководство по юридическому процессу (https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf)
- *За пределами США:* Руководство по юридическому процессу (https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf)

## Запись подозрительной активности

Если Вы стали жертвой домогательств или беспокоитесь о подозрительной активности в Вашей учетной записи или на Вашем устройстве, Вы можете сделать снимок экрана или запись экрана с соответствующим контентом. Снимок экрана — это изображение того, что показано на экране устройства. Запись экрана — это видеозапись того, что происходит на экране устройства. Она включает аудио, которое воспроизводится на устройстве во время записи. Снимки экрана и записи экрана можно сохранять в виде файлов изображений и видео на iPhone, iPad или Mac.

О том, как запросить у Apple информацию об учетной записи другого человека в связи с преследованиями или домогательствами, см. в разделе Получение доказательств, связанных с Аккаунтом Apple другого человека далее в этом руководстве.


### Как создать снимок или запись экрана на iPhone или iPad

1. Выполните одно из описанных ниже действий.
   - На iPhone или iPad с Face ID. Одновременно нажмите, а затем отпустите боковую кнопку и кнопку увеличения громкости.
   - *На iPhone или iPad с кнопкой «Домой»*. Одновременно нажмите, а затем отпустите кнопку «Домой» и боковую кнопку либо кнопку «Домой» и кнопку «Сон/Пробуждение» (в зависимости от модели).
2. Коснитесь снимка экрана в левом нижнем углу, затем коснитесь «Готово».
3. Выберите «Сохранить в Фото», «Сохранить в Файлы» или «Удалить снимок экрана».

   Если выбрать параметр «Сохранить в Фото», снимок экрана можно будет просмотреть в альбоме «Снимки экрана» приложения «Фото» или в альбоме «Все фото», если функция «Фото iCloud» включена в разделе «Настройки» > «Фото».

### Создание снимков или записей экрана на Mac

1. Нажмите Shift-Command-5 (или воспользуйтесь Launchpad), чтобы открыть приложение «Снимок экрана» и показать инструменты.


2. Нажмите инструмент, чтобы выбрать то, что нужно снять или записать.

   В случае записи части экрана перетяните рамку, чтобы переместить ее, или перетяните края рамки, чтобы изменить размер снимаемой области.

| Действие | Инструмент |
| --- | --- |
| Создание снимка всего экрана | |
| Создание снимка окна | |
| Создание снимка части экрана | |
| Запись всего экрана | |
| Запись части экрана | |

3. Выберите необходимые параметры.

   Доступные параметры зависят от того, создаете ли Вы снимок или запись экрана. Например, можно установить задержку спуска или отображать указатель или нажатия, а также указать место сохранения файла.

   Благодаря параметру «Отображать плавающую миниатюру» проще работать со снимком или записью после их создания. Миниатюра отображается в правом нижнем углу экрана в течение нескольких секунд. Созданный файл можно перетянуть в документ, разметить или отправить перед сохранением в нужном месте.

4. Запуск создания снимка экрана или записи экрана.
   - *Весь экран или его часть.* Нажмите «Снимок».
   - *Только окно.* Наведите указатель на окно, затем нажмите окно.
   - *Запись.* Нажмите «Запись». Чтобы остановить запись, нажмите ⊙ в строке меню.

   Если задан параметр «Отображать плавающую миниатюру», можно выполнить одно из указанных ниже действий, пока миниатюра отображается в правом нижнем углу экрана в течение нескольких секунд.
   - Смахните вправо, чтобы сразу сохранить файл и скрыть его миниатюру.
   - Перетяните миниатюру на документ, в письмо, заметку или окно Finder.
   - Нажмите миниатюру, чтобы открылось окно, в котором можно разметить снимок экрана или обрезать запись, а затем поделиться результатом.

   В зависимости от места сохранения снимка экрана или записи может открыться приложение.

## Восстановление заводских настроек устройства

Если Вы полагаете, что кто-то мог получить физический доступ к Вашему устройству, вмешаться в работу встроенных средств защиты и установить вредоносное ПО, например ПО для отслеживания, Вы можете восстановить заводские настройки устройства. Это поможет гарантировать, что доступ к устройству есть только у Вас.

**ВАЖНО!**

- При восстановлении заводских настроек с устройства стираются все настройки и весь контент. Прежде чем восстанавливать заводские настройки на устройстве, запустите Управление доступом в функции «Проверка безопасности». Проблемы могут быть связаны с настройками общего доступа или доступа для приложений, заданными не так, как Вы предполагали.
- Если Вы стираете весь контент и настройки из-за того, что в работу устройства вмешались посторонние лица, установившие вредоносное ПО, не восстанавливайте устройство из резервной копии. При восстановлении из резервной копии может быть снова установлено вредоносное ПО, от которого Вы пытаетесь избавиться.

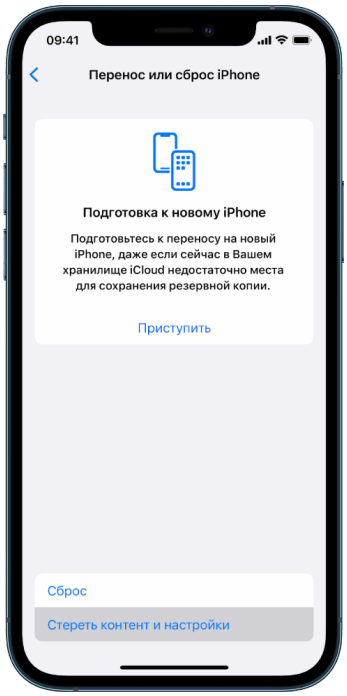
Восстановление заводских настроек.

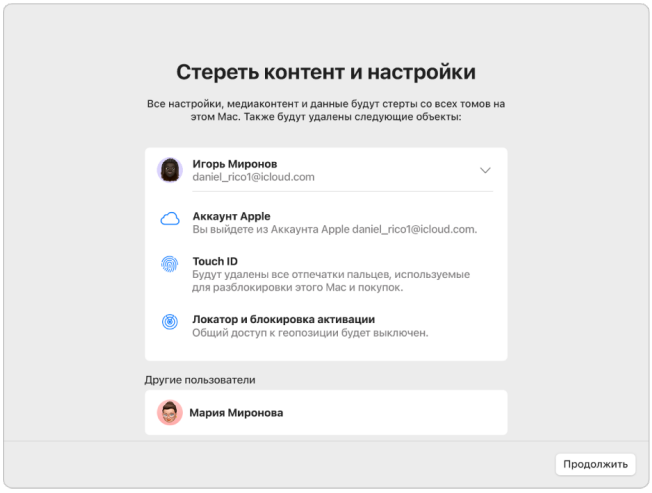
- При этом стираются все хранящиеся на устройстве данные, в том числе данные Face ID и Touch ID, пароли и код-пароли, сообщения, электронная почта, фото, файлы, медиаданные и другая информация.
- Удаляются все приложения, в том числе установленные без Вашего ведома.
- Сбрасываются настройки конфиденциальности, поэтому Вы больше не делитесь своей геопозицией ни с какими людьми или приложениями.
- Устанавливается новейшая версия операционной системы, независимо от того, какая версия была установлена ранее.


Необходимые условия:

- доступ к интернету;
- наличие пароля или код-пароля на устройстве;
- наличие пароля Аккаунта Apple.
- Время

Команда «Стереть контент и настройки» поддерживается на Mac под управлением macOS 12.0.1 или новее. Либо можно стереть все данные с Mac. См. статьи службы поддержки Apple Стирание данных с компьютера Mac с чипом Apple с помощью приложения «Дисковая утилита» (https://support.apple.com/102506) и Стирание данных с компьютера Mac с процессором Intel при помощи Дисковой утилиты (https://support.apple.com/HT208496).



### Для iPhone и iPad

- Восстановление заводских настроек iPhone, iPad или iPod с помощью компьютера (https://support.apple.com/108931) — статья службы поддержки Apple

### Стирание всего контента и настроек на Mac

- Стирание данных с компьютера Mac (с macOS 12.0.1 или новее) — удаление всего контента, настроек и установленных приложений без переустановки macOS для восстановления заводских настроек.
  - Стирание данных с компьютера Mac — для стирания всего контента (приложений и данных) и настроек (например, перед продажей, обменом на скидку или передачей другому человеку) (https://support.apple.com/guide/mac-help/mchl7676b710).
  - Стирание и переустановка macOS — для компьютера Mac с чипом Apple или компьютера Mac с процессором Intel. (https://support.apple.com/guide/mac-help/mh27903)
- Стирание данных с компьютера Mac с чипом Apple с помощью приложения «Дисковая утилита» — статья службы поддержки Apple (https://support.apple.com/102506)
- Стирание данных с компьютера Mac с процессором Intel при помощи Дисковой утилиты — статья службы поддержки Apple (https://support.apple.com/102639)

# Конкретные приложения и функции

## Совершение экстренного вызова или отправка экстренного текстового сообщения на iPhone или Apple Watch

В экстренной ситуации Вы можете быстро позвонить или отправить сообщение в экстренные службы с iPhone или Apple Watch.


Если Вы разрешили отправку своей Медкарты, iPhone сможет отправлять Ваши медданные в экстренные службы после звонка или отправки сообщения на номер 911 или активации функции «Экстренный вызов — SOS» (только в США). Подробнее о Медкарте см. в разделе Создание Медкарты в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph08022b194/#iphbcea12902).

*Примечание.* В некоторых местах для вызова экстренных служб также можно отправить сообщение на номер 911. Там, где такая отправка не поддерживается, Вам может прийти автоответ о том, что сообщение не доставлено. См. статью службы поддержки Apple Отправка текстовых сообщений на номер 911 с помощью iPhone или Apple Watch (https://support.apple.com/101996).

Функция «Экстренный вызов — SOS» дает возможность быстро вызывать помощь и уведомлять контакты на случай ЧП о вызове. Именно поэтому важно, чтобы те, кого Вы выбрали в качестве контактов на случай ЧП, были теми, кому Вы доверяете.

### Изменение настроек функции «Экстренный вызов — SOS» на iPhone

1. Откройте «Настройки» > «Экстренный вызов — SOS».
2. Выполните одно из перечисленных ниже действий.
   - *Включение и выключение функции «Вызов удержанием кнопок».* Нажмите и удерживайте боковую кнопку и кнопку громкости, чтобы начать обратный отсчет до вызова экстренных служб.
   - *Включение и выключение функции «Вызов пятью нажатиями».* Быстро нажмите боковую кнопку пять раз, чтобы начать обратный отсчет до вызова экстренных служб.
   - *Управление контактами на случай ЧП.* В приложении «Здоровье» коснитесь «Настроить контакты на случай ЧП» или «Изменить контакты на случай ЧП». См. раздел Настройка и просмотр Медкарты в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph08022b192).

### Настройка или изменение контактов на случай ЧП на iPhone

Контакты на случай ЧП можно настроить таким образом, чтобы при экстренном вызове iPhone отправлял этим контактам уведомление о том, что Вы вызвали помощь, передавал Вашу геопозицию и уведомлял о ее изменении. Если Вы ранее добавили кого-то в контакты на случай ЧП, но потом передумали, удалите этого человека из контактов на случай ЧП.

