Руководство по личной безопасности пользователя

Обезопасьте себя и свои личные данные

Содержание

Пошаговые инструкции

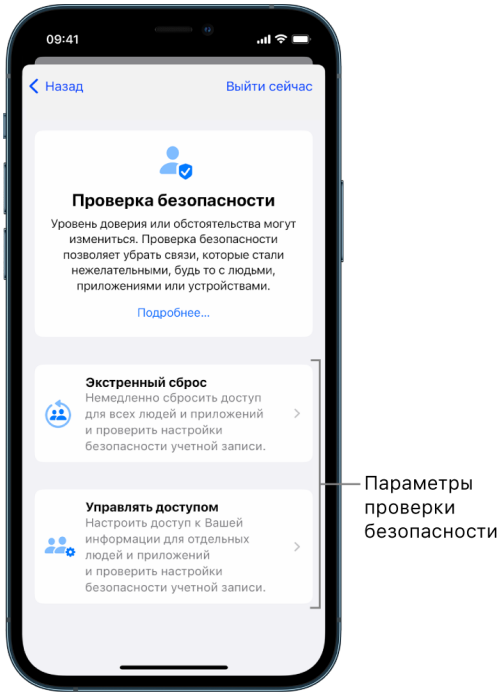
Функция «Проверка безопасности» (iOS 16 или новее)

Закрытие доступа к личной информации и защита учетной записи с помощью функции «Проверка безопасности»

Если Вам угрожает опасность, Вы можете использовать функцию «Проверка безопасности» на iPhone, чтобы быстро закрыть доступ к своей информации или просмотреть и обновить настройки доступа для отдельных людей и приложений. Для использования функции «Проверка безопасности» требуется iOS 16 или новее. (Чтобы определить версию программного обеспечения, установленного на устройстве, откройте «Настройки» > «Основные» и коснитесь «Об устройстве».)

Закрыть доступ к информации с помощью функции «Проверка безопасности» можно одним из двух способов.

- Используя Экстренный сброс, можно немедленно закрыть доступ к информации, перечисленной в разделе Что делает функция «Проверка безопасности» для Вашей безопасности. Экстренный сброс также позволяет просматривать и сбрасывать настройки, связанные с Вашим Apple ID.
- Используя Управление доступом, можно закрыть доступ к личной информации для определенных людей или приложений. Если Вы хотите узнать, чем именно и с кем Вы делитесь, используйте этот вариант.



При использовании Экстренного сброса и Управления доступом помните следующее:

- люди могут заметить, если Вы закроете им доступ к своей информации;
- когда Вы прекращаете делиться информацией с другими людьми, Вы можете потерять доступ к данным, таким как общие фотографии и заметки.

Подробнее о функции «Проверка безопасности» см. в разделе Что делает функция «Проверка безопасности» на iPhone для Вашей безопасности далее в этом документе.

Быстрый выход из функции «Проверка безопасности»

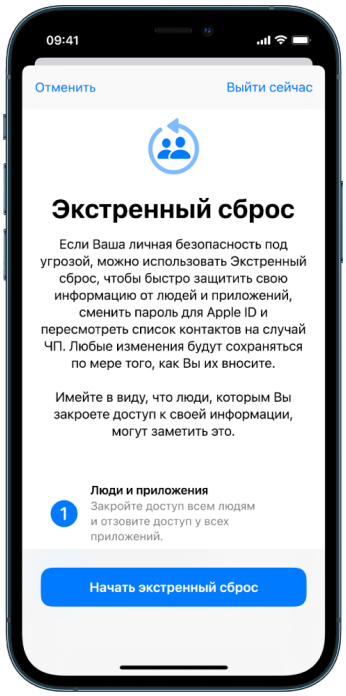
Кнопка «Выйти сейчас» позволяет быстро выйти из функции «Проверка безопасности». Любые изменения, которые Вы внесли до использования кнопки «Выйти сейчас», сохраняются.

- При касании кнопки «Выйти сейчас» на любом экране функции «Проверка безопасности» приложение «Настройки» сразу же закрывается, и Вы возвращаетесь на экран «Домой».

Как использовать Экстренный сброс в функции «Проверка безопасности»?

1. Откройте «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».
2. Коснитесь «Экстренный сброс», затем следуйте инструкциям на экране.

   Внесенные Вами изменения сохраняются сразу.



3. После завершения перейдите к разделу Контроль закрытия доступа ниже.

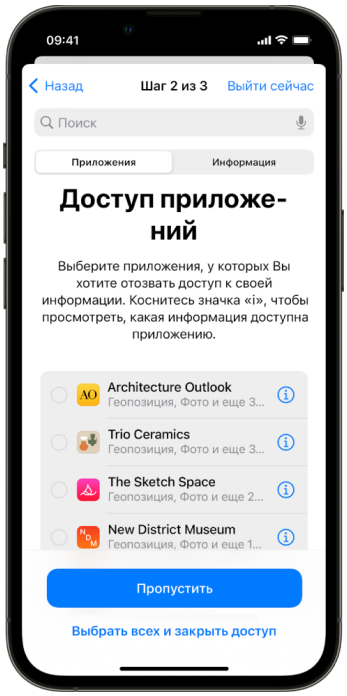
   Примечание. Если Вы включили функцию «Защита украденного устройства», проверка безопасности может работать немного по-другому. Подробнее о защите украденного устройства см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone (https://support.apple.com/HT212510).

Как использовать Управление доступом в функции «Проверка безопасности»?

Используйте Управление доступом, если хотите исследовать доступность Вашей информации более детально. В этом разделе можно просмотреть и сбросить информацию, которой Вы делитесь с другими людьми или которая доступна приложениям, а также изменить настройки безопасности устройства и Apple ID. Внесенные Вами изменения сохраняются сразу.

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

3. Выполните одно из указанных действий, чтобы прекратить делиться информацией с другими людьми.
   - 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.
4. Выполните одно из указанных действий, чтобы прекратить делиться информацией с приложениями.
   - 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.

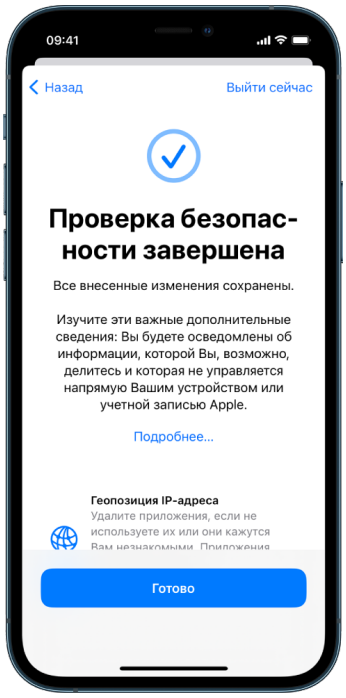


   - Коснитесь «Информация», выберите открытую информацию в списке, просмотрите информацию, которой Вы делитесь с приложениями, затем выберите информацию, которой Вы больше не хотите делиться с выбранными приложениями.
5. Коснитесь «Продолжить», затем выполните одно из указанных действий.

   Примечание. Вам будет предложено просмотреть только те параметры, которые Вы можете изменить.
   - Просмотрите и удалите устройства, которые подключены к Вашей учетной записи Apple ID.
   - Просмотрите и обновите номера телефонов, которые используются для подтверждения Вашей личности.
   - Обновите пароль Apple ID.
   - 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 для iOS 17 или новее).
- Если у Вас есть iCloud+ и Вы еще не включили Частный узел, включите эту функцию (только для iOS 17 или новее).

6. Коснитесь «Готово».



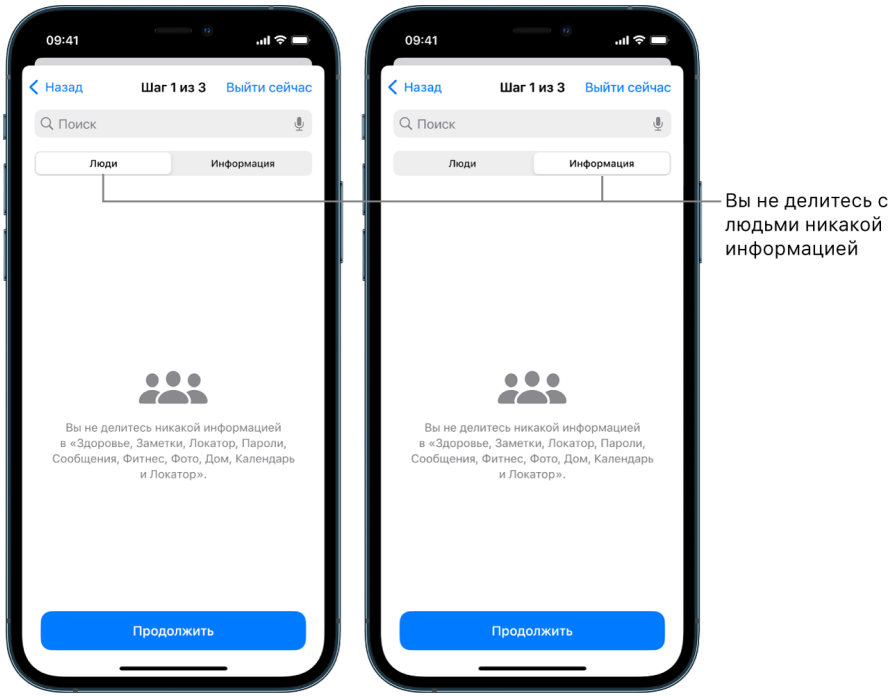
7. По завершении перейдите к следующему разделу и убедитесь, что доступ закрыт.

   Важно! Изучите дополнительные соображения при использовании функции «Проверка безопасности» далее в этом документе, чтобы ознакомиться с советами о том, какими еще способами можно защитить Вашу конфиденциальную информацию.

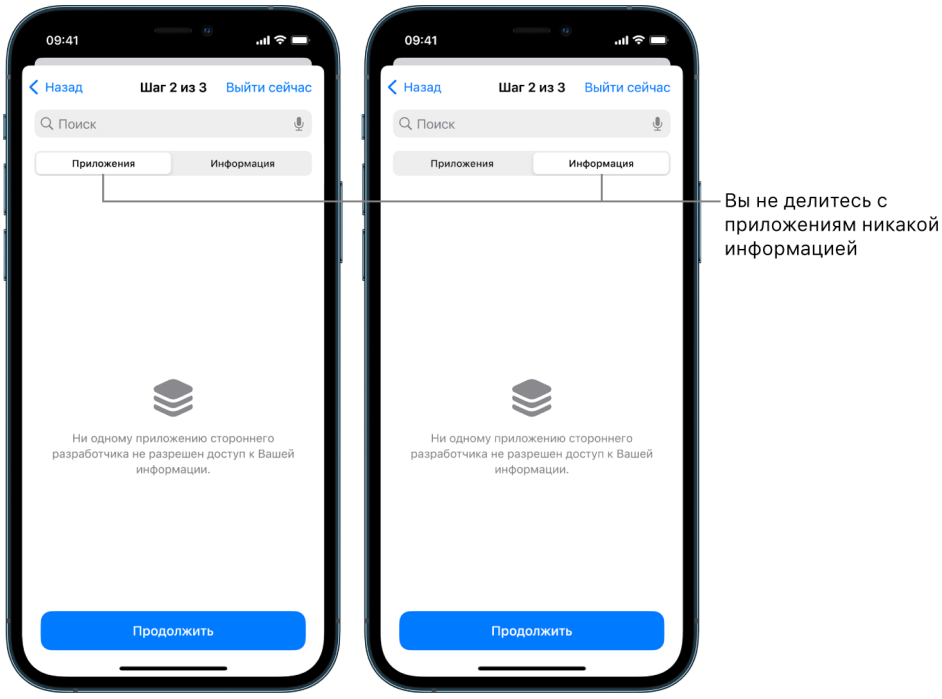
Контроль закрытия доступа

После использования функции «Проверка безопасности» можно подтвердить, что изменения были внесены. Вы можете убедиться в том, что доступ к информации был закрыт. Эта процедура состоит из трех шагов.

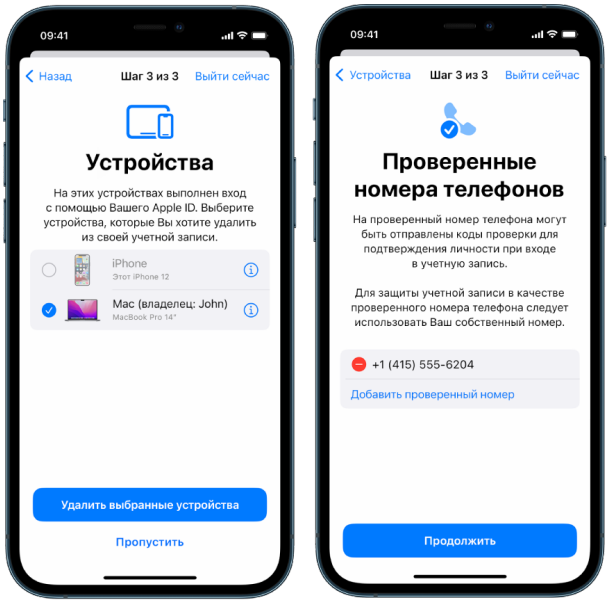
- *Шаг 1.* Убедитесь, что доступ к Вашей личной информации для других людей закрыт.



