Центр сертификации безопасности и соответствия требованиям

Декабрь 2021 г.

Содержание

Обзор гарантий компании Apple в отношении безопасности

В рамках своих обязательств по обеспечению безопасности компания Apple регулярно обращается в сторонние организации для сертификации и подтверждения безопасности устройств, программного обеспечения и сервисов Apple. Признанные на международном уровне организации предоставляют Apple сертификаты в отношении каждого основного выпуска операционных систем. Таким образом они обеспечивают гарантию безопасности, то есть определенную степень уверенности в том, что потребности системы в области безопасности удовлетворены. В тех технических областях, где не приняты соглашения о взаимном признании (MRA) или отсутствуют тщательно проработанные стандарты сертификации в области безопасности, компания Apple участвует в разработке соответствующих стандартов безопасности. Наша цель заключается в создании общепринятой исчерпывающей системы сертификации для всех устройств, операционных систем, приложений и сервисов компании Apple.

Часто сертификация необходима для соответствия требованиям законодательства, нормативных актов и производственных норм. Такие сервисы, как Apple School Manager и Apple Business Manager —, сертифицируются компанией Apple по стандартам ISO/IEC 27001 и ISO/IEC 27018. Все клиенты, включая государственные органы, предприятия и образовательные организации, развертывающие устройства Apple, могут использовать сертификаты устройств, операционных систем, программного обеспечения и сервисов для подтверждения соответствия требованиям.

Сертификация устройств

Поскольку программное обеспечение не может быть безопасным без надежного фундамента, предоставляемого аппаратным обеспечением, все устройства Apple — с iOS, iPadOS, macOS, tvOS и watchOS — имеют встроенные в микросхему функции безопасности. К этим функциям относится центральный процессор, обеспечивающий работу функций безопасности системы, и выделенный чип, который отвечает только за функции, связанные с безопасностью. Самым важным компонентом является сопроцессор Secure Enclave, которым оснащены все современные устройства iOS, iPadOS, watchOS и tvOS, а также все компьютеры Mac с чипом Apple и компьютеры Mac с процессором Intel и чипом безопасности Apple T2. Secure Enclave предоставляет фундамент для шифрования хранящихся на устройстве данных, безопасной загрузки macOS и работы биометрических систем.

Для предоставления гарантий безопасности компания Apple сертифицирует фундаментальные компоненты безопасности в чипе: аппаратный корень доверия, обеспечение безопасной загрузки, безопасное хранилище ключей Secure Enclave и безопасную аутентификацию с помощью Touch ID и Face ID. Своим существованием функции безопасности устройств Apple обязаны уникальному сочетанию микросхем, оборудования, программного обеспечения и сервисов, которое предлагает только компания Apple. Сертификация этих компонентов является важной частью гарантий, предоставляемых Apple.

Сведения об открытой сертификации устройств и соответствующих компонентов прошивки доступны в следующих разделах.

- Сертификация безопасности для чипа безопасности Apple T2
- Сертификация безопасности для процессора Secure Enclave

Сертификация программного обеспечения и приложений

Apple обращается за независимой сертификацией и аттестацией своих операционных систем и приложений: криптографические модули проверяются на соответствие Федеральным стандартам обработки информации США (FIPS) 140-2/-3, а операционные системы, приложения и службы — стандарту оценки по общим критериям. Сертификация проводится для следующих операционных систем: iOS, iPadOS, macOS, sepOS, прошивка T2, tvOS и watchOS. Первыми приложениями, прошедшими независимую сертификацию, станут браузер Safari и приложение «Контакты», в будущем сертификация будет расширена на другие приложения.

Сведения об открытой сертификации *операционных систем* Apple доступны по ссылкам ниже.

- Сертификация безопасности для iOS
- Сертификация безопасности для iPadOS
- Сертификация безопасности для macOS
- Сертификация безопасности для tvOS
- Сертификация безопасности для watchOS

Сведения об открытой сертификации *приложений* Apple доступны по ссылкам ниже.

- Сертификация безопасности для приложений Apple

Сертификация сервисов

Apple проводит сертификацию безопасности для поддержки корпоративных клиентов и образовательных организаций. Благодаря этой сертификации клиенты Apple могут выполнять свои законодательные и контрактные обязательства при использовании сервисов Apple с аппаратным и программным обеспечением Apple. Сертификация позволяет пользователям получить независимую оценку практик компании Apple в области информационной безопасности, охраны окружающей среды и конфиденциальности относительно систем Apple.

Сведения об открытой сертификации *интернет-сервисов* Apple доступны по ссылкам ниже.

- Сертификация безопасности для интернет-сервисов Apple

Вы можете задать вопросы касательно сертификации Apple в области безопасности и конфиденциальности, отправив электронное письмо по адресу security-certifications@apple.com.

Сертификация безопасности оборудования

Обзор сертификации безопасности оборудования Apple

Apple сертифицирует sepOS и прошивку T2 на соответствие Федеральному стандарту обработки информации США (FIPS) 140-2/-3 и другим стандартам. В основе этого процесса лежат *ключевые аспекты сертификации*, которые широко применяются к разным платформам (насколько это возможно). Одним из аспектов является проверка библиотеки corecrypto, которая используется при развертывании программных и аппаратных криптографических модулей в операционных системах Apple. Второй ключевой аспект — сертификация процессора Secure Enclave, который встроен во многие устройства Apple. Третьим аспектом является сертификация чипа Secure Element (SE), который встроен в устройства Apple с Touch ID и устройства с Face ID. Эти ключевые аспекты сертификации аппаратных компонентов составляют основу для более обширной сертификации платформ в области безопасности.

Проверка криптографических модулей

Подтверждение правильности реализации различных криптографических алгоритмов и связанных функций безопасности является необходимым условием для прохождения проверки на соответствие стандарту FIPS 140-3 и помогает в получении других сертификатов. Проверка проводится в соответствии с программой проверки криптографических алгоритмов (CAVP) Национального института стандартов и технологий (NIST). Сертификаты проверки реализаций Apple можно найти с помощью функции поиска CAVP. Дополнительная информация приведена на веб-сайте программы проверки криптографических алгоритмов (CAVP).

Проверка криптографических модулей: FIPS 140-2/3 (ISO/IEC 19790)

Криптографические модули Apple неоднократно проверялись по программе проверки криптографических модулей (CMVP) на соответствие Федеральному стандарту обработки информации США (FIPS) 140-2 для криптографических модулей. Эти проверки проводятся при выпуске каждого крупного обновления ОС начиная с 2012 г. Apple отправляет криптографические модули в CMVP для проверки на соответствие стандарту после выхода каждого основного выпуска. Помимо использования в операционных системах и приложениях Apple, эти модули выполняют криптографические операции для сервисов Apple и могут использоваться приложениями сторонних разработчиков.

Компания Apple каждый год успешно проходит проверку. **Уровень безопасности 1** присваивается следующим программным модулям: модуль Corecrypto для устройств с процессорами Intel и модуль Corecrypto Kernel для устройств с процессорами Intel (для macOS). Для чипа Apple: модуль Corecrypto для устройств с процессорами ARM и модуль Corecrypto Kernel для устройств с процессорами ARM (для iOS, iPadOS, tvOS, watchOS и для прошивки чипа безопасности Apple T2, встроенного в компьютеры Mac).

В 2019 г. встроенный аппаратный криптографический модуль безопасного хранилища ключей Apple Corecrypto прошел первую проверку на соответствие **уровню безопасности 2** по стандарту FIPS 140-2, что позволяет одобренное правительством США использование ключей, которые генерирует и которыми управляет Secure Enclave. Apple продолжает деятельность по проверке аппаратного криптографического модуля для каждого последующего крупного выпуска операционной системы.

Стандарт **FIPS 140-3** был утвержден Министерством торговли США в 2019 г. Самым заметным изменением в этой версии стандарта является спецификация стандартов ISO/IEC, в частности ISO/IEC 19790:2015 и соответствующего стандарта тестирования ISO/IEC 24759:2017. В рамках CMVP была инициирована программа перехода, согласно которой с 2020 г. проверка криптографических модулей будет проводиться в соответствии со стандартом FIPS 140-3. Цель компании Apple — привести криптографические модули в соответствие со стандартом FIPS 140-3 в кратчайшие сроки и таким образом завершить переход на новый стандарт сертификации.