Чтобы добавить или удалить контакты на случай ЧП, следуйте инструкции далее.

1. Откройте приложение «Здоровье», затем коснитесь своего изображения в профиле.
2. Коснитесь «Медкарта».
3. Коснитесь «Править», затем прокрутите до раздела «Контакты на случай ЧП».
4. Добавьте или удалите контакт.
   - *Добавление контакта.* Коснитесь, чтобы добавить контакт на случай ЧП (в качестве контакта на случай ЧП нельзя добавить экстренные службы).
   - *Удаление контакта.* Коснитесь рядом с контактом, который нужно удалить, затем коснитесь «Удалить».
5. Чтобы сохранить изменения, коснитесь «Готово».

### Совершение экстренного вызова на заблокированном iPhone

1. На экране ввода код-пароля коснитесь «SOS».
2. Наберите нужный экстренный номер (например, 112) и коснитесь кнопки.

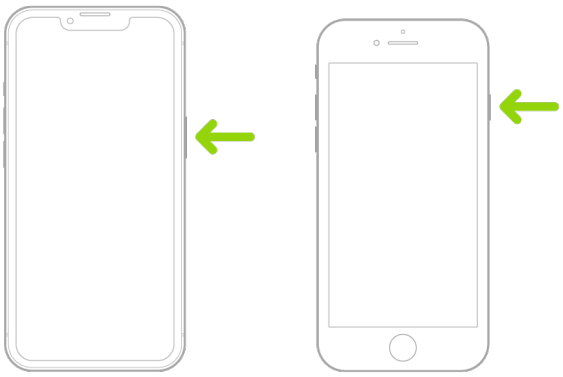
### Использование функции «Экстренный вызов — SOS» на iPhone (во всех странах и регионах, кроме Индии)

В экстренной ситуации с iPhone можно быстро и легко вызвать помощь и оповестить Ваши контакты на случай ЧП (если доступна сотовая связь). После завершения экстренного вызова iPhone отправит Вашим контактам на случай ЧП текстовое сообщение, если Вы не выберете отмену. iPhone отправляет Вашу текущую геопозицию (если она доступна). Кроме того, в течение некоторого времени после перехода в режим SOS Ваши контакты на случай ЧП будут получать уведомления об изменении Вашей геопозиции.

*Примечание.* На iPhone 14 или новее (любой модели) у Вас может быть возможность вызвать экстренные службы по спутниковой связи, если сотовая связь недоступна. См. раздел Использование функции «Экстренный вызов — SOS по спутниковой связи» на iPhone далее в этом руководстве.

- Одновременно нажмите боковую кнопку и любую из кнопок громкости и удерживайте их, пока не появятся бегунки и не закончится обратный отсчет функции «Экстренный вызов — SOS», а затем отпустите кнопки.

  На iPhone также можно настроить вызов функции «Экстренный вызов — SOS» быстрым пятикратным нажатием боковой кнопки. Откройте «Настройки» > «Экстренный вызов — SOS», затем включите «Вызов пятью нажатиями».



### Использование функции «Экстренный вызов — SOS» (в Индии)

- Быстро нажмите боковую кнопку три раза, пока не появятся бегунки и не закончится обратный отсчет функции «Экстренный вызов — SOS».
- Если включена быстрая команда Универсального доступа, одновременно нажмите боковую кнопку и любую из кнопок громкости и удерживайте их, пока не появятся бегунки и не закончится обратный отсчет функции «Экстренный вызов — SOS», а затем отпустите кнопки.

По умолчанию iPhone издает предупреждающий сигнал, начинает обратный отсчет, а затем вызывает экстренные службы.

После завершения экстренного вызова iPhone отправит Вашим контактам на случай ЧП текстовое сообщение, если Вы не выберете отмену. iPhone отправляет Вашу текущую геопозицию (если она доступна). Кроме того, в течение некоторого времени после перехода в режим SOS Ваши контакты на случай ЧП будут получать уведомления об изменении Вашей геопозиции.

### Вызов экстренных служб с Apple Watch

Выполните одно из описанных ниже действий.

- Нажмите боковую кнопку и удерживайте ее, пока не появятся бегунки, а затем перетяните бегунок «Экстренный вызов» влево.

  Часы Apple Watch совершат вызов на номер экстренных служб в Вашем регионе, например 911. (В некоторых регионах для завершения вызова может потребоваться нажать одну из кнопок на цифровой клавиатуре.)

- Нажмите боковую кнопку и удерживайте ее, пока часы Apple Watch не воспроизведут звук предупреждения и не начнут обратный отсчет. Когда обратный отсчет завершится, часы Apple Watch вызовут экстренные службы. Часы Apple Watch воспроизводят звук предупреждения даже в бесшумном режиме. Поэтому, если Вы не хотите шуметь, для вызова экстренных служб используйте бегунок «Экстренный вызов» без обратного отсчета.

  Чтобы часы Apple Watch не начинали обратный отсчет экстренного вызова автоматически при нажатии и удерживании боковой кнопки, выключите «Автоматический набор». Откройте приложение «Настройки» на Apple Watch, коснитесь «SOS», коснитесь «Удерживание боковой кнопки» и выключите «Удерживание боковой кнопки». (Либо откройте приложение Apple Watch на iPhone, коснитесь «Мои часы», коснитесь «Экстренный вызов — SOS» и выключите «Удерживание боковой кнопки для вызова».) Вы по-прежнему сможете совершить экстренный вызов с помощью бегунка «Экстренный вызов».

- Скажите: «Привет, Siri, позвони 911».

### Отправка текстового сообщения в экстренные службы с iPhone (доступно не во всех регионах)

1. Откройте приложение «Сообщения», затем в поле «Кому» введите 911 или местный номер экстренных служб.
2. В поле «Сообщение» введите свое экстренное сообщение.
3. Коснитесь кнопки .

   **Важно!** После ввода номера 911 iPhone переходит в режим экстренных вызовов на 30 минут. Для выхода из режима экстренных вызовов перезагрузите iPhone.

### Отправка текстового сообщения в экстренные службы с Apple Watch (доступно не во всех регионах)

1. Откройте приложение «Сообщения» и коснитесь «Новое сообщение».
2. Коснитесь «Добавить контакт».
3. Коснитесь , введите 911 и коснитесь «OK».
4. Коснитесь «Создать сообщение» и выберите SMS.
5. Напишите сообщение пальцем, коснитесь для диктовки или введите сообщение с клавиатуры.
6. Коснитесь «Готово», затем коснитесь «Отправить».

   **Важно!** После ввода номера 911 часы Apple Watch переходят в режим экстренных вызовов на 30 минут. Для выхода из режима экстренных вызовов перезагрузите Apple Watch.

### Использование функции «Экстренный вызов — SOS по спутниковой связи» на iPhone

На iPhone 14 и новее (любой модели) с iOS 16.1 или новее можно использовать функцию «Экстренный вызов — SOS по спутниковой связи» для отправки текстового сообщения в экстренные службы, если Вы находитесь вне зоны действия сотовой сети и сети Wi-Fi. Подробнее см. в статье службы поддержки Apple Использование функции «Экстренный вызов — SOS по спутниковой связи» на iPhone 14 (https://support.apple.com/HT213426).

Кроме того, Вы можете использовать приложение «Локатор», чтобы делиться с другими пользователями своей геопозицией через спутниковые системы. Обратитесь к разделу Отправка геопозиции по спутниковой связи в приложении «Локатор» на iPhone в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph2aac8ae20).

Подробнее см. в разделе Важная информация об экстренных вызовах на iPhone в Руководстве пользователя iPhone.

# Управление отправкой данных об активности на Apple Watch

Если у Вас есть часы Apple Watch и Вы ранее делились кольцами Активности с кем-либо, то те, с кем Вы делились, могут просматривать информацию о Вашем уровне активности и тренировках. Но они не получают данные о том, где Вы находитесь.


### Прекращение отправки данных на Apple Watch

Вы можете скрыть свой прогресс или полностью прекратить делиться данными о своей активности с другим человеком. Для этого перейдите на вкладку «Поделиться» в приложении «Активность».

Прекращение отправки данных о кольцах активности определенному человеку с помощью Apple Watch.

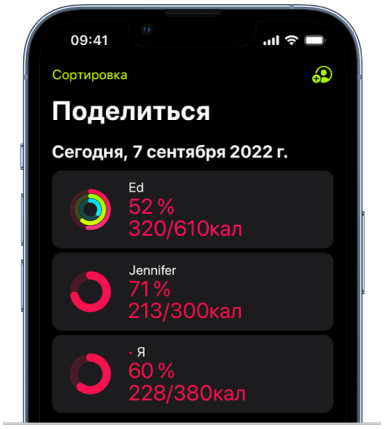
1. Откройте приложение «Активность» на часах Apple Watch.
2. Смахните влево, затем поверните колесико Digital Crown, чтобы перейти к нижней части экрана.
3. Чтобы удалить того, с кем Вы делитесь, коснитесь имени этого человека, затем коснитесь «Удалить».

Подробнее об этом можно узнать в источниках ниже.

- Обмен данными об активности на Apple Watch в Руководстве пользователя Apple Watch (https://support.apple.com/guide/watch/apd68a69f5c7)

### Прекращение отправки данных на iPhone

Прекращение отправки данных о кольцах активности определенному человеку с помощью iPhone.




1. На iPhone откройте приложение «Фитнес» , затем коснитесь «Поделиться».
2. Коснитесь имени человека, с которым Вы делитесь данными.
3. В правом верхнем углу экрана коснитесь кнопки «Поделиться».
4. Коснитесь «Удалить друга» или «Скрыть мою активность».

Подробнее об этом можно узнать в источниках ниже.

- Обмен данными об активности на Apple Watch в Руководстве пользователя Apple Watch (https://support.apple.com/guide/watch/apd68a69f5c7)

# Безопасность AirDrop

## Что такое AirDrop?

AirDrop — это простой способ передавать изображения, документы или другие файлы между устройствами Apple, которые находятся рядом друг с другом. Вы можете разрешить своему устройству передавать данные любым пользователям рядом с Вами, разрешить передачу данных только Вашим контактам или полностью запретить передачу данных.

*Примечание.* Параметр «Только для контактов» доступен на устройствах с iOS 10, iPadOS 13.1 и macOS 10.12 или новее. Если на устройстве установлена более ранняя версия ПО и Вы хотите установить ограничения для отправителей файлов через AirDrop, Вы можете включить этот параметр, когда потребуется, а затем выключить его за ненадобностью.