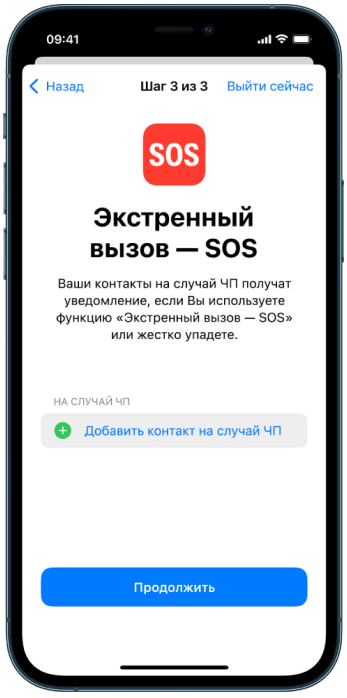
- *Шаг 2.* Убедитесь, что доступ для приложений закрыт.



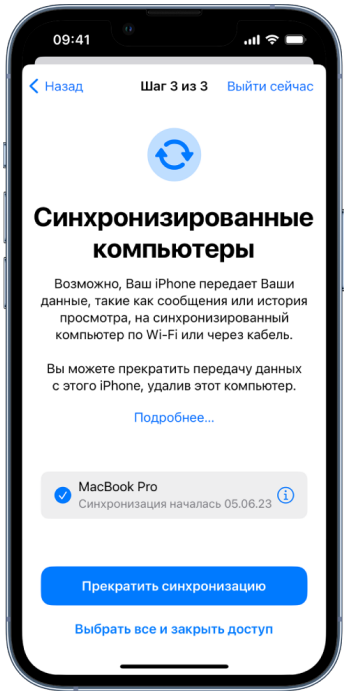
- *Шаг 3.* Убедитесь, что сохранены следующие изменения, внесенные в учетную запись.
  - Устройства, которые подключены к Вашей учетной записи Apple ID.
  - Номера телефонов, которые используются для подтверждения Вашей личности.



  - Добавленные или измененные контакты на случай ЧП.



- Удаленные компьютеры, синхронизированные с устройством.



Что делает функция «Проверка безопасности» на iPhone для Вашей безопасности

Если Вам угрожает опасность, Вы можете использовать функцию «Проверка безопасности» на iPhone, чтобы быстро закрыть доступ к своей информации или просмотреть и обновить настройки доступа для отдельных людей и приложений.

Если Вам нужно немедленно закрыть доступ к информации, обратитесь к разделу Как использовать Экстренный сброс в функции «Проверка безопасности»? ранее в этом документе.

Если Вам нужно просмотреть текущие настройки или закрыть доступ к информации для отдельных людей или приложений, обратитесь к разделу Как использовать Управление доступом в функции «Проверка безопасности»? ранее в этом документе.

Что делает функция «Проверка безопасности»?

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, изменить код-пароль, изменить пароль Apple ID и выполнить другие действия.

Если Вы хотите снова предоставить кому-то доступ после использования функции «Проверка безопасности», просто откройте приложение или службу, в которых находится контент, и снова поделитесь этим контентом.

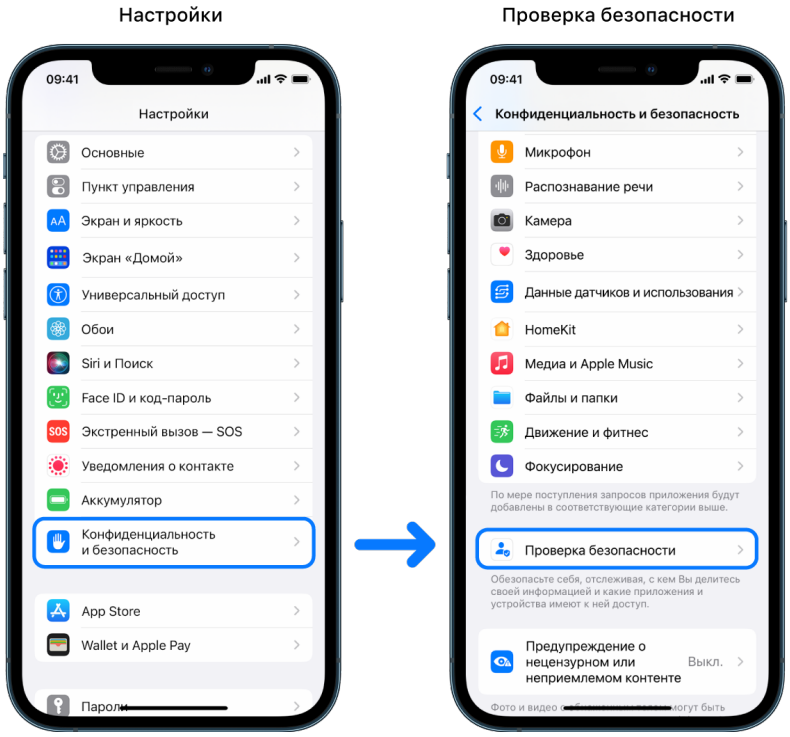
Если Вы включили функцию «Защита украденного устройства», проверка безопасности может работать немного по-другому. Подробнее о защите украденного устройства см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone (https://support.apple.com/HT212510).

Примечание. Если на Вашем iPhone включены ограничения Экранного времени или установлен профиль управления мобильными устройствами (MDM), Вы все равно 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 под управлением iOS 16 или новее. Для использования функции «Проверка безопасности» требуется Apple ID с включенной двухфакторной аутентификацией. Вы также должны выполнить вход в меню «Настройки» > [*Ваше имя*] на iPhone. (Чтобы определить версию программного обеспечения, установленного на устройстве, откройте «Настройки» > «Основные» и коснитесь «Об устройстве».)

Для доступа к функции «Проверка безопасности» откройте «Настройки» > «Конфиденциальность и безопасность» > «Проверка безопасности».



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 Закрытие предоставленного доступа к контенту на iPhone или iPad далее в этом документе.

Какие приложения Apple прекращают делиться информацией с другими людьми при использовании функции «Проверка безопасности»?

Функция «Проверка безопасности» может закрыть доступ других людей к информации из перечисленных ниже приложений Apple.

Приложение	Информация
	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

Доступ к какой информации закрывает для приложений функция «Проверка безопасности»?

Функция «Проверка безопасности» удаляет из всех приложений на iPhone любые данные, собранные перечисленными ниже приложениями, сетями и функциями.

	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

Что можно изменить в моем Apple ID с помощью функции «Проверка безопасности»?

С помощью функции «Проверка безопасности» можно изменить информацию, связанную с Вашим Apple ID. Вы можете сделать следующее:

- просмотреть и удалить устройства, на которых выполнен вход в Вашу учетную запись;
- просмотреть и изменить доверенные номера телефона;
- изменить пароль Apple ID;
- изменить контакты на случай ЧП;
- изменить код-пароль устройства и информацию Face ID или Touch ID.

Примечание. Если Вы включили функцию «Защита украденного устройства», проверка безопасности может работать немного по-другому. Подробнее о защите украденного устройства см. в статье службы поддержки Apple Сведения о функции «Защита украденного устройства» для iPhone (https://support.apple.com/HT212510).

Что такое Экстренный сброс?

Функция «Проверка безопасности» предлагает такую возможность, как Экстренный сброс. С ее помощью можно немедленно закрыть любой доступ к перечисленным выше элементам. Экстренный сброс также позволяет просматривать и сбрасывать настройки, связанные с Вашим Apple ID.

Если Вы не знаете, чем именно и с кем Вы делитесь, обратитесь к разделу Как использовать Управление доступом? ранее в этом документе.

Дополнительные соображения при использовании функции «Проверка безопасности»

Используйте функцию «Проверка безопасности» на iPhone (под управлением iOS 16 или новее), чтобы быстро закрыть доступ к своей информации или с легкостью просматривать и обновлять настройки доступа для отдельных людей и приложений.

В некоторых случаях у Вас также может быть открыт доступ к информации, которая недоступна для функции «Проверка безопасности». Например, это могут быть учетные записи и пароли, общий доступ в социальных сетях, или Вы могли поделиться информацией на iPad или Mac. Внимательно просмотрите указанные рекомендации и подумайте, какие дополнительные шаги Вы можете предпринять, чтобы уменьшить объем открытой информации.

IP-адрес и приложения

IP-адрес — это назначаемый интернет-провайдером уникальный идентификатор устройства, необходимый для выполнения действий в интернете. IP-адреса не содержат точной информации о Вашей геопозиции, но могут указывать Вашу приблизительную геопозицию и помогать компаниям по сбору данных научиться распознавать Вас со временем. Установленные на устройстве приложения могут собирать информацию о Вашей приблизительной геопозиции на основе Вашего IP-адреса. Просмотрите список установленных приложений и удалите те из них, которыми Вы не пользуетесь или которые не узнаете.

Подробнее о просмотре и удалении установленных приложений см. в разделе Удаление подозрительного контента с устройств далее в этом документе.

Учетные записи и пароли

Подумайте о том, какие из используемых Вами учетных записей содержат конфиденциальную личную информацию, которую Вы хотите защитить. Это могут быть банковские приложения, интернет-магазины, электронная почта, социальные сети, образовательные сервисы и так далее. Измените пароли для этих учетных записей, чтобы никто другой не мог получить к ним доступ. Проверьте настройки безопасности и конфиденциальности каждой учетной записи, чтобы убедиться, что Ваша информация защищена. Если учетная запись используется для общения (например, электронная почта, телефон и обмен сообщениями), убедитесь, что ничего никуда не перенаправляется без Вашего разрешения.

Социальные сети

Помните о том, что при публикации фотографий и другой личной информации в социальных сетях можно случайно раскрыть сведения о своей геопозиции и личной жизни. Проверяйте настройки конфиденциальности, просматривайте списки контактов и подписчиков и тщательно думайте над тем, что Вы публикуете, чтобы обеспечить необходимый уровень конфиденциальности.

Другие устройства, которыми Вы владеете или которые Вы используете

Проверьте настройки общего доступа на любых других устройствах, которые Вы используете, и убедитесь, что Ваша информация в безопасности. Если рядом с Вами есть кто-то еще, например ребенок или друг, помните, что их устройства также могут делиться информацией.

Нежелательное отслеживание

Предупреждения о нежелательном отслеживании защищают от использования AirTag и других небольших аксессуаров в Локаторе для отслеживания другого человека без его ведома. Чтобы получать предупреждения, если с Вами перемещается неизвестный AirTag или другой аксессуар с поддержкой сети Локатора, необходимо включить Bluetooth®, Службы геолокации и Уведомления об отслеживании. Чтобы включить Уведомления об отслеживании, откройте приложение «Локатор», коснитесь «Я», прокрутите до раздела «Настроить уведомления об отслеживании», затем включите «Допуск уведомлений».

См. статью службы поддержки Apple Что делать, если Вы получили уведомление, что трекер AirTag, аксессуар с поддержкой сети «Локатор» или набор AirPods находится рядом с Вами (https://support.apple.com/119874).

Дом и HomeKit

Если Вы являетесь пользователем, добавленным в приложение «Дом» от Apple, и решили удалить себя из приложения, помните о том, что человек, который управляет этим 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 документе.

Apple Wallet

Если Вы используете карты или ключи в Wallet совместно с другим человеком, он может просматривать историю Ваших транзакций или использования ключей. Чтобы просмотреть последние транзакции, откройте приложение Wallet. Помните о том, что сведения о финансовых транзакциях также могут быть доступны через общие банковские счета и общие кредитные карты, или если у другого человека есть онлайн-доступ к Вашим финансовым учетным записям. Регулярно обновляйте свои пароли.

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 за подробной информацией о 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. Регулярно обновляйте свои пароли.

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. Детские учетные записи нельзя удалить из группы Семейного доступа. Однако их можно переместить в другую группу Семейного доступа либо удалить Apple ID ребенка.

Подробнее о том, как выйти из группы Семейного доступа, см. в шагах 1 и 2 контрольного списка Закрытие предоставленного доступа к геопозиции iPhone или iPad далее в этом документе.

Подробную информацию о Семейном доступе см. в разделе Управление настройками Семейного доступа далее в этом документе.

Контрольные списки

Ограничение доступа к iPhone или iPad

Если Вы используете iOS 15 или более ранней версии, с помощью этого контрольного списка можно узнать, у кого есть доступ к Вашим устройствам или к Вашему Apple ID. Если Вы используете iOS 16 или новее, обратитесь к разделу Что делает функция «Проверка безопасности» на iPhone для Вашей безопасности ранее в этом документе.

1. Проверьте, на каких устройствах выполнен вход в Ваш Apple ID. Для этого откройте «Настройки» > [*Ваше имя*]. Если какое-то из устройств Вам незнакомо, коснитесь его имени и выберите «Удалить из учетной записи».
2. Проверьте, зарегистрирован ли альтернативный внешний вид для Face ID или дополнительный отпечаток пальца для Touch ID на Вашем устройстве. Для проверки следуйте инструкциям в разделах: Настройка Face ID и Настройка Touch ID на iPhone или iPad.
3. Войдите в учетную запись на веб-сайте Apple ID (https://appleid.apple.com) и просмотрите все личные данные и сведения о безопасности, имеющиеся в Вашей учетной записи. Проверьте, есть ли что-то, что добавили не Вы.
4. Если двухфакторная аутентификация включена, просмотрите список доверенных устройств и проверьте, есть ли в нем незнакомые устройства. Если она не включена, ее можно включить, следуя инструкциям в разделе: Настройка двухфакторной аутентификации на iPhone или iPad.
5. Просмотрите приложения, установленные на устройстве, и проверьте, есть ли незнакомые Вам приложения или приложения, об установке которых Вы не помните. Если Вы не знаете, для чего предназначено приложение, найдите его описание в App Store.