В отношении тех криптографических модулей, которые в настоящий момент проходят проверку и тестирование, программа CMVP предусматривает два отдельных списка, которые могут содержать информацию о предлагаемых проверках. В случае тестирования в аккредитованной лаборатории криптографический модуль может быть включен в список компонентов, переданных на тестирование. После того как лаборатория завершает тестирование криптографических модулей Apple и рекомендует их проверку по программе CMVP, они появляются в списке проверяемых модулей. В настоящее время лабораторные испытания завершены и ожидается тестирование по программе CMVP. Поскольку продолжительность процесса оценки может варьироваться, для определения текущего статуса криптографических модулей Apple в период между датой основного выпуска операционной системы и выпуском сертификата следует проверять оба упомянутых выше списка.

Сертификация продукции: общие критерии (ISO/IEC 15408)

Общие критерии (ISO/IEC 15408) — это стандарт, который используют многие организации для оценки безопасности ИТ-продуктов.

Дополнительная информация о сертификации, которая признана участниками Соглашения о признании общих критериев (CCRA), доступна на портале общих критериев. Стандарт оценки по общим критериям также может использоваться в рамках государственных и частных схем проверки, а не только участниками Соглашения о признании общих критериев. В Европе взаимное признание регулируется соглашением SOG-IS, а также CCRA.

Как следует из заявления сообщества оценки по общим критериям, цель состоит в том, чтобы создать пакет международных стандартов в области безопасности, которые позволят прозрачно и достоверно оценивать функции безопасности в сфере информационных технологий. Сертификация по общим критериям предполагает независимую оценку соответствия продукта стандартам безопасности. Таким образом, покупатели могут принять информированное решение, получив представление о том, какой уровень безопасности обеспечивает тот или иной продукт в сфере информационных технологий.

Вступив в CCRA, страны-участницы договорились признавать сертификацию продуктов в сфере информационных технологий с одинаковым уровнем доверия. Для сертификации требуется обширная оценка, включая:

- профили защиты (PP);
- задания по безопасности (ST);
- функциональные требования к безопасности (SFR);
- требования к гарантиям безопасности (SAR);
- уровни гарантии оценки (EAL).

Профили защиты (PP) являются документами, в которых указаны требования к безопасности для классов типов устройств, таких как «Мобильность». Они используются для сравнения оценок безопасности ИТ-продуктов одного и того же класса. Количество членов CCRA, участвующих в разработке постоянно увеличивающегося количества профилей защиты и расширении сферы их применения, продолжает расти с каждым годом. В соответствии с принятым соглашением каждый разработчик может обратиться за сертификатом по любой из схем утверждения сертификатов, и этот сертификат будет признан всеми подписавшими сторонами.

Задания по безопасности (ST) определяют, *какие характеристики* будут оцениваться при сертификации ИТ-продукта. Задания по безопасности преобразуются в более конкретные *функциональные требования к безопасности (SFR)*, используемые для более детальной оценки заданий по безопасности.

Общие критерии (CC) также включают *требования к гарантиям безопасности*. Одним из часто определяемых показателей является *уровень гарантии оценки (EAL)*. Уровни гарантии оценки объединяют часто встречающиеся наборы требований к гарантиям безопасности и могут быть приведены в профилях защиты или заданиях по безопасности для обеспечения сопоставимости.

Многие использовавшиеся ранее профили защиты были отправлены в архив и по мере разработки замещаются узкоспециализированными профилями защиты, которые предназначены для отдельных решений и сред. Для обеспечения признания со стороны всех членов CCRA были основаны международные технические сообщества (iTC). В конечном итоге целью является разработка и поддержка совместных профилей защиты (cPP), которые с самого начала разрабатываются с учетом схем, используемых участниками CCRA. Профили защиты, предназначенные для групп пользователей и соглашений о взаимном признании, отличных от CCRA, по-прежнему разрабатываются соответствующими заинтересованными сторонами.

Компания Apple обращается за сертификацией в соответствии с новым CCRA на основе определенных совместных профилей защиты с начала 2015 г. С тех пор компания Apple получает сертификаты оценки по общим критериям для каждого основного выпуска iOS, а также запрашивает оценку на основе новых профилей защиты.

Apple активно участвует в работе международных технических сообществ, которые занимаются оценкой технологий в области безопасности мобильных устройств. К таким сообществам относятся международные технические сообщества, отвечающие за разработку и обновление совместных профилей защиты. Apple продолжает деятельность, направленную на оценку и получение соответствующих сертификатов на основе текущих профилей защиты и совместных профилей защиты.

Сертификация платформ компании Apple для североамериканского рынка, как правило, выполняется при участии Национального партнерства по обеспечению достоверности информации (NIAP), которое ведет список проектов, проходящих проверку, но пока не являющихся сертифицированными.

В дополнение к сертификатам основных платформ список включает прочие сертификаты, которые предназначены для подтверждения выполнения требований определенных рынков.

Сертификация безопасности для процессора Secure Enclave

Вводная информация о сертификации Secure Enclave

Аппаратный криптографический модуль — *криптографический модуль безопасного хранилища ключей Apple SEP* — встроен в систему на кристалле Apple SOC, которая используется в следующих продуктах: серия Apple A для iPhone и iPad, серия M для компьютеров Mac с чипом Apple, серия S для Apple Watch и чип безопасности серии T, используемый в компьютерах Mac начиная с iMac Pro, представленного в 2017 г.

В 2018 г. компания Apple согласовала проверку программных криптографических модулей с операционными системами, выпущенными в 2017 г. (iOS 11, macOS 10.13, tvOS 11 и watchOS 4). Было впервые подтверждено соответствие аппаратного криптографического модуля SEP (криптографического модуля безопасного хранилища ключей Apple SEP версии 1.0) требованиям уровня безопасности 1 по стандарту FIPS 140-2.

В 2019 г. компания Apple подтвердила соответствие аппаратного модуля требованиям уровня безопасности 2 по стандарту FIPS 140-2 и обновила идентификатор версии модуля до 9.0, чтобы согласовать его с версиями соответствующих проверок модулей Corecrypto User и Corecrypto Kernel. В 2019 г. сюда входили iOS 12, macOS 10.14, tvOS 12 и watchOS 5.

В 2020 и 2021 годах Apple выполняла проверку на соответствие стандарту FIPS 140-3, а также дополнительную деятельность в отношении гарантий безопасности с подтверждением уровня безопасности 3 согласно требованиям к физической безопасности следующих чипов Apple: чипы A13, A14, S6 и M1.

Apple также активно участвует в проверке модулей Corecrypto User и Corecrypto Kernel для каждого основного выпуска операционных систем. Проверка на соответствие может быть выполнена только для окончательной версии.

Статус проверки криптографических модулей

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей. В списке проверяемых модулей отображается статус проверки по программе CMVP. Это может быть один из четырех этапов, которые перечислены далее.
  - *Ожидается проверка*. Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка*. Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование*. Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение*. Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для FIPS 140-3.

Сертификаты FIPS 140-3

Текущий статус

В следующей таблице показаны криптографические модули за 2020 г. и 2021 г., которые в настоящее время проходят лабораторное тестирование на соответствие стандарту FIPS 140-3.

Безопасное хранилище ключей для выпусков операционных систем 2020 и 2021 года прошло лабораторное тестирование и было рекомендовано лабораторией для проверки по программе CMVP. Оно содержится в списке проверяемых модулей и после проверки будет перенесено в список проверенных криптографических модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей iOS 15 (2021 г.) проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sep OS, распространяемая с iOS, iPadOS, macOS, tvOS и watchOS, выпущенными в 2021 году *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14, T2, M1, S3-S6) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sep OS, распространяемая с iOS, iPadOS, macOS, tvOS и watchOS, выпущенными в 2021 году *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A13, A14, S6, M1) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sep OS, распространяемая с iOS, iPadOS, macOS, tvOS и watchOS, выпущенными в 2020 году *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14, T2, M1, S3-S6) *Уровень общей безопасности:* 2

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с iOS, iPadOS, macOS, tvOS и watchOS, выпущенными в 2020 году *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A13, A14, S6, M1) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Сертификаты FIPS 140-2

В таблице ниже показаны криптографические модули, которые прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 05.02.2021	*Сертификаты:* 3811 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 10.0 *Операционная система:* sepOS для macOS 10.15 Catalina *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2018 *Даты проверок:* 10.09.2019	*Сертификаты:* 3523 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 9.0 *Операционная система:* sepOS для macOS 10.14 Mojave *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2017 *Даты проверок:* 10.09.2019	*Сертификаты:* 3223 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 1.0 *Операционная система:* sepOS для macOS 10.13 High Sierra *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Сертификация по общим критериям (CC)

Apple активно участвует в сертификации по общим критериям, если соответствующие профили защиты подходят для оценки функций безопасности, обеспечиваемых технологиями Apple.