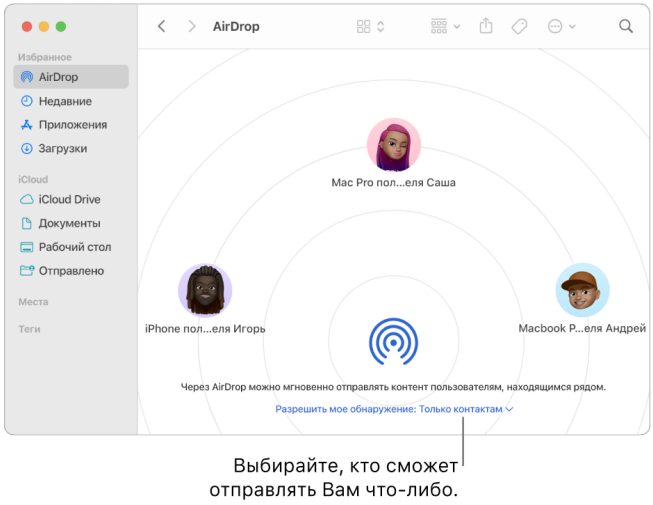
### iPhone или iPad

- На iPhone или iPad откройте «Настройки» > «Основные», коснитесь «AirDrop» и выберите нужный вариант.

  Подробнее об этом можно узнать в источниках ниже.

  - Использование AirDrop на iPhone для отправки объектов на находящиеся рядом устройства в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iphcd8b9f0af)
  - Отправка объектов с iPad на находящиеся рядом устройства через AirDrop в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipadf0a1530e)

### На Mac с помощью Finder

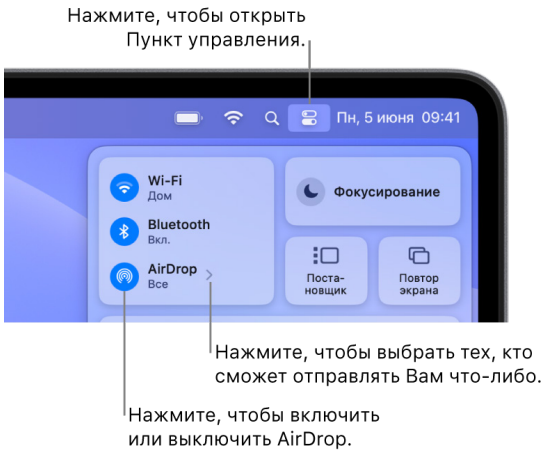



1. Нажмите значок Finder в Dock, чтобы открыть окно Finder.
2. В боковом меню Finder нажмите «AirDrop».
3. В окне AirDrop нажмите всплывающее меню «Разрешить мое обнаружение», затем выберите нужный параметр.

   Подробнее об этом можно узнать в источниках ниже.

   - Использование AirDrop для отправки объектов на устройства Apple, находящиеся рядом в Руководстве пользователя Mac (https://support.apple.com/guide/mac-help/mh35868)

### На Mac с помощью Пункта управления




1. На Mac нажмите в строке меню, затем нажмите . Когда он синий, он включен.
2. Рядом с пунктом AirDrop нажмите , затем выберите подходящий Вам вариант.

   Подробнее об этом можно узнать в источниках ниже.

   - Использование AirDrop для отправки объектов на устройства Apple, находящиеся рядом в Руководстве пользователя Mac (https://support.apple.com/guide/mac-help/mh35868)

# Управление настройками общего доступа к календарям на устройствах Apple

Если Вы открыли доступ к своему календарю другому пользователю, Вы можете разрешить или запретить ему редактировать календарь либо закрыть ему доступ к календарю.

**ВАЖНО!** Когда Вы удаляете календарь или закрываете общий доступ к нему, другие участники получить уведомления об этих изменениях.


### Управление настройками доступа к календарям на iPhone или iPad

1. На iPhone или iPad коснитесь «Календарь», затем рядом с общим календарем, который хотите отредактировать, коснитесь.
2. Выберите пользователя, затем выполните одно из перечисленных действий.
   - Включите или выключите функцию «Разрешить правку».
   - Коснитесь «Закрыть доступ».

### Удаление календаря на Mac

Некоторые календари нельзя удалить.

- Вы не можете удалить календари, управление которыми передано другим пользователям, но можете скрыть их в главном окне приложения «Календарь». См. раздел Отмена публикации календаря на Mac.
- Если Вам не удается удалить календарь в определенной учетной записи календаря, попробуйте удалить его на сайте поставщика этой учетной записи. Например, для удаления календаря Google перейдите на сайт google.com.
- Если в учетной записи есть только один календарь (помимо календарей других пользователей, предоставивших Вам доступ), Вы не сможете удалить этот календарь.

1. На Mac откройте приложение «Календарь», затем нажмите один из календарей в списке.

   Если слева не отображается список календарей, выберите меню «Вид» > «Показать список календарей».
2. Выберите меню «Правка» > «Удалить».

Подробнее об этом можно узнать в источниках ниже.

- Добавление или удаление календарей на Mac в Руководстве пользователя приложения «Календарь» (https://support.apple.com/guide/calendar/icl1005)

### Отмена подписки на календарь на Mac

Если Вы хотите прекратить подписку на календарь другого пользователя, Вы можете отписаться от этого календаря.

- На Mac откройте приложение «Календарь» 14, при нажатой клавише Control нажмите нужный календарь в списке, затем выберите «Отписаться».

  Если слева не отображается список календарей, выберите меню «Вид» > «Показать список календарей».

  *Примечание.* Отменяя подписку на календарь, Вы также можете сообщить о нем как о спаме. Сообщения о спаме помогают приложению «Календарь» лучше распознавать подписки на спам.

Подробнее об этом можно узнать в источниках ниже.

- Подписка на календари на Mac в Руководстве пользователя приложения «Календарь» (https://support.apple.com/guide/calendar/icl1022)

### Отмена публикации календаря на Mac

Если в Вашем списке календарей есть раздел На моем Mac, Вы можете опубликовать календари из этого раздела на сервере WebDAV, к которому у Вас есть доступ. Другие пользователи могут подписаться на Ваш опубликованный календарь или просматривать его в веб-браузере. В любое время Вы можете отменить публикацию календаря, не удаляя его со своего Mac.

*Примечание.* При отмене публикации календарей они не удаляются с Mac.

1. На Mac откройте приложение «Календарь» 14, затем нажмите один из календарей или группу календарей в списке.

   Если слева не отображается список календарей, выберите меню «Вид» > «Показать список календарей». Рядом с названием опубликованного календаря отображается .

2. Выберите меню «Правка» > «Отменить публикацию».

   После отмены публикации календаря на него не могут подписываться новые пользователи. Ранее подписавшиеся пользователи по-прежнему будут видеть последнюю опубликованную копию, пока не удалят ее.

Подробнее об этом можно узнать в источниках ниже.

- Публикация и отмена публикации календаря на Mac в Руководстве пользователя приложения «Календарь» (https://support.apple.com/guide/calendar/icl1017)

### Закрытие общего доступа к календарю iCloud на Mac

Если Вы настроили iCloud на Mac, в приложении «Календарь» Вы можете управлять своими календарями iCloud с общим доступом. Если Вы открыли общий доступ к своему календарю iCloud или присоединились к календарю iCloud другого пользователя, Вы можете получать электронные письма при каждом обновлении общего календаря. Если Вы не хотите получать эти письма, выключите соответствующую настройку Календаря на сайте iCloud.com.

Получив приглашение присоединиться к общему календарю iCloud, Вы можете принять это приглашение на iPhone, iPad или Mac, на котором выполнен вход в тот же Аккаунт Apple, либо в Календаре iCloud или на сайте iCloud.com.

1. Откройте приложение «Календарь» на Mac.

   Если слева не отображается список календарей, выберите меню «Вид» > «Показать список календарей».

2. Выполните одно из перечисленных ниже действий.

   - *Закрытие доступа к календарю определенным пользователям*. Наведите указатель на название календаря в списке, затем нажмите . Нажмите имя человека, затем нажмите клавишу Delete.
   - *Закрытие доступа к календарю всем пользователям* При нажатой клавише Control нажмите календарь в списке, затем выберите «Закрыть общий доступ».
   - *Отмена подписки на календарь другого пользователя*. При нажатой клавише Control нажмите календарь в списке, затем выберите «Отписаться».

     Отменяя подписку на календарь, Вы также можете сообщить о нем как о спаме. Сообщения о спаме помогают приложению «Календарь» лучше распознавать подписки на спам.

Подробнее об этом можно узнать в источниках ниже.

- Получение информации об обновлениях календарей на сайте iCloud.com в Руководстве пользователя приложения «Календарь» (https://support.apple.com/guide/icloud/mm8074582205)

## Управление настройками Семейного доступа

До пяти членов семьи могут использовать Семейный доступ, чтобы делиться подписками, покупками, фотографиями, фотоальбомами, календарем и другим контентом, не делясь своими Аккаунтами Apple. Если Вы пользуетесь семейным планом хранилища iCloud, файлы и документы каждого участника остаются конфиденциальными, а остальные пользователи видят только объем пространства, используемого каждым участником.

Чтобы проверить, состоите ли Вы в группе Семейного доступа, выберите «Настройки» > [*Ваше имя*] > вкладку «Семейный доступ». Если отображается параметр «Настройка Семейного доступа», то Вы не используете Семейный доступ с этим Аккаунтом Apple. Если отображается значок с Семейным доступом, можно коснуться значка, чтобы просмотреть, кто входит в семейную группу и какие у каждого роли.

Полезные советы.

- Чтобы проверить, состоите ли Вы в группе Семейного доступа, откройте «Настройки» и под своим именем найдите слово «Семья».
- О закрытии Семейного доступа см. в разделах Закрытие Семейного доступа на iPhone или iPad с iOS 17, iPadOS 17 или более ранней версии и Закрытие Семейного доступа на компьютере Mac.
- О том, как покинуть семейную группу, см. в разделах Выход из группы Семейного доступа на iPhone или iPad с iOS 17, iPadOS 17 или более ранней версии и Выход из группы Семейного доступа на компьютере Mac.
- Об удалении участников из семейной группы см. в разделах Удаление участников из семейной группы на iPhone или iPad с iOS 17, iPadOS 17 или более ранней версии и Удаление участников из семейной группы на компьютере Mac.

## Кто может покинуть группу Семейного доступа?

Возможность изменить или покинуть группу Семейного доступа зависит от роли пользователя.

- Организатор может выйти из группы Семейного доступа, выключив Семейный доступ. При выключении Семейного доступа все участники семейной группы удаляются из нее. Если в семейной группе есть дети до 13 лет, организатор должен сначала перевести их в другую семейную группу. Члены семьи больше не смогут совместно пользоваться подписками, покупками и другими сервисами, которые предоставляет Семейный доступ.
- Любой член семьи старше 13 лет может удалить себя из семейной группы в любое время. Для этого достаточно выбрать свое имя и нажать «Покинуть семью». Либо можно войти в Аккаунт Apple на сайте, а затем в разделе «Семейный доступ» выбрать пункт «Удалить учетную запись».
- Из соображений безопасности ребенок (младше 13 лет) не может удалить себя из семейной группы и не может прекратить делиться такими данными, как экранное время, без код-пароля Экранного времени. Организатор имеет доступ к общему семейному контенту на Вашем устройстве, в том числе к фотоальбомам и общим календарям, и может просматривать отчеты об экранном времени.

## Типы пользователей в группе Семейного доступа

Пользователи в группе Семейного доступа могут иметь разные роли в зависимости от возраста.

*Примечание*. Возраст, в зависимости от которого кого-либо считают взрослым или ребенком, может отличаться в разных странах или регионах.