6. Профили конфигурации системы управления мобильными устройствами (MDM), обычно устанавливаемые для контроля сотрудников, учащихся или служащих, предоставляют владельцу профиля дополнительные права и доступ к устройству пользователя. Сведения о том, как найти неизвестный профиль конфигурации MDM на устройстве, приведены в разделе Удаление неизвестных профилей конфигурации с iPhone или iPad.
7. Чтобы проверить, были ли изменены или дополнены права общего доступа, обратитесь к контрольному списку Закрытие предоставленного доступа к геопозиции iPhone или iPad.

Закрытие предоставленного доступа к контенту на iPhone или iPad

Если Вы используете iOS 15 или более ранней версии, с помощью этого контрольного списка можно узнать, как закрыть ранее предоставленный доступ. Если Вы используете iOS 16 или новее, обратитесь к разделу Что делает функция «Проверка безопасности» на iPhone для Вашей безопасности ранее в этом документе.

1. Проверьте, состоите ли Вы в группе Семейного доступа. Для этого откройте «Настройки» > [*Ваше имя*] и найдите вкладку «Семейный доступ». Если Вы в группе Семейного доступа, отобразятся имена участников этой группы.
2. Если Вы являетесь членом группы «Семья» и больше не хотите делиться информацией, Вы можете выйти из группы (если Вам уже исполнилось 13 лет). Если это Вы настроили группу «Семья» (под Вашим именем отображается слово *организатор*), Вы можете удалить кого угодно старше 13 лет из группы «Семья».
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 альбомом владеете Вы и хотите закрыть доступ для кого-то из подписчиков, коснитесь его имени и выберите этот параметр.
   - Если Вы подписчик, выберите «Отписаться» внизу экрана. Вы также можете удалить любые фото, которыми поделились.
5. В приложении «Календарь» коснитесь вкладки «Календари». Выберите общий календарь и коснитесь значка информации, 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 Безопасное управление доступом к контенту на iPhone, iPad и Apple Watch.

Закрытие предоставленного доступа к геопозиции iPhone или iPad

1. С помощью функции «Проверка безопасности» на iPhone (iOS 16 или новее) можно управлять доступом других пользователей и приложений к Вашей геопозиции.

2. Чтобы закрыть доступ к геопозиции для всех приложений, служб и сервисов (даже на короткое время), откройте «Настройки» > «Конфиденциальность» > «Службы геолокации» и выключите доступ к геопозиции. После этого все приложения на Вашем устройстве, например 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, откройте «Настройки» > «Конфиденциальность» > «Службы геолокации», затем выберите приложения и сервисы, которым нужно закрыть общий доступ. Коснитесь названия приложения, затем выберите «Никогда» под параметром «Разрешать доступ к геопозиции».

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 кнопки информации 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 Apple ID, откройте «Локатор» > «Устройства» и просмотрите список. Если в списке есть незнакомое устройство и Вы хотите просмотреть информацию о нем, коснитесь названия устройства. Затем коснитесь «Удалить это устройство».

   Примечание. Если Вы являетесь участником группы Семейного доступа, ниже будут перечислены другие участники группы, предоставившие Вам доступ к геопозиции 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.

Краткий обзор мер личной безопасности

Технологии Apple помогают Вам поддерживать связь с близкими и отслеживать, чем именно и с кем Вы делитесь. Если Вы предоставили кому-то доступ к личным данным, но больше не хотите это делать, или если Вы полагаете, что кто-то, у кого был доступ к Вашему устройству или учетным записям, внес изменения без Вашего разрешения, обратитесь к этому руководству, где есть стратегии и решения, с помощью которых можно вернуть контроль в свои руки.

Это руководство в первую очередь относится к устройствам Apple с новейшей операционной системой (iOS 17, iPadOS 17 и macOS Sonoma 14), а также к Apple Watch и HomePod.

В iOS 16 или новее можно использовать функцию «Проверка безопасности» на iPhone, чтобы быстро просмотреть, чем именно и с кем Вы делитесь. Затем Вы можете решить, стоит ли закрыть доступ к этой информации. Даже если Вы еще не обновили систему до iOS 16, Вы можете просмотреть составленный Apple список действий и подробные инструкции на тот случай, если Вы столкнулись с преследованием, домогательствами или травлей, совершаемыми с применением технологий. Сюда входят пошаговые инструкции о том, как закрыть доступ к данным, к которым ранее был открыт общий доступ, например: к геопозиции в приложении «Локатор», встречам, отправленным в Календаре, а также другим типам данных. Вы также узнаете о функциях, помогающих повысить Вашу личную безопасность: например, как автоматически сообщить другу о том, что Вы вернулись домой, и как активировать функцию «Экстренный вызов — SOS».

Это руководство регулярно обновляется, чтобы у Вас была вся необходимая информация и Вы чувствовали себя в безопасности и защищенности при использовании продукции Apple.

Совет. Здесь также приведены дополнительные сведения или ссылки, касающиеся других продуктов, в том числе ссылки на руководства пользователя устройств Apple. Можно загрузить это руководство в формате PDF и распечатать его, если так будет удобнее. Функции, инструкции и настройки могут отличаться в зависимости от модели устройства или версии программного обеспечения. Сведения об использовании определенных функций можно найти на веб-сайте службы поддержки Apple https://support.apple.com/ru-ru.

Дополнительные ресурсы по безопасности

Если Вам угрожает опасность, могут оказаться полезными перечисленные ниже дополнительные ресурсы.

- *США:* Проект Safety Net (https://www.techsafety.org/resources-survivors)
- *США:* Национальный центр помощи жертвам преступлений (https://victimsofcrime.org/getting-help/)
- *Великобритания:* Refuge UK (https://refuge.org.uk/i-need-help-now/how-we-can-help-you/national-domestic-abuse-helpline/)
- *Австралия:* WESNET Safety Net Australia (https://techsafety.org.au/resources/resources-women/)

Проверка и принятие мер

Безопасное использование AirDrop и NameDrop

Что такое AirDrop?

AirDrop — это простой способ передавать изображения, документы или другие файлы между устройствами Apple, которые находятся рядом друг с другом. Передачу можно настроить таким образом, чтобы все, кто находится рядом с Вами, могли выполнять отправку, или чтобы отправка была доступна только Вашим контактам, или чтобы никто не мог ничего отправить.

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.

Что такое NameDrop?

NameDrop (входит в состав AirDrop) — это удобный способ делиться Вашими контактными данными с другими пользователями и получать их контактные данные, не передавая свой iPhone. С помощью NameDrop пользователи могут обменяться контактными данными, просто поднеся свои iPhone друг к другу либо поднеся iPhone к Apple Watch(Apple Watch Ultra, Apple Watch Series 7 или новее либо Apple Watch SE 2-го поколения).

Вы также можете указать конкретные контактные данные, которыми хотите поделиться — и, что самое важное, те данные, которыми *не хотите* делиться. Для использования NameDrop оба устройства должны работать под управлением iOS 17.1 или новее либо watchOS 10.1 или новее. См. раздел Просмотр и обновление Вашей карточки контакта далее в этом документе.

NameDrop работает автоматически. Сведения о том, как выключить NameDrop, приводятся в разделе Выключение NameDrop далее в этом документе.

Примечание. 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.

Управление AirDrop

- 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/ru-ru/guide/ipad/ipad46a13d74/ipados)

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.

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

Отправка Ваших контактных данных через NameDrop

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, которые Вы хотите включить, 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.

Выключение NameDrop

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

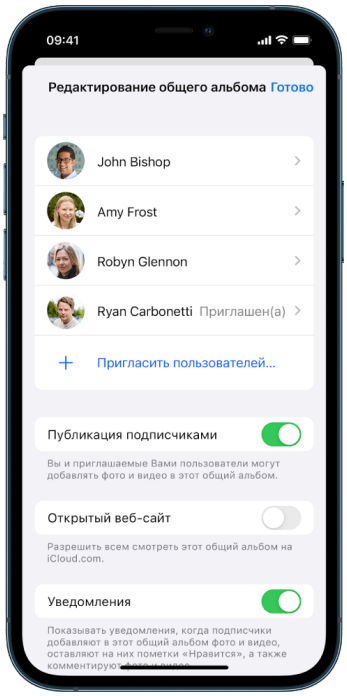
Безопасное управление доступом к контенту на iPhone, iPad и Apple Watch

Вы можете безопасно делиться контентом с другими людьми, используя свои устройства Apple. Отправка возможна несколькими способами. В любом случае на экране отображается список людей, с которыми Вы делитесь контентом. Вы также можете удалить пользователей из общего доступа к контенту на iPhone, iPad и Apple Watch.

Об управлении доступом к контенту на Mac см. в разделе Безопасное управление доступом к контенту на Mac далее в этом документе.

Управление настройками общего доступа к общим альбомам в Фото

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. Если перестать делиться фото или альбомом с кем-то, этот человек не получит уведомление и потеряет 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.

1. Выберите общий альбом на iPhone или iPad, затем коснитесь кнопки «Добавить подписчиков» .
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».
   - *Выключение уведомлений.* Коснитесь кнопки «Уведомления». Коснитесь снова, чтобы включить уведомления.

Подробнее об этом можно узнать в источниках ниже.

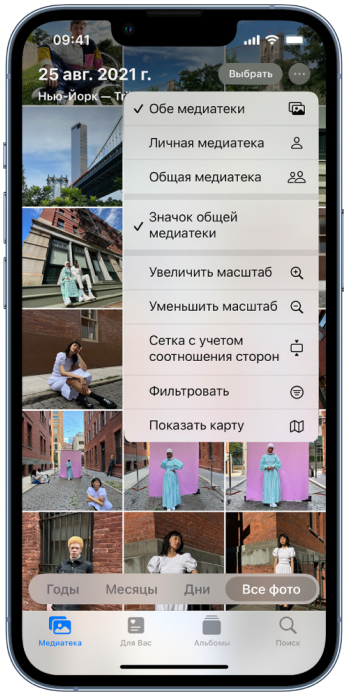
- Обмен фото и видео на iPhone в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iphf28f17237)
- Обмен фото и видео на iPad в Руководстве пользователя iPad (https://support.apple.com/guide/ipad/ipad4f44c78f)

Удаление участников из общей медиатеки в Фото

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 выбрать, к какому контенту хотите предоставить общий доступ в общей медиатеке, и автоматически делиться материалами прямо с камеры. Все пользователи общей медиатеки могут добавлять, редактировать и удалять контент. Весь контент хранится в хранилище iCloud, предоставляемом создателем общей медиатеки.

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».



1. Выполните одно из перечисленных ниже действий.
   - Чтобы удалить участников из общей медиатеки, перейдите в «Настройки» > «Фото» > «Общая медиатека», затем коснитесь «Удалить участников».
   - Чтобы покинуть общую медиатеку, откройте «Настройки» > «Фото» > «Общая медиатека», затем 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.
   - Удалить общую медиатеку может только ее организатор. Откройте «Настройки» > «Фото» > «Общая медиатека», затем 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 календарям

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

Если календарем владеете Вы и хотите закрыть доступ, коснитесь имени подписчика, чтобы отобразились параметры. Если Вы подписчик, выберите «Удалить календарь», чтобы удалить общий календарь.

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

Подробнее об этом можно узнать в источниках ниже.

- Общий доступ к календарям iCloud на iPhone в Руководстве пользователя iPhone (https://support.apple.com/guide/iphone/iph7613c4fb)
- Общий доступ к календарям iCloud на iPad в Руководстве пользователя iPad (https://support.apple.com/ru-ru/guide/ipad/ipadc2a14a22/ipados)

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 своими Apple ID, а также включить Safari в настройках iCloud (https://support.apple.com/guide/iphone/iphde0f868fd) и двухфакторную аутентификацию.

1. Коснитесь «Safari», затем коснитесь кнопки «Совместная работа» в правом верхнем углу.
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/ru-ru/guide/ipad/ipad76b9549e#iPad252604e8)

Управление настройками функции «Отправлено Вам» для определенного человека

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. 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)

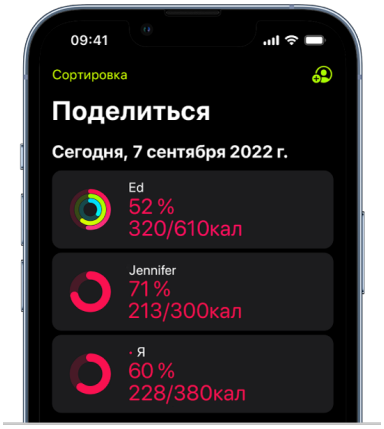
Управление настройками функции «Отправлено Вам» для определенного приложения

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 обменом данными 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.



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». Если Вы прекратите делиться своей активностью, то другой человек не получит уведомление о закрытии доступа.