Статус сертификации по общим критериям (CC)

За управление схемой США отвечает Национальное партнерство по обеспечению достоверности информации (NIAP), которое ведет список продуктов, проходящих проверку. Этот список включает продукты, которые в настоящее время проходят оценку в США в одобренной NIAP лаборатории тестирования по общим критериям (CCTL) и по которым было проведено вводное совещание (или его аналог), во время которого руководство CCEVS официально приняло продукт для оценки.

После сертификации продуктов NIAP вносит текущие действующие сертификаты в список совместимых продуктов. Через 2 года эти сертификаты проверяются на соответствие текущей политике поддержания гарантий безопасности. По истечении срока поддержания гарантий безопасности NIAP перемещает список сертификатов в список архивных продуктов.

На портале общих критериев перечислены сертификаты, которые признаны участниками Соглашения о признании общих критериев (CCRA). Портал общих критериев может поддерживать продукты в списке сертифицированных продуктов в течение 5 лет и сохраняет записи для архивных сертификатов.

В таблице ниже показаны сертификаты, которые в настоящее время проходят проверку в лаборатории или которые были сертифицированы как соответствующие общим критериям.

Операционная система/дата сертификации	**Идентификатор схемы/ документы**	**Название/профили защиты**
Операционная система: sepOS *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple Secure Enclave [2020 г.] *Профили защиты:* CPP_DSC_V1.0 *Аппаратное обеспечение:* Secure Enclave для (A9-A14, M1, T2, S3-S6) *Программное обеспечение:* sep OS, распространяемая с iOS 14, iPadOS 14, macOS 11 Big Sur, tvOS 14, watchOS 7

Дополнительные сертификаты

В таблице ниже показаны сертификаты для Secure Enclave, которые не используют ни стандарты оценки по общим критериям, ни FIPS 140-3.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* с 07.12.2019 г. по 26.12.2022 г.	*Сертификаты:* CFNR201902910002 (KHP: Технологическая сертификация мобильного финансового сервиса) Версия на китайском языке Версия на английском языке	*Название:* Доверенная среда исполнения мобильного терминала *Операционная система:* iOS 13.5.1 *Спецификация:* JR/T 0156-2017

Сертификация безопасности для чипа безопасности Apple T2

Вводная информация о проверке криптографических модулей

Apple активно участвует в проверке встроенных программных и аппаратных модулей Apple для каждого основного выпуска операционных систем. Проверка на соответствие может быть выполнена только для окончательной версии модуля.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для Федерального стандарта обработки информации США (FIPS) 140-3.

Помимо центрального процессора Intel, в большинстве компьютеров Mac начиная с 2017 г. также имеется отдельный чип безопасности Apple T2, который представляет собой систему на кристалле (SoC) Apple. Эти компьютеры Mac с чипом T2 используют все пять криптографических модулей для работы различных служб на устройстве:

- модуль Corecrypto User для процессоров Intel (используется в macOS на компьютерах Mac с процессором Intel);
- модуль Corecrypto Kernel для процессоров Intel (используется в macOS на компьютерах Mac с процессором Intel);
- модуль Corecrypto User для устройств с процессорами ARM (используется чипом T2);
- модуль Corecrypto Kernel для устройств с процессорами ARM (используется чипом T2);
- криптографический модуль безопасного хранилища ключей (используется сопроцессором Secure Enclave, который встроен в чип T2).

Примечание. В чипе T2 используются такие же модули Apple, как и в других чипах Apple, таких как Apple серии A, серии S и серии M.

Статус проверки криптографических модулей

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей (MIP). В списке проверяемых модулей отображается статус проверки по CMVP. Это может быть один из четырех этапов:
  - *Ожидается проверка*. Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка*. Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование*. Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение*. Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

Сертификаты FIPS 140-3

Текущий статус

Модули 2020 г. пространства пользователя, пространства ядра и безопасного хранилища ключей прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей модулей 2021 г. проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* sepOS для macOS 12 Monterey *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* sepOS для macOS 12 Monterey *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* sepOS для macOS 12 Monterey *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (T2) *Уровень безопасности:* 2
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS для macOS 11 Big Sur *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS для macOS 11 Big Sur *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sep OS для macOS 11 Big Sur на компьютере с процессором Intel *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Сертификаты FIPS 140-2

В таблице ниже показаны криптографические модули, которые прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3856 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 10.0 для устройств с процессорами ARM *Операционная система:* sepOS для macOS 10.15 Catalina *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3855 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 10.0 для устройств с процессорами ARM *Операционная система:* sepOS для macOS 10.15 Catalina *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 05.02.2021	*Сертификаты:* 3811 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple Corecrypto версии 10.0 *Операционная система:* sepOS для macOS 10.15 Catalina *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2018 *Даты проверок:* 23.04.2019	*Сертификаты:* 3438 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 9.0 для устройств с процессорами ARM *Операционная система:* sepOS для macOS 10.14 Mojave *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 11.04.2019	*Сертификаты:* 3433 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 9.0 для устройств с процессорами ARM *Операционная система:* sepOS для macOS 10.14 Mojave *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 10.09.2019	*Сертификаты:* 3523 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 9.0 *Операционная система:* sepOS для macOS 10.14 Mojave *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 22.05.2018, 06.07.2018	*Сертификаты:* 3148 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 8.0 для устройств с процессорами ARM *Операционная система:* sepOS для macOS 10.13 High Sierra *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 17.05.2018, 03.07.2018	*Сертификаты:* 3147 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 8.0 для устройств с процессорами ARM *Операционная система:* sepOS для macOS 10.13 High Sierra *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 10.07.2018	*Сертификаты:* 3223 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 1.0 *Операционная система:* sepOS для macOS 10.13 High Sierra *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2016 *Даты проверок:* 01.02.2017	*Сертификаты:* 2828 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 7.0 для iOS *Операционная система:* sepOS для macOS 10.12 Sierra *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2016 *Даты проверок:* 01.02.2017	*Сертификаты:* 2827 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 7.0 для iOS *Операционная система:* sepOS для macOS 10.12 Sierra *Тип:* программное обеспечение *Уровень безопасности:* 1

Сертификация безопасности операционных систем

Обзор сертификации безопасности операционных систем Apple

Apple сертифицирует sepOS и прошивку T2 на соответствие Федеральному стандарту обработки информации США (FIPS) 140-2/-3 и другим стандартам. В основе этого процесса лежат *ключевые аспекты сертификации*, которые широко применяются к разным платформам (насколько это возможно). Одним из аспектов является проверка библиотеки corecrypto, которая используется при развертывании программных и аппаратных криптографических модулей в операционных системах Apple. Второй ключевой аспект — сертификация процессора Secure Enclave, который встроен во многие устройства Apple. Третьим аспектом является сертификация чипа Secure Element (SE), который встроен в устройства Apple с Touch ID и устройства с Face ID. Эти ключевые аспекты сертификации аппаратных компонентов составляют основу для более обширной сертификации платформ в области безопасности.

Проверка криптографических модулей

Подтверждение правильности реализации различных криптографических алгоритмов и связанных функций безопасности является необходимым условием для прохождения проверки на соответствие стандарту FIPS 140-3 и помогает в получении других сертификатов. Проверка проводится в соответствии с программой проверки криптографических алгоритмов (CAVP) NIST. Сертификаты проверки реализаций Apple можно найти с помощью функции поиска CAVP.

Проверка криптографических модулей: FIPS 140-2/3 (ISO/IEC 19790)

Криптографические модули операционных систем Apple неоднократно проверялись по программе проверки криптографических модулей (CMVP) на соответствие Федеральным стандартам обработки информации США (FIPS) 140-2. Эти проверки проводятся при выпуске каждого крупного обновления ОС начиная с 2012 г. После выпуска каждого крупного обновления компания Apple отправляет все модули на полную криптографическую проверку в рамках программы CMVP. Проверяемые модули выполняют криптографические операции для сервисов Apple и могут использоваться приложениями сторонних разработчиков.

Компания Apple каждый год успешно проходит проверку. **Уровень безопасности 1** присваивается следующим программным модулям: модуль Corecrypto для устройств с процессорами Intel и модуль Corecrypto Kernel для устройств с процессорами Intel (для macOS). Для чипа Apple: модуль Corecrypto для устройств с процессорами ARM и модуль Corecrypto Kernel для устройств с процессорами ARM (для iOS, iPadOS, tvOS, watchOS и для прошивки чипа безопасности Apple T2, встроенного в компьютеры Mac).

В 2019 г. встроенный аппаратный криптографический модуль безопасного хранилища ключей Apple Corecrypto прошел первую проверку на соответствие **уровню безопасности 2** по стандарту FIPS 140-2, что позволяет одобренное правительством США использование ключей, которые генерирует и которыми управляет Secure Enclave. Apple продолжает деятельность по проверке аппаратного криптографического модуля для каждого последующего крупного выпуска операционной системы.