Чтобы изменять статус в Семейном доступе, полезно знать, какие роли есть в группах Семейного доступа.

- *Организатор.* Взрослый, настроивший группу Семейного доступа. Организатор может приглашать членов семьи, удалять членов семьи и распускать группу.
- *Взрослый.* Член группы Семейного доступа в возрасте 18 лет или старше.
- *Родитель/Опекун.* Взрослый член группы Семейного доступа, который может помочь с родительским контролем детей в группе. Когда организатор добавляет взрослого в группу Семейного доступа, он может назначить его родителем или опекуном.
- *Ребенок или подросток.* Участник группы Семейного доступа в возрасте до 18 лет. Организатор, родитель или опекун может создать Аккаунт Apple для ребенка, который слишком мал, чтобы сделать это самостоятельно.

Один из взрослых членов семьи — *организатор* — выбирает то, чем делится семейная группа, и приглашает в нее до пяти членов семьи. После принятия приглашений Семейный доступ автоматически настраивается на устройствах участников, в том числе настраивается общий календарь и общий фотоальбом. Организатор может добавить любого человека с Аккаунтом Apple в семейную группу и удалить из нее любого участника старше 13 лет.

## Что происходит, когда Вы покидаете группу Семейного доступа?

Если участник был удален из группы Семейного доступа или покинул ее, у этого участника останутся покупки, оплаченные общей кредитной картой, но этот участник сразу же потеряет доступ к тому, чем делятся другие участники семейной группы, то есть произойдут указанные далее изменения.

- Геопозиции устройств членов семьи не отобразятся, когда Вы будете использовать приложение «Локатор» на сайте iCloud.com либо на Mac, iPhone или iPad.
- Контент бывших участников семейной группы не будет отображаться в разделе «Покупки» в iTunes Store, App Store и Apple Books.
- Музыка, фильмы, телешоу, книги и приложения, загруженные ранее, будут недоступны, если их изначально купил другой участник семейной группы. Бывшие участники семейной группы не смогут получать доступ к контенту, загруженному из Вашей коллекции.
- Встроенные покупки станут недоступны, если они сделаны в приложении, приобретенном другим участником семейной группы. Вы можете восстановить доступ к встроенным покупкам, купив приложение.

### Выход из группы Семейного доступа на iPhone или iPad с iOS 18, iPadOS 18 или новее

Если Вы старше 13 лет и входите в группу Семейного доступа.

1. Откройте «Настройки» > «Семья» под [*Ваше имя*].
2. Коснитесь [*Ваше имя*], затем коснитесь «Перестать использовать семейный доступ».

### Выход из группы Семейного доступа на iPhone или iPad с iOS 17, iPadOS 17 или более ранней версии

Если Вы старше 13 лет и входите в группу Семейного доступа.

1. Откройте «Настройки» > [*Ваше имя*] > «Семейный доступ».
2. Коснитесь [*Ваше имя*], затем коснитесь «Перестать использовать семейный доступ».

### Выход из группы Семейного доступа на компьютере Mac

Если Вы старше 13 лет и входите в группу Семейного доступа.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 15 или новее. Выберите меню Apple > «Системные настройки», затем нажмите «Семья» под [*Ваше имя*].
   - На Mac с macOS 13 или macOS 14. Выберите меню Apple > «Системные настройки» > «Семейный доступ», затем в боковом меню выберите «Семейный доступ».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Семейный доступ», затем выберите «Семейный доступ».
2. В списке участников семейной группы нажмите свое имя или кнопку «Подробнее» рядом со своим именем, нажмите «Закрыть семейный доступ», затем следуйте инструкциям на экране.
3. Нажмите «Готово».

### Закрытие Семейного доступа на iPhone или iPad с iOS 18, iPadOS 18 или новее

Только организатор семейной группы может выключить функцию «Семейный доступ».

1. Откройте «Настройки» > «Семья» под [*Ваше имя*].
2. Коснитесь своего имени, затем коснитесь «Прекратить семейный доступ».

### Закрытие Семейного доступа на iPhone или iPad с iOS 17, iPadOS 17 или более ранней версии

Только организатор семейной группы может выключить функцию «Семейный доступ».

1. Откройте «Настройки» > [*Ваше имя*] > «Семейный доступ».
2. Коснитесь своего имени, затем коснитесь «Прекратить семейный доступ».

### Закрытие Семейного доступа на компьютере Mac

Для закрытия Семейного доступа требуется выполнение указанных ниже условий.

- Вы должны быть организатором семейной группы.
- Детская учетная запись должна быть перемещена в другую семейную группу.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 15 или новее. Выберите меню Apple  > «Системные настройки», затем нажмите «Семья» под [*Ваше имя*].
   - На Mac с macOS 13 или macOS 14. Выберите меню Apple  > «Системные настройки» > «Семейный доступ» , затем в боковом меню выберите «Семейный доступ».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки» > «Семейный доступ» , затем выберите «Семейный доступ».
2. Рядом со своим именем нажмите >, затем нажмите «Закрыть семейный доступ».

### Удаление участников из семейной группы на iPhone или iPad с iOS 18, iPadOS 18 или новее

Если Вы организатор.

1. Откройте «Настройки»  > «Семья» под [*Ваше имя*].
2. Коснитесь [*имя участника*], коснитесь «Удалить пользователя [*имя участника*] из семьи», затем снова коснитесь «Удалить пользователя [*имя участника*]».

*Примечание.* Если Вы организатор, Вы не сможете удалить себя из группы Семейного доступа.

### Удаление участников из семейной группы на iPhone или iPad с iOS 17, iPadOS 17 или более ранней версии

Если Вы организатор.

1. Откройте «Настройки»  > [*Ваше имя*] > «Семейный доступ».
2. Коснитесь [*имя участника*], затем коснитесь «Удалить [*имя участника*] из семьи».

*Примечание.* Если Вы организатор, Вы не сможете удалить себя из группы Семейного доступа.

### Удаление участников из семейной группы на компьютере Mac

Если Вы организатор, Вы можете удалять других участников из семейной группы, но Вы не сможете удалить себя из группы.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 15 или новее. Выберите меню Apple  > «Системные настройки», затем нажмите «Семья» под [*Ваше имя*].
   - На Mac с macOS 13 или macOS 14. Выберите меню Apple  > «Системные настройки» > «Семейный доступ» , затем в боковом меню выберите «Семейный доступ».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple  > «Системные настройки» > «Семейный доступ» , затем выберите «Семейный доступ».
2. Выполните одно из описанных ниже действий.
   - На Mac с macOS 15 или новее. Выберите участника в списке, нажмите «Удалить пользователя [*имя участника*] из семьи», затем снова нажмите «Удалить пользователя [*имя участника*]».
   - На Mac с macOS 14 или более ранней версии. Выберите участника в списке, нажмите —, затем подтвердите удаление участника.

## Безопасное хранение данных в iCloud

iCloud безопасно хранит Ваши фото, видео, документы, музыку, приложения, резервные копии и другие данные и синхронизирует их на всех Ваших устройствах. Через iCloud также можно делиться фото, календарями, геопозициями и другими данными с друзьями и близкими. Для входа в iCloud на устройстве или в интернете можно использовать Аккаунт Apple.

Подробную информацию о том, что хранится в iCloud, см. в Руководстве пользователя iCloud (https://support.apple.com/guide/icloud/).


### Функции безопасности iCloud

Apple предлагает два варианта шифрования и защиты данных, хранящихся в iCloud.

- *Стандартная защита данных (параметр по умолчанию).* Ваши данные в iCloud защищены, ключи шифрования хранятся в дата-центрах Apple, и Apple может помочь Вам с восстановлением данных и учетной записи. Только 14 определенных категорий данных iCloud, включая данные Здоровья и пароли в Связке ключей iCloud, защищаются сквозным шифрованием.
- *Расширенная защита данных в iCloud.* Дополнительный параметр, обеспечивающий высший уровень защиты облачных данных компанией Apple. Включение функции «Расширенная защита данных» предоставляет Вашим доверенным устройствам уникальный доступ к ключам шифрования для большинства данных iCloud, чтобы защитить их сквозным шифрованием. С использованием функции «Расширенная защита данных» количество категорий данных, использующих сквозное шифрование, повышается до 23 — в их числе функция «Резервное копирование iCloud», приложения «Фото», «Заметки» и многое другое.

Подробнее см. в статье службы поддержки Apple Как включить расширенную защиту данных в iCloud (https://support.apple.com/108756) и в таблице «Категории данных и шифрование» в статье Обзор системы защиты данных в iCloud (https://support.apple.com/102651).

### Просмотр и изменение настроек iCloud

Вы можете просмотреть настройки iCloud на каждом устройстве и изменить их, в том числе указав, какие приложения (компании Apple и других разработчиков) могут использовать iCloud, резервные копии iCloud и многое другое.

- *На iPhone или iPad.* Откройте «Настройки» > > [*Ваше имя*] > «iCloud».

  После выключения этой функции Вы не сможете ею воспользоваться, если потерянное или украденное устройство выключено.

- На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Аккаунт Apple» , затем нажмите «iCloud».
- На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Аккаунт Apple» , затем нажмите «iCloud».

### Выход из iCloud

Кроме того, можно полностью выйти из iCloud на устройстве. Если выйти из iCloud, информация с устройства перестанет передаваться в резервную копию.

- *На iPhone или iPad.* Откройте «Настройки» > [*Ваше имя*], прокрутите вниз, затем коснитесь «Выйти».
- На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Аккаунт Apple» , нажмите «Обзор», затем нажмите «Выйти».
- На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Аккаунт Apple» , нажмите «Обзор», затем нажмите «Выйти».

# Управление настройками безопасности в приложении «Сообщения»

В приложении «Сообщения» можно отправлять текстовые сообщения двумя разными способами.

- По сети Wi-Fi или сотовой сети можно отправлять сообщения iMessage другим пользователям iMessage на iPhone, iPad или Mac. Текстовые сообщения iMessage отображаются в синих облачках.
- Можно отправлять сообщения SMS/MMS, переадресованные с iPhone на другие устройства. Сообщения SMS/MMS отображаются в зеленых облачках.

Через iMessage можно отправлять сообщения, фото и видео на другой iPhone, iPad или Mac по сети Wi-Fi или сотовой сети. Эти сообщения всегда зашифрованы и отображаются на iPhone, iPad и Mac в синих облачках.


### Ограничение использования приложения «Сообщения» одним устройством

Если Вы хотите ограничить использование приложения «Сообщения» одним устройством, Вам потребуется выйти из учетной записи Сообщений на устройствах, на которых Вы больше не хотите получать сообщения, и выключить параметр «Сообщения» в iCloud.

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Откройте «Настройки» > «Сообщения», затем включите или выключите iMessage.
   - *На Mac.* В приложении «Сообщения» выберите «Сообщения» > «Настройки», нажмите «iMessage», затем нажмите «Выйти». Подтвердите действие, затем снова нажмите «Выйти».

### Выключение Сообщений в iCloud с iPhone или iPad

При использовании Сообщений в iCloud все сообщения, которые Вы отправляете, получаете и удаляете, обновляются на всех Ваших устройствах Apple автоматически.