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)

Безопасное управление доступом к контенту на Mac

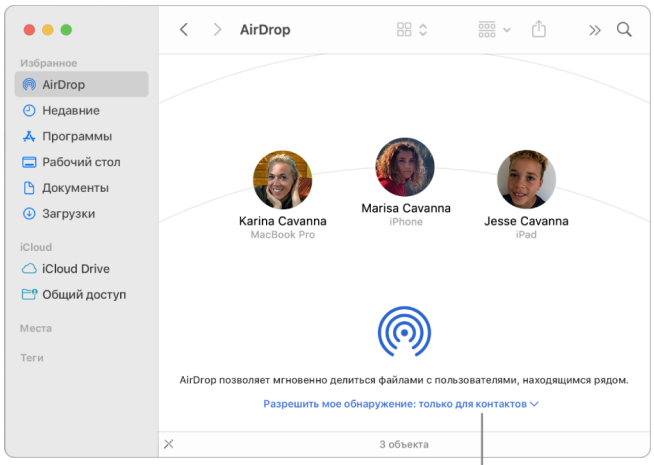
Вы можете безопасно делиться контентом с другими пользователями, используя свои устройства Apple. Отправка возможна несколькими способами. При отправке любым из способов Вы можете просмотреть, с кем Вы делитесь, а также удалить пользователей из общего доступа к контенту на Mac.

Сведения об управлении доступом к контенту на iPhone, iPad и Apple Watch приводятся в разделе Безопасное управление доступом к контенту на iPhone, iPad и Apple Watch ранее в этом документе.

Управление настройками доступа к файлу при отправке через AirDrop на Mac

AirDrop — это простой способ передавать изображения, документы или другие файлы между устройствами Apple, которые находятся рядом друг с другом. Передачу можно настроить таким образом, чтобы все, кто находится рядом с Вами, могли выполнять отправку, или чтобы отправка была доступна только Вашим контактам, или чтобы никто не мог ничего отправить.

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 при отправке файлов через AirDrop, Вы можете включать функцию AirDrop, когда она требуется, и выключать ее в остальное время.



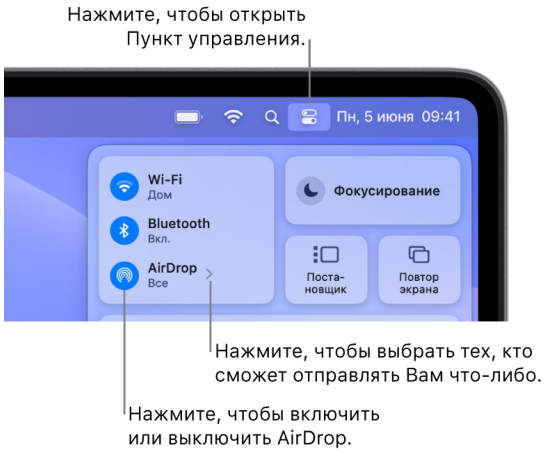
Выбирайте, кто сможет отправлять Вам что-либо.

Управление AirDrop из окна Finder

1. На Mac 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.

Управление AirDrop в Пункте управления на Mac

В Пункте управления на Mac можно быстро включить или выключить AirDrop и выбрать тех, кто может отправлять Вам что-либо через AirDrop.



1. На Mac нажмите Пункт управления в строке меню.
2. Выполните одно из перечисленных ниже действий.
   - *Включение или выключение AirDrop.* Нажмите значок AirDrop.
   - *Выбор тех, кто может отправлять Вам объекты.* Нажмите кнопку со стрелкой рядом с AirDrop, затем выберите нужный параметр.

Подробнее об этом можно узнать в источниках ниже.

- Использование AirDrop на Mac для отправки файлов на соседние устройства в Руководстве пользователя macOS (https://support.apple.com/guide/mac-help/mh35868)

Управление настройками доступа к общим альбомам в Фото на Mac

В общих альбомах в приложении «Фото» на Mac 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. Если перестать делиться фото или альбомом с кем-то, этот человек не получит уведомление и потеряет 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.

1. Откройте приложение «Фото» на Mac, затем нажмите общий альбом в разделе «Общие альбомы» бокового меню.
2. Нажмите кнопку «Люди» в панели инструментов.
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 в Фото на Mac

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.

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. Пользователи, имевшие доступ к общей медиатеке менее 7 дней, могут сохранить только контент, который загрузили 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 кнопку «Еще» рядом с пользователем, которого хотите удалить, 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 в Фото на Mac или ее удаление

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 настройками доступа к календарям на Mac

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

Если календарем владеете Вы и хотите закрыть доступ, коснитесь имени подписчика, чтобы отобразились параметры. Если Вы подписчик, Вы можете выбрать «Удалить календарь», и общий календарь будет удален.

1. Откройте приложение «Календарь» на Mac.
2. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Выберите «Календарь» > «Настройки».
   - На Mac с macOS 12 или более ранней версии. Выберите «Календарь» > «Настройки».

3. Нажмите «Учетные записи», выберите учетную запись календаря, затем нажмите «Делегирование».

   В списке «Учетные записи, к которым я имею доступ» отобразится учетная запись CalDAV.

   Примечание. В случае учетной записи Microsoft Exchange нажмите кнопку добавления ┼, затем введите имя того пользователя, который дал Вам доступ.

Подробнее об этом можно узнать в источниках ниже.

- Общий доступ к учетным записям календарей на Mac в Руководстве пользователя приложения «Календарь» (https://support.apple.com/guide/calendar/icl27527)

Управление общими группами вкладок в Safari на Mac

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 своими Apple ID, а также включить Safari в настройках iCloud и двухфакторную аутентификацию.

1. В приложении Safari на Mac нажмите кнопку «Совместная работа» 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)

Управление настройками функции «Отправлено Вам» для определенного человека на Mac

1. Откройте приложение «Сообщения» на Mac, затем выберите разговор.
2. Нажмите кнопку «Подробнее» в правом верхнем углу разговора, 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 приложения «Сообщения» (https://support.apple.com/guide/messages/ichtdc9ebc32)

Управление настройками функции «Отправлено Вам» для определенного приложения на Mac

Чтобы включить или выключить функцию «Отправлено Вам» в приложении «Музыка», Apple TV, News, «Фото», «Подкасты» и Safari, можно изменить настройки на Mac.

1. Откройте приложение «Сообщения» на Mac.
   - На Mac с macOS 13 или новее. Выберите «Сообщения» > «Настройки».
   - На Mac с macOS 12 или более ранней версии. Выберите «Сообщения» > «Настройки».
2. Нажмите «Отправлено Вам», затем выполните одно из описанных ниже действий.
   - *Выключение для всех приложений.* Нажмите «Выключить».
   - *Выключение для выбранных приложений.* Снимите флажки приложений.

Управление доступом к геопозиции

Предоставление или закрытие доступа к своей геопозиции другим пользователям

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. Обратитесь к разделу Управление настройками Семейного доступа далее в этом документе.

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. Подробнее см. в разделе Использование функции «Точное местонахождение» на iPhone 15 для встречи с другом в Руководстве пользователя iPhone. (https://support.apple.com/guide/iphone/iph3effd0ed6)
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 документе.

Приложение	Описание
Сообщения	Когда другие пользователи касаются значка Вашего контакта в Сообщениях, они переходят на экран «Подробнее», где показана Ваша текущая геопозиция, если Вы делитесь ей с помощью Локатора.
Сообщения	В Сообщениях в iOS 17 либо iPadOS 17 и новее другие пользователи также могут видеть Ваше приблизительное местонахождение вверху экрана разговора.
Карты	Когда другие пользователи выполняют поиск по Вашему имени в Картах, они видят на карте Вашу текущую геопозицию, если Вы делитесь ей с помощью Локатора.

Просмотр и удаление уведомлений о Вас

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 о своей геопозиции. В том числе уведомления, установленные Вами, и уведомления, созданные Вашими друзьями. Чтобы просматривать все уведомления о Вас, следуйте инструкциям далее.

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Откройте приложение «Локатор», затем коснитесь «Я».
   - *На Mac.* Откройте приложение «Локатор», нажмите «Я», затем нажмите кнопку информации ⓘ.
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 и iPad

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

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

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».

Закрытие доступа к Вашей геопозиции в Сообщениях на iPhone и 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 и 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 выключать функцию «Найти iPhone» в случае потери или кражи устройства

Чтобы предотвратить кражу и легче найти свой телефон в случае его потери, Вы можете включить функцию «Найти iPhone». Для этого откройте «Настройки» > [*Ваше имя*] > «Локатор».

Когда функция «Найти iPhone» включена, Ваше устройство можно найти в сети Локатора в течение 24 часов с момента 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.

Важно! После выключения приложения «Найти [*название устройства*]» и сети Локатора Вы не сможете найти, заблокировать или стереть потерянное или украденное устройство.

- *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. Откройте меню Apple > «Системные настройки», нажмите «Apple ID», нажмите «iCloud», затем нажмите «Параметры» рядом с «Найти Mac».

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

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 и iPad

1. В приложении «Карты» на iPhone или iPad (модели Wi-Fi + Cellular) коснитесь значка профиля справа от строки поиска.
2. Выберите «Избранное», чтобы открыть окно со всеми геопозициями, которые Вы отметили как избранные.
3. Коснитесь кнопки информации ⓘ рядом с избранным пунктом интереса.
4. Прокрутите вниз до раздела «Сообщить о прибытии», чтобы просмотреть, кому автоматически сообщается примерное время Вашего прибытия.
5. Чтобы удалить человека, коснитесь кнопки удаления рядом с его именем.
6. Чтобы добавить человека, коснитесь «Пользователи», затем выберите из списка Ваших контактов пользователя, 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 настройками Служб геолокации

С Вашего разрешения Службы геолокации могут предоставлять приложениям (таким как Карты, Камера и Погода) и сайтам доступ к информации из различных сетей для определения Вашей примерной или точной геопозиции. Службы геолокации доступны на iPhone, iPad и Mac.

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 веб-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.

Выключение Служб 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.* Откройте «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации» и выключите отправку геопозиции.
- На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Защита 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», нажмите «Защита и безопасность», затем нажмите «Конфиденциальность». Нажмите «Службы геолокации». Если замок в левом нижнем углу закрыт, нажмите его, чтобы снять защиту с панели настроек. Снимите флажок «Включить 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. Откройте меню Apple > «Системные настройки», нажмите «Защита и безопасность», нажмите «Службы геолокации», включите параметр «Службы геолокации», введите пароль, затем нажмите «Снять защиту».
- На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Защита и безопасность», затем нажмите «Конфиденциальность». Нажмите «Службы геолокации». Если замок в левом нижнем углу закрыт, нажмите его, чтобы снять защиту с панели настроек. Установите флажок «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 следующих вариантов.

- Однократно
- При использовании
- Запретить

Вы также можете просмотреть или изменить доступ к своей геопозиции для отдельных приложений и указать, как часто они могут использовать Вашу геопозицию. Далее приведены инструкции для iPhone и iPad

1. Откройте «Настройки» > «Конфиденциальность и безопасность» > «Службы геолокации» и 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 нажмите значок замка в левом нижнем углу, 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 кнопку удаления —. Чтобы удалить все геопозиции, нажмите кнопку «Еще» , затем нажмите «Очистить журнал».

Прекращение использования метаданных геопозиций и их удаление в приложении «Фото»

Когда в приложении «Камера» включены Службы геолокации, приложение определяет геопозицию снятых фото и видео на основе данных о геопозиции, полученных от сотовых сетей, Wi-Fi, GPS и Bluetooth®. Эти метаданные о геопозиции, встроенные в каждое фото и видео, помогают Вам находить фото и видео в приложении «Фото» по месту съемки и просматривать коллекции 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 следующих 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 кнопку информации и просмотрите информацию о геопозиции.

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 следующих 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 кнопки информации 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 страницы экспорта, затем коснитесь «Параметры».
3. Выключите параметр «Геопозиция» и коснитесь «Готово».
4. Поделитесь фото любым из способов, предлагаемых на странице экспорта.

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 iOS 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.

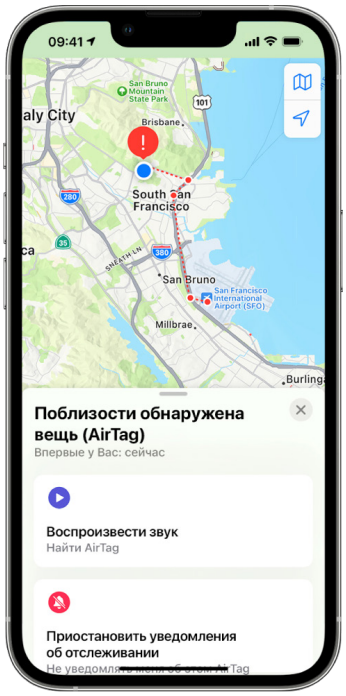
Доступность ПО для предупреждений о нежелательном отслеживании:

- предупреждения о нежелательном отслеживании для AirTag и других аксессуаров с поддержкой сети «Локатор» доступны на iPhone или iPad с iOS 14.5 или iPadOS 14.5 или новее;
- предупреждения 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. (https://datatracker.ietf.org/doc/draft-detecting-unwanted-location-trackers/01/)
- Google обеспечивает обнаружение нежелательного отслеживания на устройствах с Android 6.0 или новее.

Если Вы получили предупреждение о нежелательном отслеживании

Выполните перечисленные ниже действия для обнаружения вещи.

1. Коснитесь предупреждения.
2. Коснитесь «Продолжить», затем коснитесь «Воспроизвести звук». Либо, если 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 Вы хотите повторно просмотреть информацию в полученном ранее предупреждении

1. Выполните одно из описанных ниже 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».

Подробнее см. в статье службы поддержки Apple Что делать, если вы получили уведомление, что трекер AirTag, аксессуар с поддержкой сети «Локатор» или набор AirPods находится рядом с вами (https://support.apple.com/HT212227).