Стандарт **FIPS 140-3** был утвержден Министерством торговли США в 2019 г. Самым заметным изменением в этой версии стандарта является спецификация стандартов ISO/IEC, в частности ISO/IEC 19790:2015 и соответствующего стандарта тестирования ISO/IEC 24759:2017. В рамках CMVP была инициирована программа перехода, согласно которой с 2020 г. проверка криптографических модулей будет проводиться в соответствии со стандартом FIPS 140-3. Цель компании Apple — привести криптографические модули в соответствие со стандартом FIPS 140-3 в кратчайшие сроки и таким образом завершить переход на новый стандарт сертификации.

В отношении тех криптографических модулей, которые в настоящий момент проходят проверку и тестирование, программа CMVP предусматривает два отдельных списка, которые могут содержать информацию о предлагаемых проверках. В случае тестирования в аккредитованной лаборатории криптографический модуль может быть включен в список компонентов, переданных на тестирование. После того как лаборатория завершает тестирование криптографических модулей Apple и рекомендует их проверку по программе CMVP, они появляются в списке проверяемых модулей. В настоящее время лабораторные испытания завершены и ожидается тестирование по программе CMVP. Поскольку продолжительность процесса оценки может варьироваться, для определения текущего статуса криптографических модулей Apple в период между датой основного выпуска операционной системы и выпуском сертификата следует проверять оба упомянутых выше списка.

Сертификация продукции: общие критерии (ISO/IEC 15408)

Общие критерии (ISO/IEC 15408) — это стандарт, который используют многие организации для оценки безопасности ИТ-продуктов.

Дополнительная информация о сертификации, которая признана участниками Соглашения о признании общих критериев (CCRA), доступна на портале общих критериев. Стандарт оценки по общим критериям также может использоваться в рамках государственных и частных схем проверки, а не только участниками Соглашения о признании общих критериев. В Европе взаимное признание регулируется соглашением SOG-IS, а также CCRA.

Как следует из заявления сообщества оценки по общим критериям, цель состоит в том, чтобы создать пакет международных стандартов в области безопасности, которые позволят прозрачно и достоверно оценивать функции безопасности в сфере информационных технологий. Сертификация по общим критериям предполагает независимую оценку соответствия продукта стандартам безопасности. Таким образом, покупатели могут принять информированное решение, получив представление о том, какой уровень безопасности обеспечивает тот или иной продукт в сфере информационных технологий.

Вступив в CCRA, страны-участницы договорились признавать сертификацию продуктов в сфере информационных технологий с одинаковым уровнем доверия. Для сертификации требуется обширная оценка, включая:

- профили защиты (PP);
- задания по безопасности (ST);
- функциональные требования к безопасности (SFR);
- требования к гарантиям безопасности (SAR);
- уровни гарантии оценки (EAL).

Профили защиты (PP) являются документами, в которых указаны требования к безопасности для классов типов устройств, таких как «Мобильность». Они используются для сравнения оценок безопасности ИТ-продуктов одного и того же класса. Количество членов CCRA, участвующих в разработке постоянно увеличивающегося количества профилей защиты и расширении сферы их применения, продолжает расти с каждым годом. В соответствии с принятым соглашением каждый разработчик может обратиться за сертификатом по любой из схем утверждения сертификатов, и этот сертификат будет признан всеми подписавшими сторонами.

Задания по безопасности (ST) определяют, *какие характеристики* будут оцениваться при сертификации ИТ-продукта. Задания по безопасности преобразуются в более конкретные *функциональные требования к безопасности (SFR)*, используемые для более детальной оценки заданий по безопасности.

Общие критерии (CC) также включают *требования к гарантиям безопасности*. Одним из часто определяемых показателей является *уровень гарантии оценки (EAL)*. Уровни гарантии оценки объединяют часто встречающиеся наборы требований к гарантиям безопасности и могут быть приведены в профилях защиты или заданиях по безопасности для обеспечения сопоставимости.

Многие использовавшиеся ранее профили защиты были отправлены в архив и по мере разработки замещаются узкоспециализированными профилями защиты, которые предназначены для отдельных решений и сред. Для обеспечения признания со стороны всех членов CCRA были основаны международные технические сообщества (iTC). В конечном итоге целью является разработка и поддержка *совместных профилей защиты (cPP)*, которые с самого начала разрабатываются с учетом схем, используемых участниками CCRA. Профили защиты, предназначенные для групп пользователей и соглашений о взаимном признании, отличных от CCRA, по-прежнему разрабатываются соответствующими заинтересованными сторонами.

Компания Apple обращается за сертификацией в соответствии с новым CCRA на основе определенных совместных профилей защиты с начала 2015 г. С тех пор компания Apple получает сертификаты оценки по общим критериям для каждого основного выпуска iOS, а также запрашивает оценку на основе новых профилей защиты.

Apple активно участвует в работе международных технических сообществ, которые занимаются оценкой технологий в области безопасности мобильных устройств. К таким сообществам относятся международные технические сообщества, отвечающие за разработку и обновление совместных профилей защиты. Apple продолжает деятельность, направленную на оценку и получение соответствующих сертификатов на основе текущих профилей защиты и совместных профилей защиты.

Сертификация платформ компании Apple для североамериканского рынка, как правило, выполняется при участии Национального партнерства по обеспечению достоверности информации (NIAP), которое ведет список проектов, проходящих проверку, но пока не являющихся сертифицированными.

В дополнение к сертификатам основных платформ список включает прочие сертификаты, которые предназначены для подтверждения выполнения требований определенных рынков.

Сертификация безопасности для iOS

Вводная информация о сертификации iOS

Apple активно участвует в проверке встроенных программных и аппаратных модулей Apple для каждого основного выпуска операционных систем. Проверка на соответствие может быть выполнена только для окончательной версии.

Статус проверки криптографических модулей iOS

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей (MIP). В списке проверяемых модулей отображается статус проверки по CMVP. Это может быть один из четырех этапов:
  - *Ожидается проверка*. Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка*. Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование*. Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение*. Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для FIPS 140-3.

Сертификаты FIPS 140-3

Текущий статус

Пространство пользователя, пространство ядра и безопасное хранилище ключей iOS 14 (2020 г.) прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей iOS 15 (2021 г.) проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* iOS 15 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* iOS 15 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с iOS 15 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с iOS 15 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A13, A14, A15) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* iOS 14 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* iOS 14 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с iOS 14 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с iOS 14 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A13-A14) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Сертификаты FIPS 140-2

В следующей таблице показаны криптографические модули, которые в настоящее время проходят тестирование и прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3856 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 10.0 для устройств с процессорами ARM *Операционная система:* iOS 13 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3855 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 10.0 для устройств с процессорами ARM *Операционная система:* iOS 13 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 05.02.2021	*Сертификаты:* 3811 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 10.0 *Операционная система:* sepOS, распространяемая с iOS 13 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2018 *Даты проверок:* 23.04.2019	*Сертификаты:* 3438 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 9.0 для устройств с процессорами ARM *Операционная система:* iOS 12 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 11.04.2019	*Сертификаты:* 3433 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 9.0 для устройств с процессорами ARM *Операционная система:* iOS 12 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 10.09.2019	*Сертификаты:* 3523 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 9.0 *Операционная система:* sepOS, распространяемая с iOS 12 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 22.05.2018, 06.07.2018	*Сертификаты:* 3148 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 8.0 для устройств с процессорами ARM *Операционная система:* iOS 11 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 17.05.2018, 03.07.2018	*Сертификаты:* 3147 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 8.0 для устройств с процессорами ARM *Операционная система:* iOS 11 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 10.09.2019	*Сертификаты:* 3223 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 1.0 *Операционная система:* sepOS, распространяемая с iOS 11 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2016 *Даты проверок:* 01.02.2017	*Сертификаты:* 2828 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 7.0 для iOS *Операционная система:* iOS 10 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2016 *Даты проверок:* 01.02.2017	*Сертификаты:* 2827 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 7.0 для iOS *Операционная система:* iOS 10 *Тип:* программное обеспечение *Уровень безопасности:* 1

Предыдущие версии

Сертификатам, выпущенным более 5 лет назад, по программе CMVP присваивается архивный статус. Перечисленные ниже предыдущие версии iOS прошли проверку криптографических модулей:

- iOS 9 (модули corecrypto версии 6.0)
- iOS 8 (модули corecrypto версии 5.0)
- iOS 7 (модули corecrypto версии 4.0)
- iOS 6 (модули corecrypto версии 3.0)

Вводная информация о сертификации по общим критериям (CC)

Apple активно участвует в оценке каждого основного выпуска операционной системы iOS. Оценка может быть выполнена только для окончательной общедоступной версии операционной системы. До версии iPadOS 13.1 вместо iPadOS использовалось название iOS.