1. *На iPhone или iPad.* Откройте «Настройки» > [*Ваше имя*], затем коснитесь «iCloud».
2. В разделе «Приложения, использующие iCloud» выберите «Все».
3. Коснитесь «Сообщения» и выключите параметр «Синхронизация этого [*iPhone*][*iPad*]».
4. Повторите эти действия на всех устройствах, чтобы удалить сообщения из iCloud.

### Выключение приложения «Сообщения» в iCloud с компьютера Mac

При использовании Сообщений в iCloud все сообщения, которые Вы отправляете, получаете и удаляете, обновляются на всех Ваших устройствах Apple автоматически.

1. В приложении «Сообщения» на Mac выберите «Сообщения» > «Настройки», затем нажмите «iMessage».
2. Нажмите «Настройки» и снимите флажок «Включить Сообщения в iCloud».
3. Выберите один из указанных ниже вариантов.
   - *Выключить на всех устройствах.* Выключение Сообщений в iCloud на всех Ваших устройствах. Сообщения больше не хранятся в iCloud; для их хранения используется только память каждого устройства.
   - *Выключить на этом устройстве.* Выключение Сообщений в iCloud только на Вашем Mac. Сообщения на Вашем Mac больше не хранятся в iCloud; для хранения сообщений на всех устройствах со включенной функцией «Сообщения в iCloud» продолжает использоваться хранилище iCloud.

### Включение и выключение iMessage

iMessage защищает Ваши сообщения на всех Ваших устройствах с помощью сквозного шифрования, поэтому никто, включая Apple, не сможет получить к ним доступ без Вашего код-пароля. Поскольку разговоры в iMessage происходят через Wi-Fi и сотовые сети, в детализации счета телефонного оператора не будет информации о том, с кем Вы переписываетесь. Можно создавать резервные копии сообщений iMessage, так что, если Ваше устройство будет потеряно или украдено, Вы все равно сможете восстановить важную переписку.

**Важно!** Чтобы сообщения сохранялись в iCloud, необходимо включить резервное копирование. Если это не было сделано, сообщения не будут восстановлены. См. раздел Настройка iCloud для приложения «Сообщения» на всех устройствах в Руководстве пользователя iCloud (https://support.apple.com/guide/icloud/mm0de0d4528d).

### Когда служба iMessage включена

Если сотовая сеть недоступна, можно отправлять iMessage по Wi-Fi. Функция «Недавно удаленные» сохраняет удаленные сообщения на срок до 30 дней, поэтому, если Вы полагаете, что кто-то мог удалить сообщения с Вашего устройства, проверьте их на этой вкладке.

### Когда служба iMessage выключена

Когда служба iMessage выключена, становятся недоступны такие функции, как редактирование сообщений, отмена отправки сообщений и отчеты о прочтении. Для отправки сообщений используются SMS/MMS.

**Важно!** При использовании SMS/MMS информация об этих сообщениях может отображаться в детализации счета телефонного оператора, и через оператора сотовой связи эта информация может стать доступна владельцу этого номера телефона.

- *На iPhone или iPad.* Откройте «Настройки» > «Сообщения», затем включите или выключите iMessage.
- На Mac с macOS 13 или новее. Откройте приложение «Сообщения», выберите меню «Сообщения» > «Настройки», нажмите «iMessage», затем нажмите «Выйти». Подтвердите действие, затем снова нажмите «Выйти».
- На Mac с macOS 12 или более ранней версии. Откройте приложение «Сообщения», выберите меню «Сообщения» > «Настройки», нажмите «iMessage», затем нажмите «Выйти». Подтвердите действие, затем снова нажмите «Выйти».

### Включение и выключение отчетов о прочтении

Благодаря отчетам о прочтении пользователи iMessage могут узнать, что их сообщения были прочитаны. Если отчеты о прочтении включены, то, после того как Вы прочитаете сообщение iMessage, его отправитель увидит индикатор «Прочитано» под сообщением на своем устройстве. Если отчеты о прочтении выключены, отправитель увидит только, что сообщение доставлено.

Вы можете включить отправку отчетов о прочтении для всех разговоров или только для отдельных разговоров. Если Вы включили отправку отчетов о прочтении для всех разговоров, Вы все равно можете выключить их для отдельных разговоров — и наоборот.

*Примечание.* Отчеты о прочтении не поддерживаются для SMS и групповых переписок.

- *На iPhone или iPad.* Откройте «Настройки» > «Сообщения», затем включите или выключите «Отчеты о прочтении».
- На Mac с macOS 13 или новее. Откройте приложение «Сообщения», выберите меню «Сообщения» > «Настройки», нажмите вкладку «iMessage», затем установите или снимите флажок «Отчет о прочтении».
- На Mac с macOS 12 или более ранней версии. Откройте приложение «Сообщения», выберите меню «Сообщения» > «Настройки», нажмите вкладку «iMessage», затем установите или снимите флажок «Отчет о прочтении».

### Редактирование отправленного сообщения

В iOS 16, iPadOS 16.1 и macOS 13 или новее можно редактировать недавно отправленное сообщение до пяти раз в течение 15 минут после его отправки. Это позволяет исправить опечатку. Получатели видят, что сообщение было отредактировано, и могут просмотреть историю изменений.

*Примечание.* Сообщения SMS редактировать нельзя.

Если получатели используют устройства Apple с более ранними версиями iOS, iPadOS или macOS, они получают последующие сообщения с текстом «Внесены правки в» и Вашим новым сообщением в кавычках.

- *На iPhone или iPad.* Коснитесь «Сообщения», коснитесь облачка сообщения и удерживайте его, коснитесь «Изменить», затем отредактируйте сообщение и отправьте его еще раз.
- На Mac с macOS 13. Откройте приложение «Сообщения», нажмите облачко сообщения при нажатой клавише Control, выберите «Изменить», затем отредактируйте сообщение и отправьте его еще раз.

**Отмена отправки сообщения**

В iOS 16, iPadOS 16.1 и macOS 13 или новее можно отменить отправку сообщения в течение 2 минут после его отправки. Это позволяет отозвать сообщение, которое было случайно отправлено не тому человеку. Получатели видят, что отправка сообщения была отменена.

*Примечание.* Отправку сообщений SMS отменить нельзя.

- *На iPhone или iPad.* Коснитесь «Сообщения», коснитесь облачка сообщения и удерживайте его, затем коснитесь «Отменить отправку».

  У Вас и у получателя в разговоре отображается сообщение о том, что Вы отменили отправку сообщения.
- На Mac с macOS 13 или новее. Откройте приложение «Сообщения», нажмите облачко сообщения при нажатой клавише Control, затем выберите «Отменить отправку».

  У Вас и у получателя в разговоре отображается сообщение о том, что Вы отменили отправку сообщения.

## Борьба с мошенническими запросами данных

Будьте бдительны, если Вам присылают сообщения о неожиданных подарках, а также просьбы загрузить документы, установить программное обеспечение или перейти по подозрительным ссылкам. Те, кто хочет получить доступ к Вашей персональной информации, прибегнут к любым средствам: поддельным письмам и сообщениям, вводящим в заблуждение всплывающим окнам с объявлениями, поддельным загрузкам, спаму в календаре и даже мошенническим телефонным звонкам. Все эти действия направлены на то, чтобы заставить Вас поделиться своими данными, например Аккаунтом Apple или паролем, или чтобы Вы сообщили код проверки для двухфакторной аутентификации.

Советы о том, как избежать обмана и не скомпрометировать свои учетные записи и личную информацию, см. в статье службы поддержки Apple Распознавайте фишинговые сообщения, ложные звонки из службы поддержки и другие виды мошенничества и не поддавайтесь на них (https://support.apple.com/102568).

*Примечание.* Фишинг — это попытки мошенников получить от Вас персональную информацию.

## Блокировка вызовов и сообщений от определенных абонентов

Если Вы получаете нежелательные сообщения, электронные письма или вызовы, в том числе по FaceTime, то Вы можете заблокировать тех, кто беспокоит Вас, чтобы они не могли связаться с Вами в дальнейшем. Тот, кого Вы заблокировали на одном устройстве, будет заблокирован на всех устройствах Apple, на которых выполнен вход с тем же Аккаунтом Apple.

**ВАЖНО!** Заблокированный пользователь не получит уведомление о блокировке, а Вы по-прежнему сможете вызывать его и отправлять ему сообщения и электронные письма, не разблокируя его. Однако, если Вы делились геопозицией с этим человеком, он *получит* уведомление о том, что Вы прекратили делиться своей геопозицией после блокировки.

Контакт, заблокированный в приложении «Телефон», FaceTime, «Сообщения» или «Почта», блокируется во всех четырех приложениях.


### Блокировка голосовых вызовов, вызовов FaceTime, сообщений и электронных писем от определенных людей

- *В приложении «Телефон» на iPhone.* В приложении «Телефон» коснитесь вкладки «Избранные», «Недавние» или «Автоответчик», коснитесь ⓘ рядом с именем, телефонным номером или адресом электронной почты контакта, который нужно заблокировать, прокрутите вниз, коснитесь «Заблокировать абонента», затем коснитесь «Заблокировать контакт».
- *В приложении FaceTime на iPhone или iPad.* В истории вызовов FaceTime коснитесь ⓘ рядом с именем, телефонным номером или адресом электронной почты контакта, который нужно заблокировать, прокрутите вниз, коснитесь «Заблокировать абонента», затем коснитесь «Заблокировать контакт».
- *В приложении FaceTime на Mac.* В истории вызовов FaceTime, удерживая клавишу Control, нажмите имя, телефонный номер или адрес электронной почты контакта, который нужно заблокировать, затем выберите «Заблокировать абонента».
- *В приложении «Сообщения» на iPhone или iPad.* В приложении «Сообщения» коснитесь разговора, коснитесь имени или номера вверху разговора, коснитесь ⓘ, прокрутите вниз, затем коснитесь «Заблокировать абонента».

- *В приложении «Сообщения» на Mac.* В истории приложения «Сообщения» выберите имя, телефонный номер или адрес электронной почты контакта, который хотите заблокировать. В меню «Разговоры» выберите «Заблокировать пользователя», затем нажмите «Заблокировать».
- *В приложении «Почта» на iPhone или iPad.* В приложении «Почта» ✉️ выберите электронное письмо от нежелательного отправителя, коснитесь имени отправителя вверху письма, выберите «Заблокировать контакт», затем коснитесь «Заблокировать контакт».
- *В приложении «Почта» на Mac.* Откройте приложение «Почта», выберите электронное письмо от нежелательного отправителя, нажмите имя отправителя вверху письма, затем в раскрывающемся меню выберите «Заблокировать контакт».

  Возле имени отправителя в списке сообщений появляется значок блокировки 🚫, а к их сообщениям добавляется баннер, сообщающий о блокировке. Баннер также является ссылкой на панель блокировки в настройках Почты, где можно редактировать список заблокированных отправителей.

*Примечание.* Если отправитель был ранее отмечен в почте как VIP, сначала коснитесь «Удалить из VIP», прежде чем блокировать этого отправителя.