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

Выполните указанные ниже действия для получения информации об устройстве.

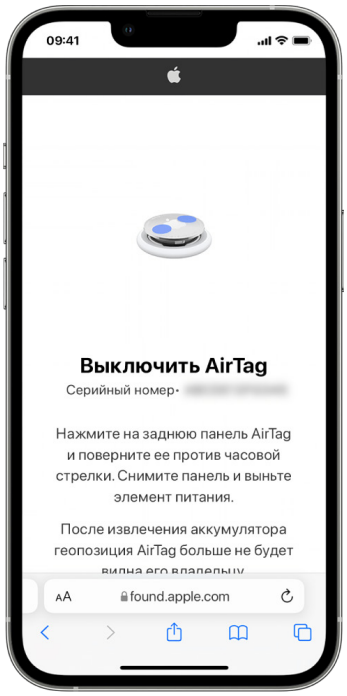
1. Поднесите верхнюю часть iPhone к вещи и дождитесь получения уведомления.
2. Коснитесь уведомления. Откроется сайт, содержащий следующую информацию о вещи:
   - серийный номер или идентификатор устройства;
   - последние четыре цифры телефонного номера или частично скрытый адрес электронной почты пользователя, 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

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 предупреждения о нежелательном отслеживании для этой вещи.



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

Посетите страницу поддержки о поиске неизвестных трекеров для получения дополнительной информации об обнаружении нежелательного отслеживания на устройствах Android. (https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&)

Если звучит сигнал AirTag

AirTag издает сигнал через некоторое время после отдаления от владельца, который зарегистрировал AirTag, и этот сигнал могут услышать все вокруг. 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, был ли он помечен как потерянный, а затем вернуть его. 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). От Вас может потребоваться предоставить AirTag или его серийный номер. (https://support.apple.com/102170)

Общий доступ к вещам с 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 Apple ID 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, предупреждения 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 предупреждения 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 с помощью функции «Проверка безопасности»

Примечание. После выхода из группы Вы не сможете видеть геопозицию AirTag, а предупреждения 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».

Выход из группы общего доступа с помощью Локатора

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

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

Удаление 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 общий доступ, затем коснитесь «Проверить доступ».
4. Коснитесь «Вещи» > «Закрыть доступ».

Удаление 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».

Безопасно управляйте перенаправляемым контентом

Вы можете просматривать и регулировать способы автоматического перенаправления контента и решать, кому Вы его отправляете на iPhone, iPad или Mac.

Управление пересылкой писем в iCloud

В приложении «Почта» легко увидеть, перенаправляются ли письма на другой адрес, и выключить такую возможность.

1. Войдите в свою учетную запись iCloud на сайте https://www.icloud.com, используя имя пользователя и пароль для Вашего Apple ID. При необходимости введите код двухфакторной аутентификации.
2. Откройте приложение «Почта», нажмите кнопку «Настройки» над списком почтовых ящиков, затем выберите «Настройки».
3. Во вкладке «Основные» проверьте, установлен ли флажок «Пересылать мои письма», и просмотрите, кому 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 текстовое сообщение на телефон, отличный от iPhone, оно отправляется в формате SMS-сообщения. Можно настроить iPhone таким образом, чтобы при отправке или получении сообщения SMS оно отображалось и на других устройствах. Вы можете просмотреть список устройств и выключить пересылку текстовых сообщений на определенные устройства.

1. На iPhone перейдите в «Настройки» > «Сообщения».
2. Коснитесь параметра «Переадресация», чтобы увидеть, какие устройства могут отправлять и получать текстовые сообщения с Вашего устройства.
3. Выключите некоторые устройства при необходимости.

Управление переадресацией вызовов в приложении «Телефон»

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 Вашем iPhone перейдите в «Настройки» > «Телефон» > «Вызовы» > «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.

Блокировка чужих попыток входа

При входе на новом устройстве на Ваших проверенных устройствах отобразится уведомление о входе. Это уведомление включает карту с местоположением нового устройства. Это уведомление может быть показано на любом доверенном устройстве: iPhone, iPad или Mac.

Это приблизительное местонахождение, рассчитанное на основе IP-адреса или сети, которые использует устройство. Эта отметка на карте не точная геопозиция устройства.

- Если Вы получили уведомление о том, что Ваш Apple ID используется для входа на новом устройстве, но Вы не выполняли на нем вход, коснитесь «Не разрешать», чтобы заблокировать попытку входа. Возможно, стоит создать снимок экрана, чтобы заснять уведомление перед тем, как его отклонить.

См. раздел Запись подозрительной активности далее в этом документе.

Если Вы считаете, что Ваш Apple ID мог быть скомпрометирован, обратитесь к разделу Поддержание безопасности Apple ID далее в этом документе и удалите неизвестные устройства.

Запись подозрительной активности

В некоторых случаях, например, когда приходит уведомление о том, что кто-то пытается использовать Ваш Apple ID для входа на новом устройстве, Вы можете создать снимок или запись экрана. Затем их можно сохранить в виде файла изображения или видео на iPhone, iPad или Mac.

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 кнопку «Остановить запись» ⏹ в строке меню.

Если задан параметр «Отображать плавающую миниатюру», можно выполнить одно из следующих 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.

Безопасное хранение данных в iCloud

iCloud безопасно хранит Ваши фото, видео, документы, музыку, приложения, резервные копии и многое другое и синхронизирует их на всех Ваших устройствах. Используя iCloud, Вы также можете делиться контентом, например фотографиями, календарями и геопозицией, с друзьями и близкими. Вы можете выполнять вход в iCloud на своем устройстве или в интернете, используя личную учетную запись Apple ID.

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. Откройте меню Apple > «Системные настройки», нажмите «Apple ID» , затем нажмите «iCloud».

- На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Apple ID» , 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. Откройте меню Apple >«Системные настройки», нажмите «Apple ID» , нажмите «Обзор», затем нажмите «Выйти».

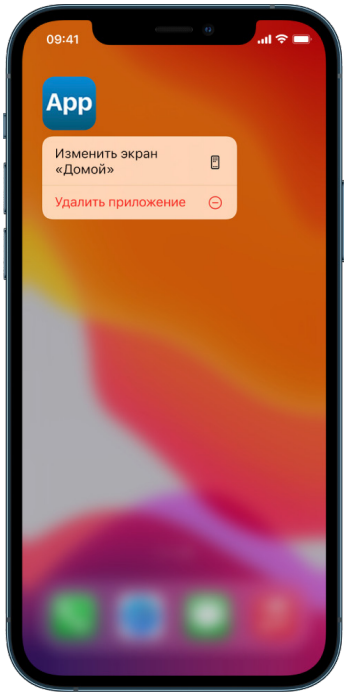
- На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Apple ID» , нажмите «Обзор», затем нажмите «Выйти».

Удаление подозрительного контента с устройств

На iPhone, iPad или Mac можно удалить все данные, которые кажутся Вам незнакомыми или подозрительными, например приложения или файлы конфигурации.

Просмотр и удаление приложений на iPhone или iPad

Если Вы полагаете, что кто-то, кому Вы доверяете, мог установить приложение на Ваше устройство без Вашего разрешения, Вы можете просмотреть список приложений, установленных на устройстве, а также проверить настройки их доступа и изменить их при необходимости. Если Вы заметили, что у приложения есть доступ к данным, но Вы его не предоставляли, или если Вы не помните, как установили это приложение или дали ему доступ, Вы можете удалить это приложение.



- *Удаление приложения из библиотеки приложений.* Перейдите на экран «Домой», затем смахните влево через все страницы экрана «Домой», пока не откроется библиотека приложений. Далее коснитесь в поле поиска, чтобы найти приложение, затем коснитесь его значка и удерживайте, пока не появится меню. Коснитесь «Удалить приложение», чтобы его удалить.
- *Удаление приложения с экрана «Домой».* Коснитесь приложения на экране «Домой» и удерживайте его, коснитесь «Удалить приложение», затем коснитесь «Удалить с экрана "Домой"», чтобы оставить его в библиотеке приложений, или коснитесь «Удалить приложение», чтобы удалить его.

Просмотр и удаление приложений на компьютере Mac

Можно удалить установленные приложения, загруженные из интернета или с диска.

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.* 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.

Просмотр 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.

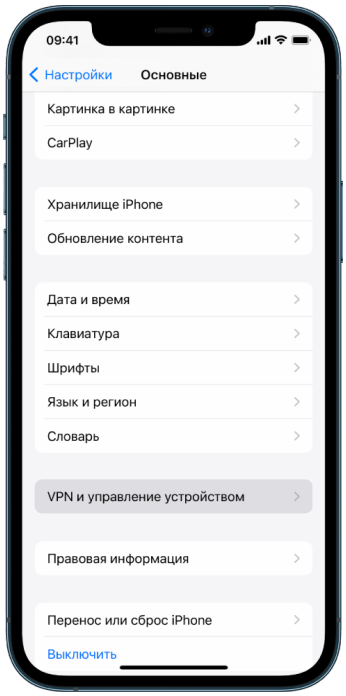
Профиль конфигурации может содержать настройки для учетной записи пользователя в приложении «Почта», а также настройки Wi-Fi, настройки VPN и многое другое. Профили конфигурации могут работать на iPhone, iPad, Mac и Apple TV.

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! 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

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. Перезагрузите устройство.

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.

Удаление неизвестных профилей конфигурации с компьютера Mac

1. Выполните одно из описанных ниже действий.

   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки» > «Конфиденциальность и безопасность», затем нажмите «Профили» .
   - На Mac с macOS 12 или более ранней версии. Откройте 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 кнопку удаления —.

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.

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 учетными записями Apple. Чтобы изменять статус в Семейном доступе, полезно знать, какие роли есть в группах Семейного доступа. На iPhone, iPad и Mac можно безопасно использовать Семейный доступ.

Если Вы пользуетесь семейным планом хранилища iCloud, файлы и документы каждого участника остаются конфиденциальными, а остальные пользователи видят только объем пространства, используемого каждым участником.

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.

- *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 учетную запись Apple ID 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 учетной записью Apple ID в семейную группу и удалить из нее любого старше 13 лет.

Чтобы проверить, входите ли Вы в семейную группу, откройте «Настройки» > [*Ваше имя*]. Если отображается параметр «Настройка Семейного доступа», Вы не используете Семейный доступ с этой учетной записью Apple ID. Если отображается значок с Семейным доступом, можно коснуться значка, чтобы просмотреть, кто входит в семейную группу и какие у каждого роли.

Удаление членов семейной группы

Организатор группы Семейного доступа может удалять других ее участников.

Примечание. Об удалении участников из семейной группы см. в разделах Удаление участников из семейной группы на iPhone или iPad и Удаление участников из семейной группы на компьютере Mac далее в этом документе.

Кроме того, 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». Также можно войти в учетную запись на веб-сайте Apple ID (https://appleid.apple.com) и выбрать пункт «Удалить учетную запись» в разделе «Семейный доступ».

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.

Примечание. Организатор не может удалить себя из группы Семейного доступа. Если Вы хотите поменять организатора, необходимо распустить группу и попросить другого взрослого создать новую.

У участника, удаленного из группы Семейного доступа или покинувшего группу, останутся покупки, оплаченные общей кредитной картой, но этот участник сразу потеряет доступ к контенту, которым делятся другие участники.

- Объекты других участников семейной группы больше не будут отображаться в разделе «Покупки» в iTunes Store, App Store и Apple Books.
- Защищенные (авторским правом) музыка, фильмы, телешоу, книги и приложения, загруженные ранее, будут недоступны, если их изначально купил кто-то другой. Другие члены семьи больше не смогут получить доступ к контенту, загруженному из Вашей коллекции.
- Встроенные покупки станут недоступны, если они сделаны в приложении, приобретенном кем-то другим. Вы можете восстановить доступ к встроенным покупкам, купив приложение.
- Геопозиции устройств членов семьи не будут отображаться для Вас в приложении «Локатор» на сайте iCloud.com, а также на iPhone, iPad и Mac.

Если Семейный доступ выключен

Если организатор выключит функцию «Семейный доступ», все участники семейной группы будут удалены из нее. Если в семейной группе есть дети до 13 лет, их нужно перевести в другую семейную группу прежде, чем распустить текущую семейную группу.

Удаление участников из семейной группы на iPhone или iPad

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.

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Семейный доступ» , затем в боковом меню выберите «Семейный доступ».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Семейный доступ» , затем выберите «Семейный доступ».
2. Выберите участника в списке, затем нажмите кнопку удаления —.

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

Выход из группы Семейного доступа на iPhone или iPad

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 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Семейный доступ» , затем в боковом меню выберите «Семейный доступ».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Семейный доступ» , затем выберите «Семейный доступ».

2. В списке членов семьи нажмите 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

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

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

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Семейный доступ», затем в боковом меню выберите «Семейный доступ».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Семейный доступ», затем выберите «Семейный доступ».
2. Нажмите кнопку «Подробнее» рядом со своим именем, затем нажмите «Закрыть семейный доступ».

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 объявлений, поддельным загрузкам, спаму в календаре и даже мошенническим телефонным звонкам. Все эти действия направлены на то, чтобы заставить Вас поделиться своими данными, например учетной записью Apple ID 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.

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 доступных аксессуаров, которые совместимы с приложением «Дом» и устройствами Apple, доступен по адресу: Аксессуары для умного дома (https://www.apple.com/home-app/accessories/).