Статус сертификации по общим критериям (CC)

За управление схемой США отвечает Национальное партнерство по обеспечению достоверности информации (NIAP), которое ведет список продуктов, проходящих проверку. Этот список включает продукты, которые в настоящее время проходят оценку в США в одобренной NIAP лаборатории тестирования по общим критериям (CCTL) и по которым было проведено вводное совещание (или его аналог), во время которого руководство CCEVS официально приняло продукт для оценки.

После сертификации продуктов NIAP вносит текущие действующие сертификаты в список совместимых продуктов. Через 2 года эти сертификаты проверяются на соответствие текущей политике поддержания гарантий безопасности. По истечении срока поддержания гарантий безопасности NIAP перемещает список сертификатов в список архивных продуктов.

На портале общих критериев перечислены сертификаты, которые признаны участниками Соглашения о признании общих критериев (CCRA). Портал общих критериев может поддерживать продукты в списке сертифицированных продуктов в течение 5 лет и сохраняет записи для архивных сертификатов.

В таблице ниже показаны сертификаты, которые в настоящее время проходят проверку в лаборатории или которые были сертифицированы как соответствующие общим критериям.

Текущий статус

В настоящее время проводится лабораторное тестирование для оценки iOS 15 при участии NIAP. Новейшая информация приведена в списке продуктов, проходящих проверку (NIAP) и в списке совместимых продуктов.

Операционная система/дата сертификации	**Идентификатор схемы/ документы**	**Название/профили защиты**
Операционная система: iOS 15 *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* —	*Название:* Apple iOS 15: iPhone *Профили защиты:* Основная защита мобильных устройств (в отношении модулей PP еще нет подтверждения)
Операционная система: iOS 14 *Дата сертификации:* 01.09.2021	*Идентификатор схемы:* 11146 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iOS 14: iPhone *Профили защиты:* Основная защита мобильных устройств, модуль для клиента VPN, модуль PP для клиента WLAN, расширенный пакет для агента MDM
Операционная система: iOS 13 *Дата сертификации:* 06.11.2020	*Идентификатор схемы:* 11036 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iOS 13 на iPhone *Профили защиты:* Основная защита мобильных устройств, модуль для клиента VPN, расширенный пакет для клиента WLAN, расширенный пакет для агента MDM

Архивные сертификаты по общим критериям для iOS

Перечисленные ниже предыдущие версии iOS прошли проверку по общим критериям. Они помещены в архив NIAP в соответствии с политикой NIAP:

Операционная система/дата сертификации	**Идентификатор схемы/ документы**	**Название/профили защиты**
Операционная система: iOS 12 *Дата сертификации:* 14.03.2019	*Идентификатор схемы:* 10937 *Документы:* Задание по безопасности Руководство	*Название:* iPhone с iOS 12 *Профили защиты:* основная защита мобильных устройств, модуль для клиента VPN, расширенный пакет для клиента беспроводной локальной сети, расширенный пакет для агента MDM
Операционная система: iOS 11 *Дата сертификации:* 17.07.2018	*Идентификатор схемы:* 10851 *Документы:* Задание по безопасности Руководство	*Название:* Apple iOS 11 *Профили защиты:* основная защита мобильных устройств, расширенный пакет для клиента беспроводной локальной сети, расширенный пакет для агента MDM
Операционная система: iOS 10 *Дата сертификации:* 27.07.2017	*Идентификатор схемы:* 10782 *Документы:* Задание по безопасности, Руководство	*Название:* iOS 10.2 на устройствах iPhone и iPad *Профили защиты:* основная защита мобильных устройств, расширенный пакет для клиента беспроводной локальной сети, расширенный пакет для агента MDM
Операционная система: iOS 10 *Дата сертификации:* 27.07.2017	*Идентификатор схемы:* 10792 *Документы:* Задание по безопасности, Руководство	*Название:* клиент VPN в iOS 10.2 на iPhone и iPad *Профили защиты:* профиль защиты клиента VPN
Операционная система: iOS 9 *Дата сертификации:* 14.10.2016	*Идентификатор схемы:* 10725 *Документы:* Задание по безопасности, Руководство	*Название:* iOS 9.3.2 с агентом MDM *Профили защиты:* основная защита мобильных устройств, расширенный пакет для агента MDM
Операционная система: iOS 9 *Дата сертификации:* 13.10.2016	*Идентификатор схемы:* 10714 *Документы:* Задание по безопасности, Руководство	*Название:* клиент VPN ОС на iPhone и iPad *Профили защиты:* профиль защиты клиента VPN
Операционная система: iOS 9 *Дата сертификации:* 28.01.2016	*Идентификатор схемы:* 10695 *Документы:* Задание по безопасности, Руководство	*Название:* iOS 9 *Профили защиты:* основная защита мобильных устройств

Сертификация безопасности для iPadOS

Вводная информация о сертификации iPadOS

Apple активно участвует в проверке операционных систем Apple для каждого основного выпуска операционных систем. При проверке используются совместные профили защиты и уровни безопасности согласно стандарту FIPS 140-3. Проверка на соответствие может быть выполнена только для окончательной версии.

Примечание. В 2019 г. операционная система устройств iPad была переименована в iPadOS. До версии iPadOS 13.1 вместо iPadOS использовалось название iOS.

Статус проверки криптографических модулей iPadOS

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей (MIP). В списке проверяемых модулей отображается статус проверки по программе CMVP. Это может быть один из четырех этапов, которые перечислены далее.
  - *Ожидается проверка.* Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка.* Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование.* Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение.* Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для FIPS 140-3.

Сертификаты FIPS 140-3

Текущий статус

Пространство пользователя, пространство ядра и безопасное хранилище ключей iPadOS 14 (2020 г.) прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей iPadOS 15 (2021 г.) проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* iPadOS 15 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* iPadOS 15 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с iPadOS 15 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14, M1) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с iPadOS 15 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14, M1) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* iPadOS 14 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* iPadOS 14 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с iPadOS 14 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14, M1) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с iPadOS 14 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A9-A14, M1) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Сертификаты FIPS 140-2

В следующей таблице показаны криптографические модули, которые в настоящее время проходят тестирование и прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3856 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 10.0 для устройств с процессорами ARM *Операционная система:* iPadOS 13 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3855 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 10.0 для устройств с процессорами ARM *Операционная система:* iPadOS 13 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 05.02.2021	*Сертификаты:* 3811 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple Corecrypto версии 10.0 *Операционная система:* sepOS, распространяемая с iPadOS 13 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2018 *Даты проверок:* 23.04.2019	*Сертификаты:* 3438 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 9.0 для устройств с процессорами ARM *Операционная система:* iOS 12 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 11.04.2019	*Сертификаты:* 3433 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 9.0 для устройств с процессорами ARM *Операционная система:* iOS 12 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 10.09.2019	*Сертификаты:* 3523 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 9.0 *Операционная система:* sepOS, распространяемая с iOS 12 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 22.05.2018, 06.07.2018	*Сертификаты:* 3148 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 8.0 для устройств с процессорами ARM *Операционная система:* iOS 11 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 17.05.2018, 03.07.2018	*Сертификаты:* 3147 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 8.0 для устройств с процессорами ARM *Операционная система:* iOS 11 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 10.09.2019	*Сертификаты:* 3223 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 1.0 *Операционная система:* sepOS, распространяемая с iOS 11 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2016 *Даты проверок:* 01.02.2017	*Сертификаты:* 2828 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 7.0 для iOS *Операционная система:* iOS 10 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2016 *Даты проверок:* 01.02.2017	*Сертификаты:* 2827 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 7.0 для iOS *Операционная система:* iOS 10 *Тип:* программное обеспечение *Уровень безопасности:* 1

Предыдущие версии

Сертификатам, выпущенным более 5 лет назад, по программе CMVP присваивается архивный статус. Перечисленные ниже предыдущие версии iOS прошли проверку криптографических модулей:

- iOS 9 (модули corecrypto версии 6.0)
- iOS 8 (модули corecrypto версии 5.0)
- iOS 7 (модули corecrypto версии 4.0)
- iOS 6 (модули corecrypto версии 3.0)

Вводная информация о сертификации по общим критериям (CC)

Apple активно участвует в оценке каждого основного выпуска операционной системы iPadOS. Оценка может быть выполнена только для окончательной общедоступной версии операционной системы.