### Управление заблокированными контактами

Вы можете управлять заблокированными контактами, изменяя параметры в любом из четырех приложений, которые допускают блокировку. К этим приложениям относятся «Телефон», FaceTime, «Сообщения» и «Почта». Разблокировка в одном приложении приводит к разблокировке во всех остальных. Выполните одно из перечисленных действий, чтобы просмотреть список заблокированных номеров.

- *На iPhone.* Откройте «Настройки» ⚙️ > «Телефон», затем коснитесь «Заблокированные контакты».
- *В приложении FaceTime на iPhone или iPad.* Откройте «Настройки» ⚙️ > «FaceTime», затем в разделе «Вызовы» коснитесь «Заблокированные контакты».
- *В приложении FaceTime на Mac.* Откройте FaceTime, перейдите в меню «FaceTime» > «Настройки», затем нажмите «Заблокированные».
- *В приложении «Сообщения» на iPhone или iPad.* Откройте «Настройки» ⚙️ > «Сообщения», затем в разделе «SMS/MMS» коснитесь «Заблокированные контакты».
- *В приложении «Сообщения» на Mac.* Откройте Сообщения, перейдите в меню «Сообщения» > «Настройки», нажмите «iMessage», затем нажмите «Заблокированные».
- *В приложении «Почта» на iPhone или iPad.* Откройте «Настройки» > «Почта», затем в разделе «Обработка тем» коснитесь «Заблокировано».
- *В приложении «Почта» на Mac.* Откройте Почту, перейдите в меню «Почта» ⚙️ > «Настройки», нажмите «Спам», затем нажмите «Заблокированные».

# Безопасность NameDrop

## Что такое NameDrop?

Сервис NameDrop, входящий в состав AirDrop, позволяет пользователям iPhone и Apple Watch легко делиться своими контактными данными, просто поднося устройства друг к другу. Вы можете выбрать конкретные контактные данные, которыми хотите делиться, и данные, которые не будут отправляться.

NameDrop работает автоматически. О том, как выключить NameDrop, см в разделе Выключение NameDrop далее в этом руководстве.

*Примечание.* NameDrop работает между устройствами iPhone, Apple Watch SE (2-го поколения), Apple Watch Series 7 либо Apple Watch Ultra или новее с iOS 17.1, iPadOS 17.1 либо watchOS 10.1 или новее.

### Просмотр и обновление Вашей карточки контакта

Вы можете обновить информацию, которой Вы делитесь через NameDrop, обновив свою карточку контакта, — например, если Вы хотите делиться только своим именем или инициалами.

*Примечание.* Через NameDrop отправляются только выбранные Вами имя, номер телефона или адрес электронной почты, а также информация из постера контакта, связанного с Вашей карточкой контакта. Через NameDrop не отправляется другая информация из Вашей карточки контакта, например Ваш домашний адрес или дата рождения. Когда Вы делитесь своими контактными данными через приложение «Контакты» или NameDrop, по умолчанию Ваши личные местоимения не отправляются. Когда Вы делитесь контактными данными другого человека, личные местоимения этого человека не отправляются никогда.

1. Откройте приложение «Контакты» .
2. Коснитесь «Моя карточка» > «Изменить».
3. Просмотрите и обновите свое имя, номера телефонов и адреса электронной почты, которыми Вы хотите делиться через NameDrop.

   Подробнее об этом можно узнать в источниках ниже.

   - Добавление или редактирование Вашей контактной информации и фотографии на iPhone в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph18b749db1)
   - Добавление или редактирование Вашей контактной информации и фотографии на iPad в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipadfcfa2d42)

### Отправка Вашей контактной информации

Вы можете поделиться своими контактными данными с другим человеком.

1. Выполните одно из описанных ниже действий.
   - *Отправка с iPhone или iPad.* Поднесите свой iPhone на расстояние в несколько сантиметров к iPhone или Apple Watch другого человека.
   - Отправка с Apple Watch на Apple Watch. Откройте приложение «Контакты» на своих Apple Watch, коснитесь своей картинки в правом верхнем углу, коснитесь «Поделиться», затем поднесите свои часы к Apple Watch другого человека.
   - Дисплеи обоих устройств начнут светиться, и часы Apple Watch завибрируют, указывая, что выполняется соединение.
2. Продолжайте удерживать два устройства рядом, пока на обоих дисплеях не отобразится NameDrop.
3. Выберите один из вариантов: отправить свою карточку контакта (либо определенный номер телефона или адрес электронной почты) и получить карточку другого человека, либо только получить карточку другого человека.

   Если Вы отправляете свою карточку контакта, коснитесь , выберите поля для отправки, затем коснитесь «Сохранить». Эти же поля будут выбраны по умолчанию в следующий раз, когда Вы воспользуетесь NameDrop.

   Чтобы отменить отправку, отдалите два устройства друг от друга или заблокируйте свой iPhone, прежде чем передача данных по NameDrop завершится.

   Подробнее об этом можно узнать в источниках ниже.

   - Использование NameDrop для передачи контактной информации новым пользователям в Руководстве пользователя Apple Watch (https://support.apple.com/guide/watch/apd8ebed6c09#apdd22da5d51)

### Выключение NameDrop

1. Откройте приложение «Настройки» .
2. Коснитесь «Основные» > «AirDrop».
3. Выключите параметр «Сближение устройств».

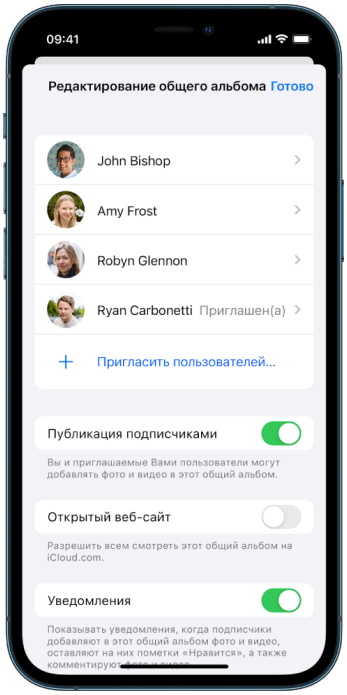
## Управление настройками общего доступа к данным Фото на устройствах Apple

В общих альбомах в приложении «Фото» можно выбирать фото и видео, которыми Вы хотите поделиться, а также тех, с кем Вы хотите ими поделиться. Вы также можете изменить настройки доступа в любое время. Человек, которому закрыт доступ к фото или альбому, теряет доступ к общему альбому и его содержимому.

Если Вы подписаны на общий альбом, Вы можете удалить любые фото, которыми делитесь. Вы также можете выбрать «Отписаться», чтобы отписаться от общего альбома.


Об управлении общим доступом к контенту на Mac см. в разделе Управление настройками «Отправлено Вам» на устройствах Apple далее в этом руководстве.

### Управление настройками доступа к общим альбомам в приложении «Фото» на Mac




1. На iPhone или iPad выберите общий альбом, затем коснитесь кнопки «Пригласить пользователей».
2. Выполните одно из перечисленных ниже действий.
   - *Приглашение новых подписчиков.* Коснитесь «Пригласить пользователей» и введите имена подписчиков, которых Вы хотите добавить.

     Подписчики могут добавлять в альбом фото и видео. Выключите кнопку «Публикация подписчиками», чтобы только Вы могли добавлять фотографии и видео.
   - *Удаление подписчиков.* Коснитесь имени подписчика, затем коснитесь «Удалить подписчика».
   - *Удаление себя из числа участников общего альбома.* Выполните одно из описанных ниже действий.
     - В правом верхнем углу экрана коснитесь многоточия, затем коснитесь «Отписаться».
     - В правом верхнем углу экрана коснитесь значка учетной записи iCloud, затем коснитесь «Отписаться».
   - *Выключение уведомлений.* Проведите пальцем, чтобы выключить параметр «Уведомления».

Подробнее об этом можно узнать в источниках ниже.

- Обмен фото и видео на iPhone в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iphf28f17237)
- Обмен фото и видео на iPad в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipad4f44c78f)

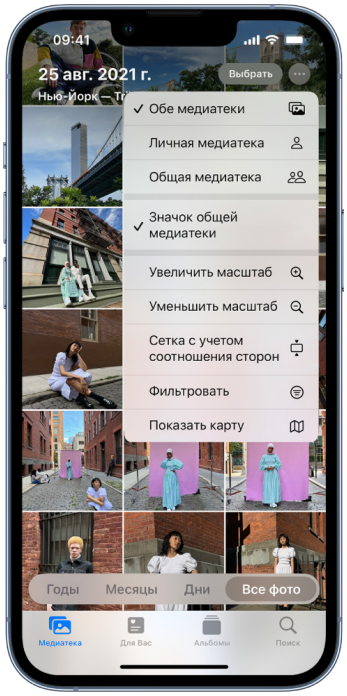
### Управление настройками общей медиатеки iCloud на iPhone или iPad

В общей медиатеке iCloud Вы можете легко делиться фото и видео с другими участниками (до пяти человек). Когда Вы отправляете фото и видео в общую медиатеку iCloud, они перемещаются из Вашей личной медиатеки в общую. Вы можете выбирать контент, к которому хотите предоставить общий доступ в общей медиатеке, или автоматически делиться материалами прямо с камеры. Все участники могут добавлять, редактировать и удалять контент в общей медиатеке, а создатель медиатеки, настроивший ее, предоставляет для нее место в хранилище iCloud.

Участники могут выйти из общей медиатеки в любой момент.

Если Вы являетесь создателем медиатеки, Вы можете в любой момент удалить участников общей медиатеки или саму медиатеку. При удалении участника из общей медиатеки этот пользователь получает уведомление и может скопировать весь контент из общей медиатеки в свою личную. Участники не могут удалять друг друга из общей медиатеки.

*Примечание.* Для использования общих медиатек в приложении «Фото» требуется iOS 16 либо iPadOS 16.1 или новее. Чтобы определить версию программного обеспечения, установленного на устройстве, откройте «Настройки» > «Основные» и коснитесь «Об устройстве».



- Откройте «Настройки» > «Фото» > «Общая медиатека», затем выполните любое из указанных действий.
  - *Удаление участников из общего альбома.* Коснитесь «Удалить участников».
  - *Выход из общей медиатеки* Коснитесь «Выйти из общей медиатеки».

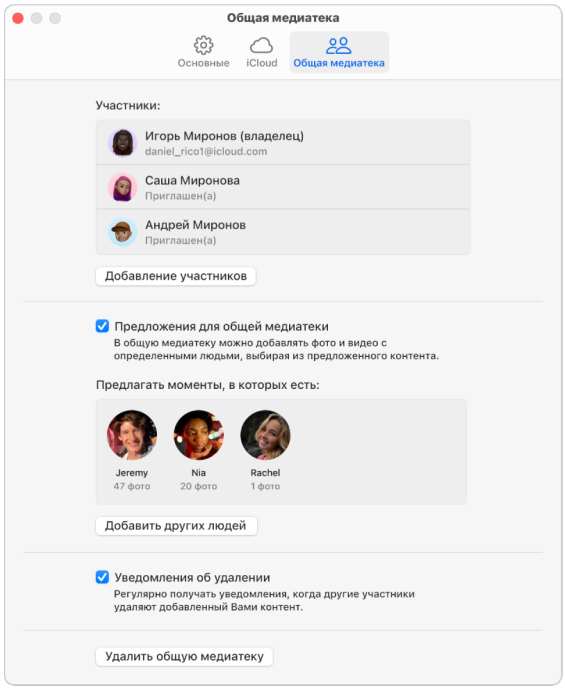
    При выходе из общей медиатеки можно скопировать все медиафайлы из общей медиатеки в личную медиатеку либо только медиафайлы, добавленные Вами.
  - *Удаление общей медиатеки (для этого Вы должны быть ее организатором).* Коснитесь «Удалить общую медиатеку».