Закрытие доступа к дому для определенного человека

1. Коснитесь приложения «Дом» или нажмите его, затем выберите «Настройки дома». Если отображаются несколько домов, выберите тот, из которого нужно выйти, затем выберите «Настройки дома».
2. В разделе «Люди» коснитесь имени пользователя, которого нужно удалить из дома, или нажмите его имя, затем коснитесь или нажмите «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» коснитесь значка приложения «Дом» или нажмите его, затем выберите «Настройки дома». Если отображаются несколько домов, выберите тот, из которого нужно выйти, затем выберите «Настройки дома».
2. Прокрутите вниз и коснитесь или нажмите «Покинуть дом». Коснитесь или нажмите «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» коснитесь значка приложения «Дом» или нажмите его, затем выберите «Настройки дома».
2. Внизу диалогового окна коснитесь или нажмите «Удалить дом», затем — «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.

Стирание всего контента и настроек

Если Вы полагаете, что кто-то мог получить физический доступ к Вашему устройству и вмешаться в работу встроенных средств защиты, Вы можете восстановить заводские настройки на устройстве, даже если Вы не используете новейшую версию iOS, iPadOS или macOS. 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. Кроме того, устанавливается новейшая версия операционной системы.

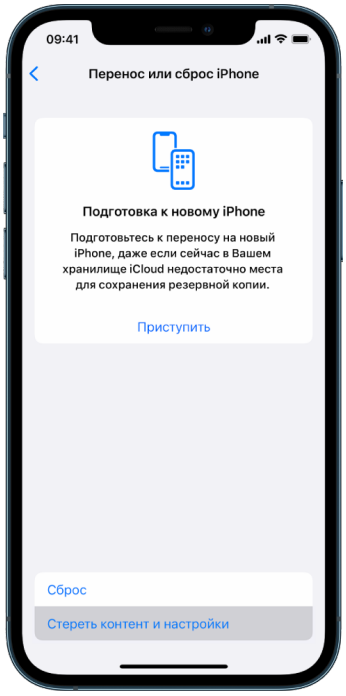
Этот процесс, запускаемый командой *«Стереть контент и настройки»* при наличии подключения к интернету, может занять некоторое время. Однако он помогает удостовериться, что доступ к устройству есть только у Вас.

Важно! При запуске команды «Стереть контент и настройки» все данные будут стерты.

Чтобы запустить команду «Стереть контент и настройки» на компьютере Mac, необходима macOS 12.0.1 или новее. Либо можно стереть компьютер 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).

Стирание iPhone или iPad и восстановление его заводских настроек

1. Откройте «Настройки» > «Основные» > «Сброс», затем коснитесь «Стереть контент и настройки».



2. Введите код-пароль или пароль учетной записи Apple ID.
3. Подождите, пока весь контент безопасно удалится с устройства.

Стирание компьютера Mac и восстановление его заводских настроек

1. Выполните одно из описанных ниже действий.
   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Основные», нажмите «Перенос или сброс», затем выберите «Стереть контент и настройки».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», затем в строке меню выберите «Системные настройки» > «Стереть контент и настройки».
2. В приложении «Ассистент стирания» введите учетные данные администратора (пароль для входа на компьютере Mac).
3. Просмотрите все, что будет удалено вместе с контентом и настройками.

   На Mac с несколькими учетными записями нажмите стрелку рядом с именем своей учетной записи, чтобы просмотреть объекты.
4. Нажмите «Продолжить», затем следуйте инструкциям на экране.

Восстановление данных из резервной копии

Если перед стиранием устройства Apple и восстановлением заводских настроек была создана резервная копия устройства, можно восстановить данные из резервной копии, хранящейся в iCloud или на компьютере. Если Вы полагаете, что в резервной копии могут быть настройки или приложения, которых не должно быть на Вашем устройстве, Вы можете проверить библиотеку приложений и настройки после восстановления из резервной копии. Для восстановления Mac используется Time Machine, а для восстановления iPhone или iPad можно использовать компьютер или iCloud.

Восстановление iPhone или iPad из резервной копии iCloud

1. Включите устройство. Отобразится экран приветствия. (Если Вы уже настроили устройство, потребуется стереть все его содержимое перед тем, как выполнить восстановление из резервной копии, следуя этой инструкции.)
2. Следуйте инструкциям по настройке, показываемым на экране, пока не отобразится экран приложений и данных, затем коснитесь «Восстановить из копии в iCloud».
3. Войдите в iCloud со своей учетной записью Apple ID.
4. Выберите резервную копию.

   Посмотрите на дату и размер каждой резервной копии и выберите наиболее подходящую. После выбора резервной копии начнется перенос. Если в сообщении говорится о том, что требуется более новая версия программного обеспечения, следуйте инструкциям на экране для обновления.
5. При появлении запроса войдите со своей учетной записью Apple ID, чтобы восстановить приложения и покупки.

   Если Вы приобретали контент в iTunes или App Store, используя несколько учетных записей Apple ID, Вам будет предложено войти в каждую из этих учетных записей. Если не удается вспомнить пароль, Вы можете пропустить этот шаг и выполнить вход позднее. Вы не сможете использовать приложения, пока не выполните вход со своей учетной записью Apple ID.
6. Не отключайте устройство от сети Wi-Fi и подождите, пока не появится индикатор выполнения.

Индикатор выполнения может показать, что для завершения передачи по сети потребуется от пары минут до часа, что зависит от размера резервной копии и скорости сетевого подключения. Если отключить устройство от сети Wi-Fi слишком рано, процесс приостановится до последующего подключения.

7. Теперь настройку можно завершить.

   Контент, такой как приложения, фото, музыка и другая информация, продолжит восстанавливаться в фоновом режиме в течение последующих нескольких часов или дней в зависимости от объема информации. Для завершения восстановления рекомендуется чаще подключать устройство к сети Wi-Fi и питанию.

После восстановления.

- Откройте библиотеку приложений и просмотрите приложения, установленные на устройстве. Любые неизвестные приложения сторонних разработчиков можно удалить. Обратитесь к разделу «Просмотр и удаление приложений на iPhone или iPad» ранее в этом документе.

  См. статью службы поддержки Apple Упорядочивание приложений на экране «Домой» и библиотеки приложений на iPhone (https://support.apple.com/108324).

- Просмотрите и удалите любые профили конфигурации устройства или профили управления мобильными устройствами (MDM), установку которых Вы не разрешали. (Учебные заведения и компании используют профили конфигурации для настройки устройств. Не удаляйте профили, установленные учебными заведениями или работодателем.) Обратитесь к разделу «Удаление подозрительного контента» ранее в этом документе.

Восстановление iPhone или iPad из резервной копии на компьютере

1. На компьютере Mac с macOS 10.15 или новее откройте Finder. На компьютере Mac с macOS 10.14 или более ранней версии либо на ПК с Windows откройте iTunes.
2. Подключите устройство к компьютеру, используя кабель USB. Если появится сообщение с запросом код-пароля устройства или сообщение «Доверять этому компьютеру», следуйте инструкциям на экране.
3. Выберите iPhone или iPad, когда он отобразится в окне Finder или iTunes.
4. Выберите «Восстановить из резервной копии».
5. Проверьте дату каждой резервной копии и выберите наиболее подходящую.
6. Нажмите «Восстановить» и дождитесь окончания восстановления. При появлении запроса введите пароль для зашифрованной резервной копии.
7. Оставьте устройство подключенным после перезагрузки и дождитесь его синхронизации с компьютером. Устройство можно будет отключить после синхронизации.

После восстановления.

- Откройте библиотеку приложений и просмотрите приложения, установленные на устройстве. Любые неизвестные приложения сторонних разработчиков можно удалить. Обратитесь к разделу «Просмотр и удаление приложений на iPhone или iPad» ранее в этом документе.

  См. статью службы поддержки Apple Упорядочивание приложений на экране «Домой» и библиотеки приложений на iPhone (https://support.apple.com/108324).

- Просмотрите и удалите любые профили конфигурации устройства или профили управления мобильными устройствами, установку которых Вы не разрешали. (Учебные заведения и компании используют профили конфигурации для настройки устройств. Не удаляйте профили, установленные учебными заведениями или работодателем.) Обратитесь к разделу «Удаление подозрительного контента с устройств» ранее в этом документе.

Восстановление объектов, сохраненных в резервной копии Time Machine на компьютере Mac

Если для резервного копирования файлов использовать Time Machine на компьютере Mac, можно с легкостью восстанавливать утраченные объекты или прошлые версии файлов. Time Machine можно использовать во многих приложениях.

1. На компьютере Mac откройте окно того объекта, который нужно восстановить.

   Например, чтобы восстановить файл, случайно удаленный из папки «Документы», откройте папку «Документы».

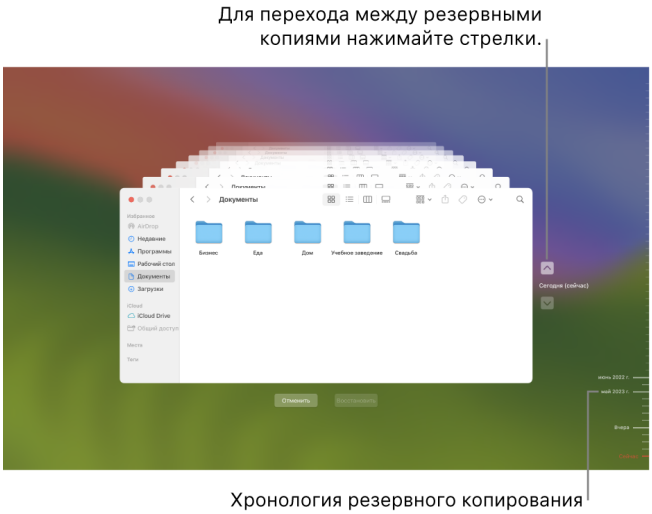
   Если нужен объект с рабочего стола, окно открывать не нужно.

2. Используйте Launchpad, чтобы просматривать и открывать приложения на компьютере Mac и открывать Time Machine. Может отобразиться сообщение, что компьютер Mac подключается к диску резервного копирования.

   Кроме того, можно открыть Time Machine, нажав значок Time Machine в строке меню, затем выбрав «Войти в Time Machine». Если в строке меню нет значка Time Machine, выполните одно из описанных ниже действий.

   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Time Machine», затем выберите «Показывать Time Machine в строке меню».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Time Machine», затем выберите «Показывать Time Machine в строке меню».

3. С помощью стрелок и временной шкалы можно перемещаться между локальными моментальными копиями и резервными копиями.



   Если отображается мигающее деление, сменяющееся полутемным серым делением, это означает, что резервная копия еще загружается или проверяется на диске резервного копирования.

4. Выберите один или несколько объектов, которые нужно восстановить (например, папки или весь диск), затем нажмите «Восстановить».

   Восстановленные объекты вернутся на прежние места. Например, если объект был в папке «Документы», он вернется в папку «Документы».

После восстановления.

- Откройте Launchpad и просмотрите приложения, установленные на компьютере Mac. Любые неизвестные приложения сторонних разработчиков можно удалить. Для этого нажмите и удерживайте клавишу Option, затем нажмите значок «X» на приложении, которое нужно удалить.
- Просмотрите и удалите любые профили конфигурации устройства или профили управления мобильными устройствами, установку которых Вы не разрешали. (Учебные заведения и компании используют профили конфигурации для настройки устройств. Не удаляйте профили, установленные учебными заведениями или работодателем.) Обратитесь к разделу «Удаление подозрительного контента с устройств» ранее в этом документе.

Инструменты обеспечения безопасности и конфиденциальности

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 на устройствах установлены актуальные версии ПО, можно узнать, как управлять учетной записью Apple ID. 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 автоматическое обновление не было включено во время первоначальной настройки устройства, это можно сделать сейчас, следуя инструкциям далее.

1. Откройте «Настройки» > «Основные» > «Обновление ПО» > «Автообновление».
2. Включите оба параметра: «Загрузка обновлений [*iOS или iPadOS*]» и «Установка обновлений [*iOS или iPadOS*]».

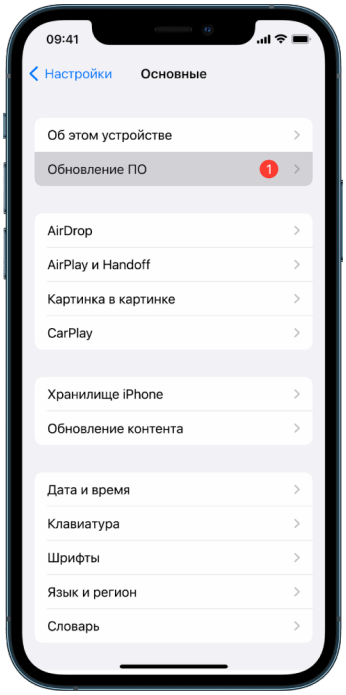
Как только обновление станет доступно, устройство загрузит и установит обновление ночью при наличии подключения к источнику питания и сети Wi-Fi. Перед установкой обновления Вы получите уведомление.

Чтобы выключить автоматическое обновление, откройте «Настройки» > «Основные» > «Обновление ПО» > «Автообновление», затем выключите оба параметра.

Обновление iPhone и 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 и 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.
   - ПК с Windows с разъемом USB и 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 ПК 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. Откройте меню Apple > «Системные настройки», нажмите «Основные», затем нажмите «Обновление ПО».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», 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. Откройте меню Apple > «Системные настройки», нажмите «Основные», затем нажмите «Обновление ПО».
  - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», 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 .