Статус сертификации по общим критериям (CC)

За управление схемой США отвечает Национальное партнерство по обеспечению достоверности информации (NIAP), которое ведет список продуктов, проходящих проверку. Этот список включает продукты, которые в настоящее время проходят оценку в США в одобренной NIAP лаборатории тестирования по общим критериям (CCTL) и по которым было проведено вводное совещание (или его аналог), во время которого руководство CCEVS официально приняло продукт для оценки.

После сертификации продуктов NIAP вносит текущие действующие сертификаты в список совместимых продуктов. Через 2 года эти сертификаты проверяются на соответствие текущей политике поддержания гарантий безопасности. По истечении срока поддержания гарантий безопасности NIAP перемещает список сертификатов в список архивных продуктов.

На портале общих критериев перечислены сертификаты, которые признаны участниками Соглашения о признании общих критериев (CCRA). Портал общих критериев может поддерживать продукты в списке сертифицированных продуктов в течение 5 лет и сохраняет записи для архивных сертификатов.

В таблице ниже показаны сертификаты, которые в настоящее время проходят проверку в лаборатории или которые были сертифицированы как соответствующие общим критериям.

Текущий статус

В настоящее время проводится лабораторное тестирование для оценки iPadOS 15 при участии NIAP. Новейшая информация приведена в списке продуктов, проходящих проверку (NIAP) и в списке совместимых продуктов.

Операционная система/дата сертификации	Идентификатор схемы/документы	Название/профили защиты
Операционная система: iPadOS 15 *Дата сертификации:* 14.03.2019	*Идентификатор схемы:* — *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* iPad с iOS 12 *Профили защиты:* основная защита мобильных устройств, модуль для клиента VPN, расширенный пакет для клиента беспроводной локальной сети, расширенный пакет для агента MDM

Операционная система/дата сертификации	Идентификатор схемы/ документы	Название/профили защиты
Операционная система: iPadOS 14 *Дата сертификации:* 01.09.2021	*Идентификатор схемы:* 11147 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iPadOS 14: iPad *Профили защиты:* основная защита мобильных устройств, модуль для клиента VPN, расширенный пакет для клиента беспроводной локальной сети, расширенный пакет для агента MDM
Операционная система: iPadOS 13 *Дата сертификации:* 06.11.2020	*Идентификатор схемы:* 11036 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* iPadOS 13 на мобильных устройствах iPad *Профили защиты:* основная защита мобильных устройств, модуль для клиента VPN, расширенный пакет для клиента беспроводной локальной сети, расширенный пакет для агента MDM

Предыдущие версии

Перечисленные ниже предыдущие версии iOS прошли проверку по общим критериям. Они помещены в архив NIAP в соответствии с политикой NIAP:

- iOS 12 (идентификатор схемы: 10937)
- iOS 11 (идентификатор схемы: 10851)
- iOS 10 (идентификатор схемы: 107782, 10792)
- iOS 9 (идентификатор схемы: 10725, 10714, 10695)

Сертификация безопасности для macOS

Вводная информация о сертификации macOS

Apple активно участвует в проверке операционных систем Apple для каждого основного выпуска операционных систем. При проверке используются совместные профили защиты и уровни безопасности согласно стандарту FIPS 140-3. Проверка на соответствие может быть выполнена только для окончательной версии.

Статус проверки криптографических модулей macOS

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей (MIP). В списке проверяемых модулей отображается статус проверки по CMVP. Это может быть один из четырех этапов:
  - *Ожидается проверка*. Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка*. Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование*. Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение*. Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для FIPS 140-3.

В приведенной ниже таблице показано, какие криптографические модули применяются для указанных технологий компьютеров Apple Mac.

Криптографический модуль	Компьютеры Mac с чипом Apple	Компьютеры Mac с чипом безопасности Apple T2	Компьютеры Mac с процессором Intel и без чипа безопасности Apple T2
Пространство пользователя чипа Apple	✓		
Ядро чипа Apple	✓		
Пространство пользователя Intel		✓	✓
Ядро Intel		✓	✓
Безопасное хранилище ключей	✓	✓	

Сертификаты FIPS 140-3

В 2020 г. Apple выпустила компьютеры Mac с чипом Apple. В столбце «Информация о модуле» таблицы ниже указано, к каким компьютерам Mac относятся криптографические модули, то есть к компьютерам с чипом Apple или с процессором Intel.

Примечание. Чипы безопасности Apple T2 устанавливаются во многие компьютеры Mac с процессором Intel. Сведения о сертификации чипа T2 см. в разделе Сертификация безопасности для чипа безопасности Apple T2.

SSH-клиент macOS

Можно настроить OpenSSH на использование модулей, проверенных на соответствие стандарту FIPS 140-3, для ряда алгоритмов FIPS 140-3. Организации могут запустить подписанный и заверенный установщик, предлагаемый компанией Apple, с паролем *FIPS140Mode*. Установщик помещает на Mac два файла:

- *fips_ssh_config*. Размещается в папке /private/etc/ssh/ssh_config.d/
- *fips_sshd_config*. Размещается в папке /private/etc/ssh/sshd_config.d/

Используя эти файлы, macOS ограничивает доступные для OpenSSH шифры только теми, которые были проверены NIST, и гарантирует, что клиент OpenSSH использует предоставленный платформой проверенный криптографический модуль. Администраторы также могут создавать собственные файлы. Дополнительная информация приведена на man-странице `apple_ssh_and_fips` в macOS 12.0.1 и новее.

Текущий статус

Пространство пользователя, пространство ядра и безопасное хранилище ключей macOS 11 Big Sur прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей macOS 12 Monterey проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0ß *Операционная система:* macOS 12 Monterey на компьютере с чипом Apple *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* macOS 12 Monterey на компьютере с чипом Apple *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* macOS 12 Monterey на компьютере с процессором Intel *Среда:* Intel, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* macOS 12 Monterey на компьютере с процессором Intel *Среда:* Intel, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* sepOS, распространяемая с macOS 12 Monterey на компьютере с чипом Apple, sepOS, распространяемая с macOS 12 Monterey на компьютере с процессором Intel и чипом T2 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (M1 и T2) *Уровень безопасности:* 2
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12.0 *Операционная система:* sepOS, распространяемая с macOS 12 Monterey на компьютере с чипом Apple *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (M1) *Уровень безопасности:* 2 *Уровень физической безопасности:* 3
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* macOS 11 Big Sur на компьютере с процессором Intel *Среда:* Intel, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* macOS 11 Big Sur на компьютере с процессором Intel *Среда:* Intel, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* macOS 11 Big Sur на компьютере с чипом Apple *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* macOS 11 Big Sur на компьютере с чипом Apple *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с macOS 11 Big Sur на компьютере с чипом Apple, sepOS, распространяемая с macOS 11 Big Sur на компьютере с процессором Intel *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (M1) *Уровень безопасности:* 2
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с macOS 11 Big Sur на компьютере с чипом Apple *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (M1) *Уровень безопасности:* 2 *Уровень физической безопасности:* 3

Сертификаты FIPS 140-2

В следующей таблице показаны криптографические модули, которые в настоящее время проходят тестирование и прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Пространство пользователя, пространство ядра и безопасное хранилище ключей macOS 10.15 Catalina прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Примечание. Чипы безопасности Apple T2 устанавливаются во многие компьютеры Mac с процессором Intel. Сведения о сертификации чипа T2 см. в разделе Сертификация безопасности для чипа безопасности Apple T2.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 24.03.2021	*Сертификаты:* 3859 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto для пространства пользователя для устройств с процессорами Intel (ccv10) *Операционная система:* macOS 10.15 Catalina *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 24.03.2021	*Сертификаты:* 3858 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 10.0 для устройств с процессорами Intel (ccv10) *Операционная система:* macOS 10.15 Catalina *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 12.04.2019	*Сертификаты:* 3402 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 9.0 для устройств с процессорами Intel *Операционная система:* macOS 10.14 Mojave *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 12.04.2019	*Сертификаты:* 3431 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 9.0 для устройств с процессорами Intel *Операционная система:* macOS 10.14 Mojave *Тип:* программное обеспечение *Уровень безопасности:* 1

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2017 *Даты проверок:* 22.03.2018	*Сертификаты:* 3155 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 8.0 для устройств с процессорами Intel *Операционная система:* macOS 10.13 High Sierra *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 22.03.2018	*Сертификаты:* 3156 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 8.0 для устройств с процессорами Intel *Операционная система:* macOS 10.13 High Sierra *Тип:* программное обеспечение *Уровень безопасности:* 1

Предыдущие версии

Перечисленные ниже предыдущие версии OS X и macOS прошли проверку криптографических модулей. Версиям, выпущенным более 5 лет назад, в рамках программы CMVP присвоен архивный статус.