    Всем участникам придет уведомление о том, что общая медиатека удалена.

Подробнее об этом можно узнать в источниках ниже.

- Настройка общей медиатеки iCloud или присоединение к ней в приложении «Фото» в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph28ac9ea81)
- Настройка общей медиатеки iCloud или присоединение к ней в приложении «Фото» в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipad94c5ed43)

### Управление настройками доступа к общим альбомам в приложении «Фото» на Mac




1. Откройте приложение «Фото» на Mac, затем нажмите общий альбом в разделе «Общие альбомы» бокового меню.
2. В панели инструментов нажмите .
3. В поле «Пригласить пользователей» выполните одно из описанных ниже действий.
   - *Приглашение новых подписчиков.* Введите адрес электронной почты.

     Если тот, кого Вы приглашаете, не использует iCloud, Вы можете установить флажок «Открытый веб-сайт», чтобы создать URL-адрес для общего альбома. С помощью этого URL-адреса кто угодно может просматривать и загружать содержимое общего альбома.
   - *Удаление подписчиков.* Выберите адрес электронной почты подписчика, затем нажмите «Удалить».
   - *Повторное приглашение подписчика.* Нажмите стрелку вниз рядом с именем подписчика и выберите «Отправить приглашение снова».

Подробнее об этом можно узнать в источниках ниже.

- Что такое общие альбомы в приложении «Фото» на Mac? в Руководстве пользователя приложения «Фото» (https://support.apple.com/guide/photos/pht7a4c765b)
- Подписка на общие альбомы в приложении «Фото» на Mac в Руководстве пользователя приложения «Фото» (https://support.apple.com/guide/photos/pht884a8908)

### Удаление участников из общей медиатеки iCloud на Mac

*Примечание.* Для использования функции общей медиатеки в Фото на Mac требуется macOS 13 или новее. Чтобы определить версию программного обеспечения, установленного на устройстве, в левом верхнем углу экрана в меню Apple  выберите параметр «Об этом Mac».

Пользователи, имеющие доступ к общей медиатеке менее 7 дней, могут сохранить только контент, который загрузили сами.

1. В приложении «Фото»  на Mac выберите «Фото» > «Настройки», затем нажмите «Общая медиатека».
2. Рядом с именем пользователя, которого хотите удалить, нажмите , затем выберите «Удалить».
3. Нажмите «Удалить из общей медиатеки».

Подробнее об этом можно узнать в источниках ниже.

- Что такое общие альбомы в приложении «Фото» на Mac? в Руководстве пользователя приложения «Фото» (https://support.apple.com/guide/photos/pht153ab3a01)

### Выход из общей медиатеки iCloud или ее удаление в приложении «Фото» на Mac

Участники могут выйти из общей медиатеки в любой момент. Если Вы являетесь организатором общей медиатеки, Вы можете удалить ее. При удалении общей медиатеки все участники получают уведомление и при желании могут сохранить все объекты из нее в личной медиатеке.

Если Вы были участником общей медиатеки менее 7 дней, при выходе из нее Вы можете сохранить только те объекты, которые добавили в нее сами.

*Примечание.* Для использования функции общей медиатеки в Фото на Mac требуется macOS 13 или новее. Чтобы определить версию программного обеспечения, установленного на устройстве, в левом верхнем углу экрана в меню Apple  выберите параметр «Об этом Mac».

1. В приложении «Фото»  на Mac выберите «Фото» > «Настройки», затем нажмите «Общая медиатека».
2. Нажмите «Выйти из общей медиатеки» (если Вы являетесь участником) и «Удалить общую медиатеку» (если Вы являетесь ее организатором).
3. Выберите один из перечисленных ниже параметров.
   - *Оставить все.* Добавить все фото из общей медиатеки в личную медиатеку.
   - *Оставить только добавленное мной.* Добавить в личную медиатеку из общей медиатеки только фото, добавленные Вами.
4. Нажмите «Удалить общую медиатеку», затем снова нажмите «Удалить общую медиатеку» для подтверждения действия.

Подробнее об этом можно узнать в источниках ниже.

- Что такое общие альбомы в приложении «Фото» на Mac? в Руководстве пользователя приложения «Фото» (https://support.apple.com/guide/photos/pht153ab3a01)
- Выход из общей медиатеки или ее удаление в Руководстве пользователя приложения «Фото» (https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22)

## Управление общими группами вкладок в Safari

Вы можете создать общую группу вкладок и работать над ней вместе с другими пользователями iCloud. Общей группой вкладок могут пользоваться не более 100 участников. Участники могут добавлять вкладки в группу вкладок и удалять их. Пользователи видят все совершаемые действия в режиме реального времени.

Все участники должны выполнить вход со своим Аккаунтом Apple, а также включить параметр «Safari» в настройках iCloud (https://support.apple.com/guide/iphone/iphde0f868fd) и двухфакторную аутентификацию.


### Управление общими группами вкладок в Safari на iPhone или iPad

Если кнопка «Совместная работа» не отображается, то Вы еще не поделились группами вкладок.

1. Коснитесь «Safari», затем в правом верхнем углу коснитесь .
2. Коснитесь «Управлять общей группой вкладок», затем выполните любое из описанных ниже действий.
   - *Удаление участника.* Коснитесь имени участника, затем коснитесь «Закрыть доступ».
   - *Закрытие доступа для всех участников.* Коснитесь «Закрыть доступ».
   - *Добавление участника.* Коснитесь «Поделиться с другими пользователями», затем пригласите их.

Подробнее об этом можно узнать в источниках ниже.

- Добавление участников в общую группу вкладок и удаление из нее в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659)
- Добавление участников в общую группу вкладок и удаление из нее в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8)

### Управление общими группами вкладок в Safari на Mac

Если кнопка «Совместная работа» не отображается, то Вы еще не поделились группами вкладок.

1. В приложении Safari на Mac нажмите в панели инструментов.
2. Нажмите «Управлять общей группой вкладок», затем выполните любое из описанных ниже действий.
   - *Удаление участника.* Нажмите имя участника, нажмите «Закрыть доступ», затем нажмите «Продолжить».
   - *Закрытие доступа для всех участников.* Нажмите «Закрыть общий доступ», затем нажмите «Продолжить».
   - *Добавление участника.* Нажмите «Поделиться с другими пользователями», затем пригласите их, нажав «Сообщения».

Подробнее об этом можно узнать в источниках ниже.

- Добавление участников в общую группу вкладок и удаление из нее в Руководстве пользователя Safari (https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659)

## Сохранение конфиденциальности истории просмотра в Safari и Картах

Если Вы полагаете, что у кого-то может быть доступ к Вашему устройству, имеет смысл просматривать и очищать историю поиска и кэши в браузерах и других приложениях. Многие приложения хранят информацию о том, что Вы искали и просматривали, чтобы Вы могли легко найти эту информацию в будущем. Например, наличие истории геопозиций, которые Вы искали или к которым прокладывали маршрут в приложении «Карты», может упростить возврат к месту, которое Вы недавно посетили.

Если Вы оказались в небезопасной ситуации и хотите найти советы по дальнейшим действиям в интернете, не сохраняя сведения о просмотренных страницах в Safari, Вы можете открыть новое окно в режиме «Частный доступ» на iPhone, iPad или Mac. В режиме «Частный доступ» данные об интернет-активности не сохраняются и не передаются между Вашими устройствами. Кроме того, если Ваши устройства обновлены до iOS 17, iPadOS 17 или macOS 14, Safari блокирует вкладки в режиме «Частный доступ» после определенного периода неактивности. Для повторного открытия вкладок требуется пароль, код-пароль, Face ID или Touch ID. Это помогает защитить Вашу конфиденциальность, если Вы отошли от устройства. Вы можете очистить историю просмотра и открыть окно в режиме «Частный доступ» на iPhone, iPad или Mac.

О том, как открыть окно в режиме «Частный доступ» на iPhone, iPad или Mac, см. далее в этом руководстве.

### Очистка истории просмотра в Safari

Если Вы искали информацию о стратегиях в области безопасности в интернете и переживаете о том, что кто-то может увидеть Вашу историю просмотра, Вы можете удалить все сохраненные в Safari записи о том, что Вы смотрели.

- *На iPhone или iPad.* Откройте «Настройки» > «Safari» > «Очистить историю и данные».
- *На Mac.* Откройте приложение Safari, выберите «История» > «Очистить историю», нажмите всплывающее меню, затем выберите, за какое время нужно очистить историю.

После очистки истории Safari удалит данные, которые сохранялись, когда Вы посещали веб-страницы. К таким данным относятся:

- История посещения веб-страниц
- Список, в котором представлен обратный и обычный порядок посещения веб-страниц
- Список часто посещаемых сайтов
- Недавние запросы
- Значки веб-страниц
- Снимки экрана, сохраненные на открытых веб-страницах
- Список загруженных объектов (загруженные файлы не удаляются)
- Сайты, добавленные для быстрого поиска веб-сайтов
- Сайты, запросившие доступ к использованию геопозиции
- Сайты, запросившие доступ на отправку Вам уведомлений

### Очистка недавних маршрутов и списка Избранного в приложении «Карты» на iPhone или iPad

1. Откройте приложение «Карты», затем в поле поиска прокрутите вниз до раздела «Недавние».
2. Выполните одно из описанных ниже действий.
   - Смахните недавний маршрут влево.
   - Коснитесь «Еще» над списком, затем смахните недавний маршрут влево; чтобы удалить группу маршрутов, коснитесь «Очистить» над группой.
3. Чтобы удалить избранную геопозицию, прокрутите до раздела «Избранное», затем коснитесь «Еще». Смахните справа налево по избранной геопозиции, которую нужно удалить, либо коснитесь «Изменить», а затем коснитесь, чтобы удалить несколько избранных геопозиций.

### Очистка недавних маршрутов и избранного в приложении «Карты» на Mac

1. Откройте приложение «Карты», затем прокрутите до раздела «Недавние» в боковом меню.
2. В разделе «Недавние» нажмите «Очистить недавние».
3. Чтобы удалить избранную геопозицию, при нажатой клавише Control нажмите геопозицию (в разделе «Избранное» в боковом меню), затем выберите «Удалить из Избранного».

### Открытие окна в режиме «Частный доступ» на iPhone

1. Откройте Safari.
2. Коснитесь .
3. Внизу в центре панели вкладок внизу экрана коснитесь ⌄, затем коснитесь «Частный».

   Вкладка автоматически добавляется в частную группу вкладок. В группе можно открыть несколько частных вкладок.