Установка уникального код-пароля или пароля на устройствах Apple

Чтобы никто, кроме Вас, не мог использовать Ваши устройства и получать доступ к Вашей информации, используйте уникальный код-пароль или пароль, известный только Вам. Если Вы используете устройство вместе с кем-то еще или если другие люди знают Ваш код-пароль или пароль, учитывайте, что они могут просмотреть информацию на Вашем устройстве или в Вашей учетной записи, а также изменить настройки устройства.

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 (где именно зависит от устройства). Пароль компьютера Mac должен содержать не менее восьми символов, включающих строчные и прописные буквы и как минимум одну цифру. Вы также можете добавить дополнительные символы и знаки пунктуации, чтобы сделать пароль еще надежнее.

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 и iPad, чтобы они были доступны только тем, кому известен код-пароль.

Примечание. Код-пароль устройства не совпадает с *паролем* Apple ID, 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 следующие 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 Apple ID, 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. Откройте меню Apple > «Системные настройки», нажмите «Основные», нажмите «Пользователи и группы» , затем нажмите кнопку информации .
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «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 выборе надежного пароля, нажмите клавишу ключа рядом с полем «Новый пароль».
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 iPhone или iPad

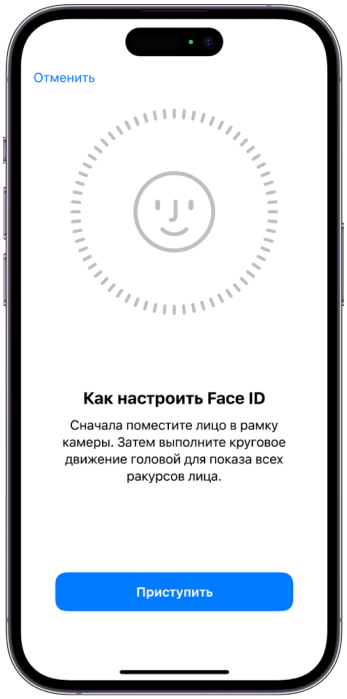
Для более надежной защиты данных Вы можете настроить устройство таким образом, чтобы оно автоматически блокировалось после определенного периода неактивности.

- Откройте «Настройки» > «Экран и яркость» > «Автоблокировка», затем укажите период времени.

Защита iPhone или iPad с помощью Face ID

Face ID создан для тех, кто хочет обеспечить дополнительный уровень защиты своего iPhone или iPad. Благодаря этой функции никто другой не может получить доступ к информации, которая хранится 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).

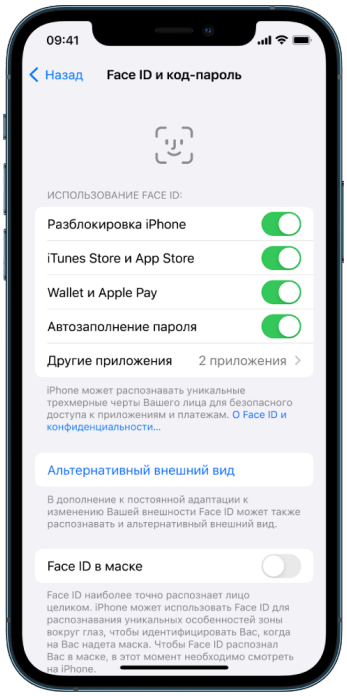


Настройка Face ID

- 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.

В случае наличия особых потребностей, связанных с физическими особенностями, можно коснуться «Параметры Универсального доступа» во время настройки Face ID. 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

Если Вы хотите перестать использовать альтернативный внешний вид или если Вы считаете, что кто-то мог добавить альтернативный внешний вид на Вашем устройстве без Вашего разрешения, Вы можете сбросить Face ID, а затем настроить его снова.

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

Защита устройств с помощью Touch ID

Используйте Touch ID, чтобы безопасно и удобно разблокировать iPhone или iPad, 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 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, что добавляли некоторые из зарегистрированных отпечатков, см. раздел Удаление неизвестных отпечатков, зарегистрированных на iPhone или iPad далее в этом документе.

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 (https://support.apple.com/101612).

Настройка Touch ID на компьютере 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. Откройте меню Apple > «Системные настройки», затем нажмите «Touch ID».
   - На Mac с macOS 12 или более ранней версии. Откройте 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 на iPhone или iPad

Если на iPhone или iPad зарегистрировано несколько отпечатков и Вы хотите обезопасить себя, чтобы никто другой не мог получить доступ к Вашему устройству с помощью зарегистрированного отпечатка, Вы можете сбросить отпечатки, чтобы на устройстве были зарегистрированы только Ваши отпечатки пальцев.

1. Откройте «Настройки» > «Touch ID и код-пароль».
2. Если доступно несколько отпечатков, поместите палец на кнопку «Домой», чтобы определить, какой это отпечаток.
3. Коснитесь отпечатка, затем выполните одно из следующих действий:
   - Введите название (например, «Большой палец»).
   - Коснитесь «Удалить отпечаток».

Добавление и удаление отпечатков на компьютере Mac

Если на компьютере Mac или клавиатуре Magic Keyboard с Touch ID зарегистрировано несколько отпечатков и Вы полагаете, что один или несколько отпечатков не принадлежат Вам, Вы можете удалить все отпечатки, а затем добавить только свои.

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

Поддержание безопасности Apple ID

Apple ID — 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. Если кто-то еще получил доступ к Вашей учетной записи Apple ID, этот человек может просматривать информацию, которая синхронизируется между устройствами и может содержать такие данные, как сообщения и геопозиция. Здесь Вы узнаете, как защитить Apple ID на iPad, iPhone и Mac.

Далее перечислены важные правила, следуя которым можно защитить свою учетную запись Apple ID и конфиденциальность.

Защита учетной записи Apple ID

1. Не делитесь своей учетной записью Apple ID ни с кем, даже членами семьи, партнерами и близкими друзьями. Если Вы делитесь учетной записью Apple ID, Вы даете другому человеку доступ к своим данным и контенту. Если кто-то другой настраивал Вашу учетную запись Apple ID и задал пароль для Вас или мог получить доступ к Вашему паролю, измените этот пароль.
2. Используйте двухфакторную аутентификацию для доступа к своей учетной записи Apple ID. 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.

   Для использования двухфакторной аутентификации необходимо иметь хотя бы один проверенный номер телефона. На этот номер будут приходить коды проверки в виде текстового сообщения или вызова.

3. Внимательно читайте уведомления об учетной записи Apple ID. Apple уведомляет Вас в электронном письме, текстовом сообщении или push-уведомлении о том, что Ваша учетная запись была изменена. Например, Вы будете уведомлены о первом входе на новом устройстве или изменении пароля. Именно поэтому важно, чтобы контактная информация была актуальной.

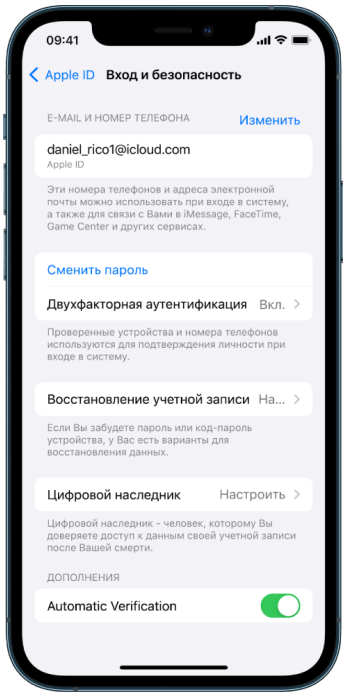
   См. раздел Блокировка чужих попыток входа ранее в этом документе.

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 в учетной записи Apple ID

Следуйте инструкциям далее, чтобы убедиться в том, что личная информация, связанная с Вашей учетной записью Apple ID, принадлежит Вам.

1. Выполните одно из описанных ниже действий.
   - *На iPhone или iPad.* Откройте «Настройки» > [*Ваше имя*].
   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», затем нажмите «Apple ID».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», затем нажмите «Apple ID».
   - *В веб-браузере на Mac или ПК с Windows.* Посетите веб-сайт Apple ID (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, следуйте указаниям в следующем разделе, чтобы удалить их.
   - Если двухфакторная аутентификация не настроена, см. раздел Использование двухфакторной аутентификации далее в этом документе.

Защита учетной записи и удаление неизвестных устройств

Если Вам незнакомы какие-то устройства, которые подключены к Вашей учетной записи Apple ID, или если Вы не разрешали использовать свою учетную запись, ее 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 инструкциям далее, чтобы просмотреть информацию в своей учетной записи и защитить ее.

1. Изменение пароля.
   - *На iPhone или iPad.* Откройте «Настройки» > [*Ваше имя*] > «Пароль 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. Откройте меню Apple > «Системные настройки», затем нажмите «Apple ID» > «Пароль 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 12 или более ранней версии. Откройте меню Apple > «Системные настройки», затем нажмите «Apple ID» > «Пароль и безопасность» > «Изменить пароль». Создайте надежный пароль (он должен содержать не менее восьми символов, включая строчные и прописные буквы и как минимум одну цифру).
   - Чтобы удалить устройства, которые подключены к Вашей учетной записи, откройте «Настройки» > «Apple ID». Прокрутите вниз до списка устройств, коснитесь устройства, которое нужно удалить, затем коснитесь «Удалить из учетной записи».
2. Чтобы в качестве меры предосторожности изменить адрес электронной почты, связанный с Вашей учетной записью Apple ID, откройте Safari и войдите в свою учетную запись на веб-сайте Apple ID (https://appleid.apple.com). Выберите «Учетная запись», под своей текущей учетной записью Apple ID выберите «Сменить Apple ID», 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. Откройте меню Apple > «Системные настройки», нажмите «Apple ID» , прокрутите вниз до списка устройств, выберите устройство, которое нужно удалить, затем нажмите «Удалить из учетной записи».
    - На Mac с macOS 12 или более ранней версии. Откройте 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 Вашей учетной записи Apple ID. 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. Откройте «Настройки» > [*Ваше имя*] > «Пароль 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?».

   Запрос кода проверки снова отобразится на iPhone только в том случае, если Вы полностью выйдете из своей учетной записи, сотрете iPhone, войдете в свою учетную запись Apple ID в браузере или поменяете пароль учетной записи Apple ID из соображений безопасности.

После включения двухфакторной аутентификации у Вас будет две недели на то, чтобы выключить ее, если Вы передумаете. По истечении этого периода выключить двухфакторную аутентификацию не получится. 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. Откройте меню Apple > «Системные настройки», нажмите «Apple ID» , затем в боковом меню выберите «Пароль и безопасность».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Apple ID» , затем выберите «Пароль 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. Запрос кода проверки снова отобразится на Mac только в том случае, если Вы полностью выйдете из своей учетной записи Apple ID, сотрете Mac или поменяете пароль из соображений безопасности.

Ключи безопасности для Apple ID

Ключ безопасности — это компактное внешнее устройство, которое выглядит как флеш-накопитель или тег и которое можно использовать для подтверждения входа с Вашим Apple ID при использовании двухфакторной аутентификации. Ключи безопасности для Apple ID — это дополнительная расширенная функция безопасности, разработанная специально для пользователей, которым необходима более надежная защита от преступных действий в их отношении, включая фишинг и мошенничество 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.

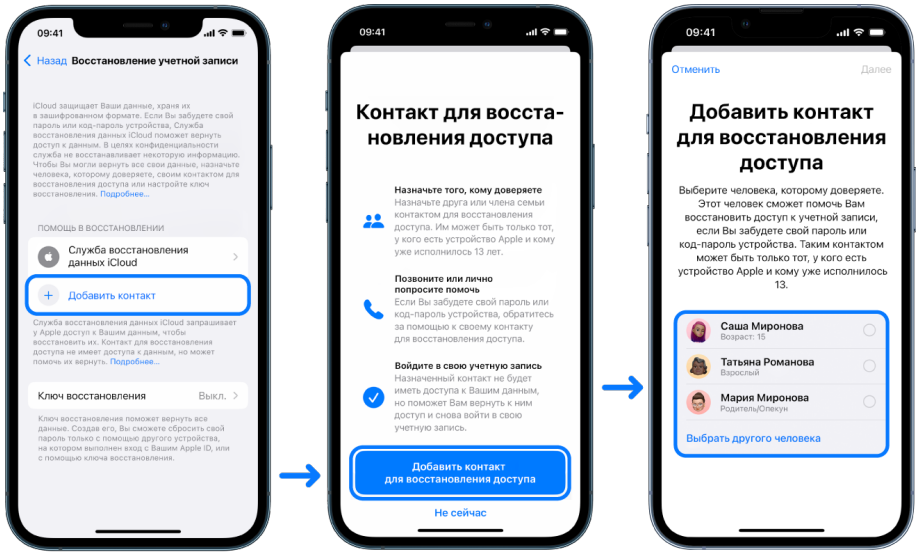
Подробнее о ключах безопасности см. в статье службы поддержки Apple Сведения о ключах безопасности для идентификатора Apple ID (https://support.apple.com/HT213154).

Предотвращение блокировки доступа к Вашему устройству Apple

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 передачи доступа к данным Вашей учетной записи Apple после Вашей смерти. Обратитесь к статье службы поддержки Apple Как добавить цифрового наследника для вашего идентификатора Apple ID (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 своей учетной записи Apple ID и код-пароль на своем устройстве.