- macOS 10.12 Sierra
- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks
- OS X 10.8 Mountain Lion
- OS X 10.7 Lion
- OS X 10.6 Snow Leopard

Вводная информация о сертификации по общим критериям (CC)

Apple активно участвует в оценке каждого основного выпуска операционной системы macOS. Оценка может быть выполнена только для окончательной общедоступной версии операционной системы.

Статус сертификации по общим критериям (CC)

За управление схемой США отвечает Национальное партнерство по обеспечению достоверности информации (NIAP), которое ведет список продуктов, проходящих проверку. Этот список включает продукты, которые в настоящее время проходят оценку в США в одобренной NIAP лаборатории тестирования по общим критериям (CCTL) и по которым было проведено вводное совещание (или его аналог), во время которого руководство CCEVS официально приняло продукт для оценки.

После сертификации продуктов NIAP вносит текущие действующие сертификаты в список совместимых продуктов. Через 2 года эти сертификаты проверяются на соответствие текущей политике поддержания гарантий безопасности. По истечении срока поддержания гарантий безопасности NIAP перемещает список сертификатов в список архивных продуктов.

На портале общих критериев перечислены сертификаты, которые признаны участниками Соглашения о признании общих критериев (CCRA). Портал общих критериев может поддерживать продукты в списке сертифицированных продуктов в течение 5 лет и сохраняет записи для архивных сертификатов.

В таблице ниже показаны сертификаты, которые в настоящее время проходят проверку в лаборатории или которые были сертифицированы как соответствующие общим критериям.

Текущий статус

В настоящее время macOS 11 и macOS 12 оцениваются с использованием профилей защиты «Операционная система общего назначения» и «Полное шифрование диска (FDE)» (AA и EE) при участии NIAP.

Новейшая информация приведена в списке продуктов, проходящих проверку (NIAP) и в списке совместимых продуктов.

Операционная система/дата сертификации	Идентификатор схемы/документы	Название/профили защиты
Операционная система: macOS 12 Monterey *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* —	*Название:* Apple FileVault 2 с macOS 12 Monterey *Профили защиты:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E (в отношении PP еще нет подтверждения)
Операционная система: macOS 12 Monterey *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* —	*Название:* macOS 12 Monterey *Профили защиты:* PP_OS_V4.21 (в отношении PP еще нет подтверждения)

Операционная система/дата сертификации	Идентификатор схемы/ документы	Название/профили защиты
Операционная система: macOS 11 Big Sur *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple FileVault 2 с macOS 11 Big Sur *Профили защиты:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Операционная система: macOS 11 Big Sur *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple macOS 11 Big Sur *Профили защиты:* PP_OS_V4.21
Операционная система: macOS 10.15 Catalina *Дата сертификации:* 29.04.2021	*Идентификатор схемы:* 11078 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple FileVault 2 на компьютерах с чипами T2 с macOS 10.15 Catalina *Профили защиты:* CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E
Операционная система: macOS 10.15 Catalina *Дата сертификации:* 23.09.2020	*Идентификатор схемы:* 11077 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* macOS 10.15 Catalina *Профили защиты:* PP_OS_V4.21

Сертификация безопасности для tvOS

Вводная информация о сертификации tvOS

Apple активно участвует в проверке криптографических модулей для каждого основного выпуска tvOS. Проверка на соответствие может быть выполнена только для окончательной версии.

Статус проверки криптографических модулей tvOS

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей (MIP). В списке проверяемых модулей отображается статус проверки по CMVP. Это может быть один из четырех этапов:
  - *Ожидается проверка*. Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка*. Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование*. Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение*. Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для FIPS 140-3.

Сертификаты FIPS 140-3

Текущий статус

Пространство пользователя, пространство ядра и безопасное хранилище ключей tvOS 14 (2020 г.) прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей tvOS 15 (2021 г.) проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* tvOS 15 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* tvOS 15 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с tvOS 15 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A10, A12) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* tvOS 14 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* tvOS 14 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с tvOS 14 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (A10, A12) *Уровень общей безопасности:* 2

Сертификаты FIPS 140-2

В следующей таблице показаны криптографические модули, которые в настоящее время проходят тестирование и прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Пространство пользователя, пространство ядра и безопасное хранилище ключей tvOS 13 (2019 г.) прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3856 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 10.0 для устройств с процессорами ARM *Операционная система:* tvOS 13 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 23.03.2021	*Сертификаты:* 3855 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 10.0 для устройств с процессорами ARM *Операционная система:* tvOS 13 *Тип:* программное обеспечение *Уровень безопасности:* 1

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* 05.02.2021	*Сертификаты:* 3811 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 10.0 *Операционная система:* sepOS, распространяемая с tvOS 13 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2018 *Даты проверок:* 23.04.2019	*Сертификаты:* 3438 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 9.0 для устройств с процессорами ARM *Операционная система:* tvOS 12 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 11.04.2019	*Сертификаты:* 3433 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 9.0 для устройств с процессорами ARM *Операционная система:* tvOS 12 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 10.09.2019	*Сертификаты:* 3523 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 9.0 *Операционная система:* sepOS, распространяемая с tvOS 12 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 22.05.2018, 06.07.2018	*Сертификаты:* 3148 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 8.0 для устройств с процессорами ARM *Операционная система:* tvOS 11 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 17.05.2018, 03.07.2018	*Сертификаты:* 3147 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 8.0 для устройств с процессорами ARM *Операционная система:* tvOS 11 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 10.09.2019	*Сертификаты:* 3223 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 1.0 *Операционная система:* sepOS, распространяемая с tvOS 11 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Сертификация безопасности для watchOS

Вводная информация о сертификации watchOS

Apple активно участвует в проверке криптографических модулей для каждого основного выпуска watchOS. Проверка на соответствие может быть выполнена только для окончательной версии.

Статус проверки криптографических модулей watchOS

Статус проверки криптографических модулей в программе проверки криптографических модулей (CMVP) указывается в трех отдельных списках в зависимости от текущего статуса.

- Чтобы модуль попал в список компонентов, переданных на тестирование, у лаборатории должен быть заключен контракт с Apple на проведение тестирования.
- После того как лаборатория завершила тестирование модуля, порекомендовала его проверку по программе CMVP и были оплачены взносы CMVP, модуль добавляется в список проверяемых модулей (MIP). В списке проверяемых модулей отображается статус проверки по CMVP. Это может быть один из четырех этапов:
  - *Ожидается проверка*. Ожидание назначения ресурсов CMVP.
  - *Выполняется проверка*. Ресурсы CMVP выполняют требуемые действия по проверке.
  - *Согласование*. Лаборатория и CMVP устраняют любые обнаруженные проблемы.
  - *Завершение*. Действия и официальные процедуры, связанные с выдачей сертификата.
- После проверки по программе CMVP модули получают сертификат соответствия и добавляются в список проверенных криптографических модулей. Список содержит модули с указанными далее статусами:
  - проверяемые модули отмечаются как текущие;
  - через 5 лет модулям присваивается архивный статус;
  - в случае отзыва сертификата модуля по какой-либо причине сертификату присваивается статус отозванного.

В 2020 г. в рамках программы CMVP международный стандарт ISO/IEC 19790 был принят в качестве основы для FIPS 140-3.

Сертификаты FIPS 140-3

Текущий статус

Пространство пользователя, пространство ядра и безопасное хранилище ключей watchOS 7 (2020 г.) прошли лабораторное тестирование и были рекомендованы лабораторией для проверки по программе CMVP. Они перечислены в списке проверяемых модулей.

Пространство пользователя, пространство ядра и безопасное хранилище ключей watchOS 8 (2021 г.) проходят лабораторное тестирование. Они находятся в списке компонентов, переданных на тестирование.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* watchOS 8 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* watchOS 8 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с watchOS 8 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (S3, S4, S5, S6) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2021 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 12 *Операционная система:* sepOS, распространяемая с watchOS 8 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (S6) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* watchOS 7 *Среда:* чип Apple, пользователь, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* watchOS 7 *Среда:* чип Apple, ядро, программное обеспечение *Тип:* программное обеспечение *Уровень общей безопасности:* 1
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с watchOS 7 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (S3, S4, S5, S6) *Уровень общей безопасности:* 2
Дата выпуска операционной системы: 2020 *Даты проверок:* —	*Сертификаты:* сертификаты пока не получены *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto версии 11.1 *Операционная система:* sepOS, распространяемая с watchOS 7 *Среда:* чип Apple, безопасное хранилище ключей, аппаратное обеспечение *Тип:* аппаратное обеспечение (S6) *Уровень общей безопасности:* 2 *Уровень физической безопасности:* 3

Сертификаты FIPS 140-2

В следующей таблице показаны криптографические модули, которые в настоящее время проходят тестирование и прошли лабораторное тестирование на соответствие стандарту FIPS 140-2.