Узнать, что режим «Частный доступ» включен, очень просто. Если панель поля поиска серая или в ней написано «Частный», то режим включен.

Чтобы скрыть веб-страницы и выйти из режима «Частный доступ», коснитесь кнопки , затем коснитесь кнопки ⌄, чтобы открыть другую группу вкладок из меню в нижней части экрана. Сайты с частным доступом отобразятся снова при переходе в режим «Частный доступ».

Чтобы закрыть частные вкладки, коснитесь , затем смахните влево по каждой вкладке, которую хотите закрыть.

### Открытие окна в режиме «Частный доступ» на iPad

- В Safari коснитесь , затем коснитесь «Частный».

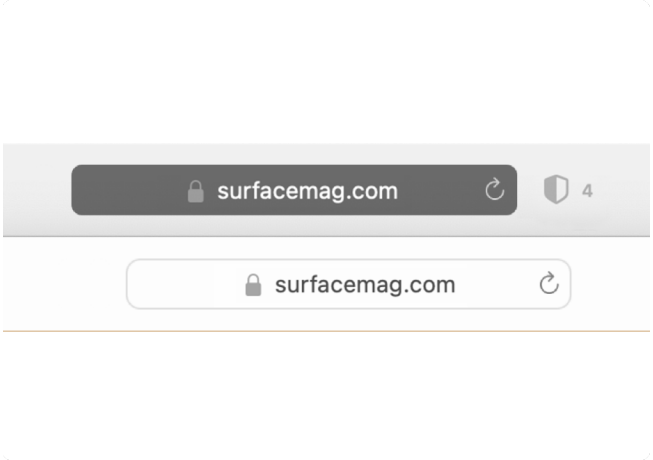
  Если включен режим «Частный доступ», фон поля поиска будет черным, а не белым, и посещаемые сайты не будут добавляться в историю на iPad и отображаться в списке вкладок на других устройствах. Можно открыть несколько частных вкладок в группе частных вкладок.

  Чтобы скрыть сайты и выйти из режима «Частный доступ», коснитесь , затем откройте другую группу вкладок. Вкладки снова отобразятся в следующий раз, когда Вы перейдете в режим «Частный доступ».

### Открытие окна в режиме «Частный доступ» на Mac

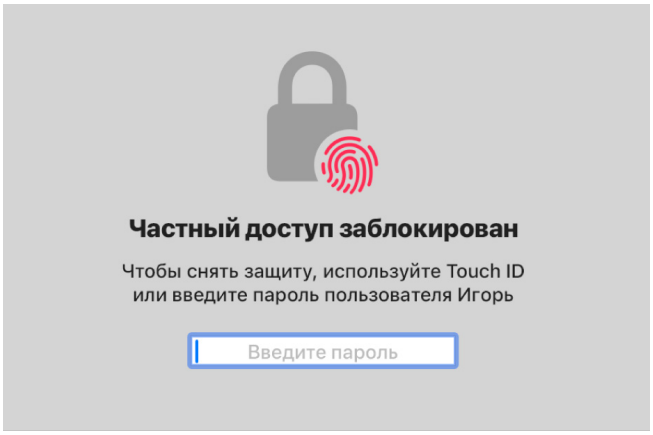
1. В приложении Safari выберите «Файл» > «Новое частное окно» или переключитесь на окно Safari, в котором уже включен режим «Частный доступ».

   В режиме «Частный доступ» поле смарт-поиска в окне становится темным, а текст — белым.




2. Посещайте веб-страницы как обычно.

   *Примечание.* Когда устройство заблокировано или находится в режиме сна, а также в те моменты, когда Вы не пользуетесь Safari, частные окна в Safari блокируются. Когда Вы разблокируете устройство или выводите его из режима сна либо снова начинаете пользоваться Safari, можно разблокировать частное окно с помощью Face ID, Touch ID либо пароля или код-пароля устройства.



### Открытие окон только в режиме «Частный доступ» на Mac

1. В приложении Safari выберите «Safari» > «Настройки», затем нажмите «Основные».
2. Нажмите всплывающее меню «При запуске Safari открывать», затем выберите «Новое частное окно».

   Если этот параметр не отображается, выполните одно из описанных ниже действий.

   - На Mac с macOS 13 или новее. Выберите меню Apple > «Системные настройки» > «Рабочий стол и Dock» и убедитесь, что установлен флажок «Закрывать окна при завершении приложения».
   - На Mac с macOS 12 или более ранней версии. Выберите меню Apple > «Системные настройки» > «Основные» и убедитесь, что установлен флажок «Закрывать окна при завершении приложения».

### Еще больше конфиденциальности в Safari

- Удалите из папки «Загрузки» все объекты, загруженные из окон в режиме «Частный доступ».
- Закройте все остальные окна в режиме «Частный доступ», если они до сих пор открыты, чтобы никто не мог воспользоваться кнопками «Назад» и «Вперед», чтобы просмотреть страницы, которые Вы посещали.

# Управление настройками функции «Отправлено Вам» на устройствах Apple

Когда кто-то делится с Вами контентом из приложения «Музыка», Apple TV, News, «Фото», «Подкасты» и Safari, функция «Отправлено Вам» автоматически помещает этот контент в раздел «Отправлено Вам» для удобного доступа. Контент, отправленный Вам в приложении «Сообщения», автоматически переносится в раздел «Отправлено Вам» в приложении «Музыка», Apple TV, News, «Фото», «Подкасты» и Safari.


### Управление контентом от определенных людей на iPhone или iPad

Чтобы контент, отправленный Вам в приложении «Сообщения», не отображался в связанных приложениях, эту функцию можно выключить для определенного человека.

1. На iPhone или iPad коснитесь «Сообщения», затем коснитесь разговора с контентом, которым Вы не хотите делиться в других приложениях.
2. Когда откроется цепочка обсуждений, коснитесь имени вверху.
3. Выключите параметр «Отображать в "Отправлено Вам"», затем коснитесь «Готово».

Подробнее об этом можно узнать в источниках ниже.

- Использование приложения «Сообщения» для получения и отправки контента друзьям в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iphb66cfeaad)
- Использование приложения «Сообщения» для получения и отправки контента друзьям в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipad5bf3d77b)

### Управление контентом от определенных людей на Mac

Чтобы контент, отправленный Вам в приложении «Сообщения», не отображался в связанных приложениях, эту функцию можно выключить для определенного человека.

1. Откройте приложение «Сообщения» на Mac, затем выберите разговор.
2. В правом верхнем углу разговора нажмите ⓘ, затем снимите флажок «Отображать в "Отправлено Вам"», чтобы убрать общий контент из раздела «Отправлено Вам».

   Когда функция «Отправлено Вам» выключена, общий контент по-прежнему можно закреплять, чтобы он отображался в соответствующем приложении.

Подробнее об этом можно узнать в источниках ниже.

- Отслеживание отправленного контента в приложении «Сообщения» на Mac в Руководстве пользователя Mac (https://support.apple.com/guide/messages/ichtdc9ebc32)

### Управление контентом в определенных приложениях на iPhone или iPad

Чтобы включить или выключить функцию «Отправлено Вам» в приложении «Музыка», Apple TV, News, «Фото», «Подкасты» и Safari, можно изменить настройки.

- На iPhone или iPad откройте «Настройки» > «Сообщения» > «Отправлено Вам», затем выключите параметр «Автоотправка» или «Отправлено Вам» для определенного приложения.

### Управление контентом в определенных приложениях на Mac

Чтобы включить или выключить функцию «Отправлено Вам» в приложении «Музыка», Apple TV, News, «Фото», «Подкасты» и Safari, можно изменить настройки.

1. Откройте приложение «Сообщения» на Mac.
2. Выберите меню «Сообщения» > «*Настройки*».
3. Нажмите «Отправлено Вам», затем выполните одно из описанных ниже действий.
   - *Выключение для всех приложений.* Нажмите «Выключить».
   - *Выключение для выбранных приложений.* Снимите флажки приложений.

Подробнее об этом можно узнать в источниках ниже.

- Отслеживание отправленного контента в приложении «Сообщения» на Mac в Руководстве пользователя Mac (https://support.apple.com/guide/messages/ichtdc9ebc32)

# Дополнительная информация

## Дополнительная информация по безопасности

Прежде чем вносить изменения или удалять информацию, примите во внимание перечисленные ниже пункты.

- Вы можете сделать запись подозрительной активности. См. также раздел Получение доказательств, связанных с Аккаунтом Apple другого человека.
- Другие люди могут заметить изменения, внесенные Вами в настройки доступа. Нажав этот значок в тексте руководства, Вы можете изучить информацию о безопасности, прежде чем предпринимать определенные действия: .
- Изменив настройки доступа, Вы можете потерять доступ к важным инструментам и информации.
- Приложения, разработанные другими компаниями (например, YouTube или Instagram), имеют собственные настройки, которые Apple контролировать не может. В руководствах каждого из приложений указано, как просмотреть или изменить их настройки, а также уведомляют ли они пользователя при изменении настроек. Подробнее см. в разделе Настройки сторонних приложений.

## Другие ресурсы по безопасности в связи с технологиями

На сайтах, указанных далее, Вы найдете дополнительную информацию о безопасности в связи с технологиями.

**США**

- Проект Safety Net Национальной сети по борьбе с домашним насилием
- Национальный центр помощи жертвам преступлений

**Великобритания**

- Refuge UK

**Австралия**

- WESNET Safety Net Australia

Дата публикации: 28 октября 2024 г.

# Другие ресурсы поддержки

Если у Вас возникли другие проблемы, связанные с технологиями Apple, обратитесь к ресурсам, указанным далее.

## Служба поддержки Apple

Ресурсы для самостоятельного изучения по широкому кругу тем, связанных с технологиями Apple, и ссылки для связи со специалистами. Служба поддержки Apple имеет крайне ограниченный доступ к Вашей информации без Вашего явного разрешения и не имеет доступа к Вашим данным и/или паролям.

- Служба поддержки Apple (https://support.apple.com)
- В США: 1-800-275-2273; в Канаде: 1-800-263-3394

## Безопасность платформы Apple

На веб-странице Безопасность платформы Apple приведена информация о безопасности оборудования и системы, шифровании и защите данных, а также безопасности сервисов, таких как Аккаунт Apple, iCloud, Вход с Apple, Apple Pay, Сообщения, FaceTime и Локатор.

## Сайт Apple о конфиденциальности

На веб-странице Apple о конфиденциальности описаны функции, защищающие Ваши данные; настройки, с помощью которых Вы можете контролировать свои данные; обозначения, применяемые для приложений; отчеты о прозрачности для запросов от государственных органов; и Политика конфиденциальности Apple.

## Ваши данные и конфиденциальность

Выполнив вход на онлайн-портал «Данные и конфиденциальность» со своим Аккаунтом Apple, Вы сможете узнать, какие данные собирает Apple; получить или перенести копию своих данных; а также исправить, деактивировать или удалить свои данные.

## Сообщество службы поддержки Apple

В сообществе службы поддержки Apple Вы можете задавать вопросы и получать ответы от других пользователей Apple по всему миру.

# Авторские права



Apple
One Apple Park Way
Cupertino, CA 95014
apple.com



RS028-00796