Назначение контакта для восстановления доступа к учетной записи

Если Вы полагаете, что кто-то может получить доступ к Вашей учетной записи, чтобы 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.* Откройте «Настройки» > [*Ваше имя*], затем коснитесь «Пароль и безопасность».
   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Apple ID», затем в боковом меню выберите «Пароль и безопасность».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Apple ID», затем выберите «Пароль 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 примут, Вы увидите сообщение о том, что этот человек был добавлен в качестве Вашего контакта 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*. Откройте «Настройки» > [*Ваше имя*], затем коснитесь «Пароль и безопасность».
   - На Mac с macOS 13 или новее. Откройте меню Apple > «Системные настройки», нажмите «Apple ID», затем в боковом меню выберите «Пароль и безопасность».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», нажмите «Apple ID», затем выберите «Пароль 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.

Защита паролей устройства, приложений и веб-сайтов на iPhone и iPad

Для управления паролями на iPhone или iPad 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 веб-сайту или платформе, на которых они сохранены.

Управление паролями

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.

Использование функции «Рекомендации по безопасности паролей»

Если Вы придумываете и сохраняете собственные пароли для веб-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.

Включение функции выявления украденных паролей

iPhone и iPad (с iOS 17, iPadOS 17 или новее) могут следить за Вашими паролями и предупреждать Вас, если они обнаружены в известных утечках данных.

- Откройте «Настройки» > «Пароли» > «Рекомендации по безопасности» и включите параметр «Выявление украденных паролей».

Автоматические удаление одноразовых кодов проверки

В iOS 17, iPadOS 17 и macOS Sonoma 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.* Откройте «Настройки» > «Пароли», выберите «Параметры паролей» и включите параметр «Автоматическая очистка».
    - *На Mac.* Откройте меню Apple > «Системные настройки» > «Пароли» в боковом меню, выберите «Параметры паролей» и включите параметр «Автоматическая очистка».

Управление общими паролями и ключами входа

В iOS 17, iPadOS 17 и macOS Sonoma 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 macOS.

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.* Откройте меню Apple > «Системные настройки» > «Пароли» в боковом меню, 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.* Откройте меню Apple > «Системные настройки» > «Пароли» в боковом меню, 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.* Откройте «Настройки» > «Пароли», найдите группу с общими паролями, выберите эту группу и удалите себя из группы.
  - *На Mac.* Откройте меню Apple > «Системные настройки» > «Пароли» в боковом меню, 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 macOS (https://support.apple.com/guide/mac-help/mchlee73013a).

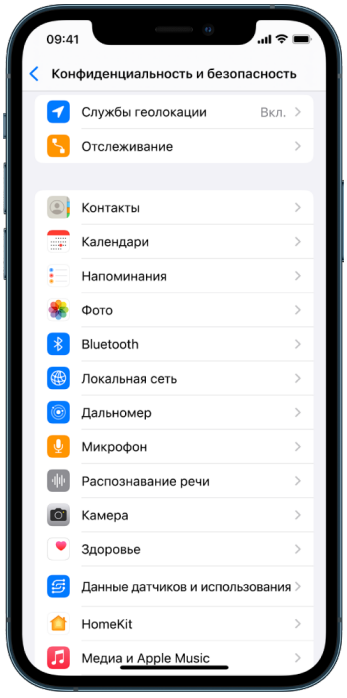
- Выполните одно из описанных ниже действий.
  - *На iPhone или iPad.* Откройте «Настройки» > «Пароли» в боковом меню, найдите группу с общими паролями, выберите эту группу и посмотрите, являетесь ли Вы ее владельцем или участником.
  - *На Mac.* Откройте меню Apple > «Системные настройки», нажмите «Пароли» в боковом меню, нажмите кнопку информации 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».

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. Если кто-то настраивал Ваше устройство или мог получить к нему доступ, зная Ваш пароль, это причина, по которой 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. Откройте меню Apple > «Системные настройки» в боковом меню выберите «Пароль и безопасность» , затем нажмите «Конфиденциальность».
   - На Mac с macOS 12 или более ранней версии. Откройте меню Apple > «Системные настройки», выберите «Пароль 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 встроенные приложения. 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».
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.

Защита устройств от узконацеленного шпионского ПО 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 можете подвергнуться высокотехнологичной кибератаке, например со стороны частной компании, которая разрабатывает спонсируемое государством узконацеленное шпионское ПО.

Примечание. Большинство людей никогда не становятся целью таких атак.

Когда устройство находится в режиме блокировки, функциональность устройства меняется. Работа приложений, веб-сайтов и функций строго ограничена в целях безопасности, а некоторые возможности полностью недоступны. Режим блокировки включает следующие 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 он также будет активирован 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.* Откройте меню Apple > «Системные настройки» > «Конфиденциальность и безопасность» > «Режим блокировки», коснитесь «Включить», затем введите пароль (если потребуется) и коснитесь «Включить и перезагрузить».

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 «Сообщения», выберите «Сообщения» > «Настройки», нажмите «iMessage», затем нажмите «Выйти». Подтвердите действие, затем снова нажмите «Выйти».
- На Mac с macOS 12 или более ранней версии. Откройте «Сообщения», выберите «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», откройте «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», откройте «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 «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 «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.

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.

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 той же учетной записью Apple ID.

Важно! Заблокированный пользователь не получит уведомление о блокировке, а Вы по-прежнему сможете вызывать его и отправлять ему сообщения и электронные письма, оставив блокировку. 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 кнопки информации ⓘ 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 кнопки информации ⓘ 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 кнопки информации ⓘ, 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 следующих 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 вызовов 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».

Получение предупреждений о нецензурных или неприемлемых фото и видео на iPhone, iPad и Mac

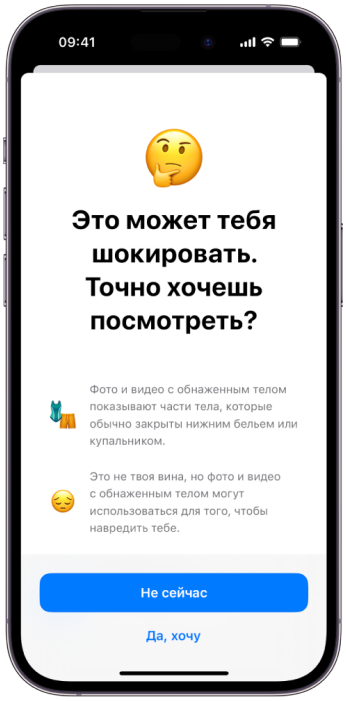
Функция «Предупреждение о нецензурном или неприемлемом контенте» помогает взрослым пользователям избегать просмотра нежелательных изображений и видео с обнаженным телом, полученных в Сообщениях, по AirDrop, в видеосообщениях FaceTime и в постерах контактов через приложение «Телефон». Эта функция задействует 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. Откройте меню Apple, нажмите «Системные настройки», нажмите «Конфиденциальность и безопасность», затем нажмите «Предупреждение об откровенном контенте».

- На Mac с macOS 12 или более ранней версии. Откройте 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.

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 Sonoma 14, Safari блокирует вкладки в режиме «Частный доступ» после определенного периода неактивности. Для повторного открытия вкладок требуется 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.

В этом документе Вы можете узнать о том, как открыть окно в режиме «Частный доступ» на iPhone, iPad или Mac

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 веб-сайтов
- Недавние запросы
- Значки веб-страниц
- Снимки экрана, сохраненные на открытых веб-страницах
- Список загруженных объектов (загруженные файлы не удаляются)
- Веб-сайты, добавленные для функции «Поиск веб-сайтов»
- Веб-сайты, запросившие доступ к использованию геопозиции
- Веб-сайты, запросившие доступ на отправку Вам уведомлений

Очистка недавних маршрутов и избранного в приложении «Карты» на iPhone и 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, или коснитесь «Изменить» и затем коснитесь кнопки «Удалить», 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 кнопки «Вкладки».
3. Коснитесь кнопки «Группы вкладок» внизу по центру панели вкладок, 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-сайты и выйти из режима «Частный доступ», коснитесь кнопки «Вкладки», затем коснитесь кнопки «Группы вкладок», чтобы открыть другую группу вкладок из меню внизу экрана. Веб-сайты с частным доступом отобразятся снова при переходе в режим «Частный доступ».

Чтобы закрыть частные вкладки, коснитесь кнопки «Вкладки», затем смахните влево по каждой вкладке, которую нужно закрыть.

Открытие окна в режиме «Частный доступ» на iPad

- В Safari коснитесь кнопки «Показать боковое меню», затем коснитесь «Частный».

  Если включен режим «Частный доступ», фон поля поиска будет черным, а не белым, и посещаемые веб-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 веб-сайты и выйти из режима «Частный доступ», коснитесь кнопки «Показать боковое меню», затем переключитесь на 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.

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

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 кнопки добавления, чтобы добавить контакт на случай ЧП (в качестве контакта на случай ЧП нельзя добавить экстренные службы).
   - *Удаление контакта.* Коснитесь кнопки удаления 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, 911 в США) и коснитесь кнопки вызова.

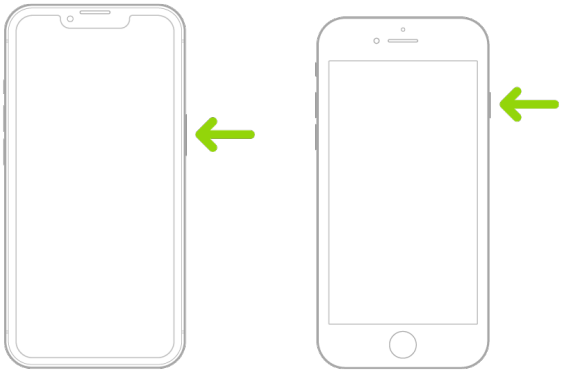
Использование функции «Экстренный вызов — SOS» на iPhone (во всех странах и регионах, кроме Индии)

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 документе.

- 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 «Отправить».

   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 кнопки цифровой панели, введите 911 и коснитесь «OK».
4. Коснитесь «Создать сообщение» и выберите SMS.
5. Напишите сообщение пальцем, коснитесь кнопки микрофона 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).

Важная информация об экстренных вызовах на iPhone

- Некоторые сотовые сети могут не принимать экстренный вызов с iPhone, если iPhone не активирован, несовместим с сотовой сетью, настроен для работы в определенной сотовой сети, не имеет SIM-карты (в использующих ее сетях) или SIM-карта защищена PIN-кодом.
- В некоторых странах или регионах, когда Вы совершаете экстренный вызов, экстренным службам может быть доступна информация о Вашей геопозиции (если она может быть определена).
- Изучите информацию об экстренных вызовах у Вашего оператора, чтобы понять, какие ограничения имеются при вызове экстренных служб по Wi-Fi.
- В сети CDMA после завершения экстренного вызова iPhone на несколько минут переходит в *режим экстренного вызова*, чтобы экстренные службы могли на него перезвонить. В это время передача данных и текстовых сообщений заблокированы.
- После совершения экстренного вызова могут быть на короткое время выключены некоторые функции, которые блокируют или заглушают входящие вызовы, чтобы экстренные службы могли Вам перезвонить. Сюда входят функции «Не беспокоить», «Заглушение неизвестных» и «Экранное время».
- Если на iPhone с двумя SIM-картами (iPhone SE 2-го поколения или новее, а также модели iPhone X или новее) не включены «Вызовы по Wi-Fi» для определенной линии, любые входящие телефонные вызовы по этой линии (в том числе вызовы от экстренных служб) во время использования другой линии будут направляться напрямую на автоответчик (если он предоставляется Вашим оператором); Вы не будете получать уведомления о пропущенных вызовах.

  Если настроить условную переадресацию вызовов (если она предоставляется Вашим оператором) с одной линии на другую, когда линия занята или не обслуживается, вызовы не будут направляться на автоответчик; за информацией о настройке обращайтесь к оператору.

Получение доказательств, связанных с учетной записью другого лица

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 следующих 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)

Авторские права

Использование «клавиатурного» логотипа Apple (Option-Shift-K) в коммерческих целях без предварительного письменного согласия Apple может являться посягательством на права владельца товарного знака и проявлением недобросовестной конкуренции, нарушающим государственные и местные законы.

Apple, логотип Apple, AirDrop, AirPods, AirTag, Apple Books, Apple Music, Apple Pay, Apple TV, Apple Watch, Digital Crown, Face ID, FaceTime, FileVault, Finder, Find My, HomeKit, HomePod, iMac, iMessage, iPad, iPadOS, iPad Pro, iPhone, iTunes, Launchpad, Lightning, Mac, MacBook Air, MacBook Pro, macOS, Magic Keyboard, OS X, Safari, Siri, Time Machine и Touch ID являются товарными знаками Apple Inc., зарегистрированными в США и других странах и регионах.

App Store, iCloud и iTunes Store являются знаками обслуживания Apple Inc., зарегистрированными в США и других странах и регионах.

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

IOS является товарным знаком или зарегистрированным товарным знаком Cisco в США и других странах и используется по лицензии.

Словесный товарный знак и логотипы Bluetooth® являются зарегистрированными товарными знаками Bluetooth SIG, Inc. и используются компанией Apple по лицензии.

Названия других компаний и продуктов, упомянутые здесь, могут являться товарными знаками соответствующих компаний.

При создании этого руководства были приложены все усилия, чтобы информация в нем была точной. Apple не несет ответственности за допущенные при обработке информации ошибки и опечатки.

Некоторые приложения доступны не везде. Доступность приложений может меняться.

RS028-00788