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2019 *Даты проверок:* —	*Сертификаты:* 3856 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 10.0 для устройств с процессорами ARM *Операционная система:* watchOS 6 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* —	*Сертификаты:* 3855 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 10.0 для устройств с процессорами ARM *Операционная система:* watchOS 6 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2019 *Даты проверок:* 05.02.2021	*Сертификаты:* 3811 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 10.0 *Операционная система:* sepOS, распространяемая с watchOS 6 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2
Дата выпуска операционной системы: 2018 *Даты проверок:* 23.04.2019	*Сертификаты:* 3438 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 9.0 для устройств с процессорами ARM *Операционная система:* watchOS 5 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 11.04.2019	*Сертификаты:* 3433 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 9.0 для устройств с процессорами ARM *Операционная система:* watchOS 5 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2018 *Даты проверок:* 10.09.2019	*Сертификаты:* 3523 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 9.0 *Операционная система:* sepOS, распространяемая с watchOS 5 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Даты	Сертификаты/документы	Информация о модуле
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 22.05.2018, 06.07.2018	*Сертификаты:* 3148 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto User версии 8.0 для устройств с процессорами ARM *Операционная система:* watchOS 4 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 09.03.2018, 17.05.2018, 03.07.2018	*Сертификаты:* 3147 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* модуль Apple Corecrypto Kernel версии 8.0 для устройств с процессорами ARM *Операционная система:* watchOS 4 *Тип:* программное обеспечение *Уровень безопасности:* 1
Дата выпуска операционной системы: 2017 *Даты проверок:* 10.09.2019	*Сертификаты:* 3223 *Документы:* Сертификат Политика безопасности Рекомендации для лица, ответственного за СКЗИ	*Название:* криптографический модуль безопасного хранилища ключей Apple версии 1.0 *Операционная система:* sepOS, распространяемая с watchOS 4 *Тип:* аппаратное обеспечение *Уровень безопасности:* 2

Сертификация безопасности программного обеспечения

Обзор сертификации безопасности программного обеспечения Apple

Apple сертифицирует sepOS и прошивку T2 на соответствие Федеральному стандарту обработки информации США (FIPS) 140-2/-3 и другим стандартам. В основе этого процесса лежат *ключевые аспекты сертификации*, которые широко применяются к разным платформам (насколько это возможно). Одним из аспектов является проверка библиотеки corecrypto, которая используется при развертывании программных и аппаратных криптографических модулей в операционных системах Apple. Второй ключевой аспект — сертификация процессора Secure Enclave, который встроен во многие устройства Apple. Третьим аспектом является сертификация чипа Secure Element (SE), который встроен в устройства Apple с Touch ID и устройства с Face ID. Эти ключевые аспекты сертификации аппаратных компонентов составляют основу для более обширной сертификации платформ в области безопасности.

Сертификация продукции: общие критерии (ISO/IEC 15408)

Общие критерии (ISO/IEC 15408) — это стандарт, который используют многие организации для оценки безопасности ИТ-продуктов.

Дополнительная информация о сертификации, которая признана участниками Соглашения о признании общих критериев (CCRA), доступна на портале общих критериев. Стандарт оценки по общим критериям также может использоваться в рамках государственных и частных схем проверки, а не только участниками Соглашения о признании общих критериев. В Европе взаимное признание регулируется соглашением SOG-IS, а также CCRA.

Как следует из заявления сообщества оценки по общим критериям, цель состоит в том, чтобы создать пакет международных стандартов в области безопасности, которые позволят прозрачно и достоверно оценивать функции безопасности в сфере информационных технологий. Сертификация по общим критериям предполагает независимую оценку соответствия продукта стандартам безопасности. Таким образом, покупатели могут принять информированное решение, получив представление о том, какой уровень безопасности обеспечивает тот или иной продукт в сфере информационных технологий.

Вступив в CCRA, страны-участницы договорились признавать сертификацию продуктов в сфере информационных технологий с одинаковым уровнем доверия. Для сертификации требуется обширная оценка, включая:

- профили защиты (PP);
- задания по безопасности (ST);
- функциональные требования к безопасности (SFR);
- требования к гарантиям безопасности (SAR);
- уровни гарантии оценки (EAL).

Профили защиты (PP) являются документами, в которых указаны требования к безопасности для классов типов устройств, таких как «Мобильность». Они используются для сравнения оценок безопасности ИТ-продуктов одного и того же класса. Количество членов CCRA, участвующих в разработке постоянно увеличивающегося количества профилей защиты и расширении сферы их применения, продолжает расти с каждым годом. В соответствии с принятым соглашением каждый разработчик может обратиться за сертификатом по любой из схем утверждения сертификатов, и этот сертификат будет признан всеми подписавшими сторонами.

Задания по безопасности (ST) определяют, *какие характеристики* будут оцениваться при сертификации ИТ-продукта. Задания по безопасности преобразуются в более конкретные *функциональные требования к безопасности (SFR)*, используемые для более детальной оценки заданий по безопасности.

Общие критерии (CC) также включают *требования к гарантиям безопасности*. Одним из часто определяемых показателей является *уровень гарантии оценки (EAL)*. Уровни гарантии оценки объединяют часто встречающиеся наборы требований к гарантиям безопасности и могут быть приведены в профилях защиты или заданиях по безопасности для обеспечения сопоставимости.

Многие использовавшиеся ранее профили защиты были отправлены в архив и по мере разработки замещаются узкоспециализированными профилями защиты, которые предназначены для отдельных решений и сред. Для обеспечения признания со стороны всех членов CCRA были основаны международные технические сообщества (iTC). В конечном итоге целью является разработка и поддержка совместных профилей защиты (cPP), которые с самого начала разрабатываются с учетом схем, используемых участниками CCRA. Профили защиты, предназначенные для групп пользователей и соглашений о взаимном признании, отличных от CCRA, по-прежнему разрабатываются соответствующими заинтересованными сторонами.

Компания Apple обращается за сертификацией в соответствии с новым CCRA на основе определенных совместных профилей защиты с начала 2015 г. С тех пор компания Apple получает сертификаты оценки по общим критериям для каждого основного выпуска iOS, а также запрашивает оценку на основе новых профилей защиты.

Apple активно участвует в работе международных технических сообществ, которые занимаются оценкой технологий в области безопасности мобильных устройств. К таким сообществам относятся международные технические сообщества, отвечающие за разработку и обновление совместных профилей защиты. Apple продолжает деятельность, направленную на оценку и получение соответствующих сертификатов на основе текущих профилей защиты и совместных профилей защиты.

Сертификация платформ компании Apple для североамериканского рынка, как правило, выполняется при участии Национального партнерства по обеспечению достоверности информации (NIAP), которое ведет список проектов, проходящих проверку, но пока не являющихся сертифицированными.

В дополнение к сертификатам основных платформ список включает прочие сертификаты, которые предназначены для подтверждения выполнения требований определенных рынков.

Сертификация безопасности для приложений Apple

Вводная информация о сертификации приложений Apple

Apple активно участвует в сертификации безопасности приложений Apple, используя соответствующие профили защиты по общим критериям. Эта оценка основана на сертификатах оборудования и операционных систем, полученных компанией Apple.

В 2018 г. компания Apple инициировала оценку безопасности ключевых приложений, работающих в iOS 11: браузера Safari и приложения «Контакты». Apple продолжила оценивать приложения в iOS 12, iOS 13 и iPadOS 13.1. В 2021 г. начали оцениваться приложения для macOS 11.

Статус сертификации криптографических модулей

Перечисленные здесь приложения Apple используют криптографические модули для соответствующих операционных систем. С подробной информацией можно ознакомиться в разделах Сертификация безопасности для iOS, Сертификация безопасности для iPadOS и Сертификация безопасности для macOS.

Статус сертификации по общим критериям (CC)

За управление схемой США отвечает Национальное партнерство по обеспечению достоверности информации (NIAP), которое ведет список продуктов, проходящих проверку. Этот список включает продукты, которые в настоящее время проходят оценку в США в одобренной NIAP лаборатории тестирования по общим критериям (CCTL) и по которым было проведено вводное совещание (или его аналог), во время которого руководство CCEVS официально приняло продукт для оценки.

После сертификации продуктов NIAP вносит текущие действующие сертификаты в список совместимых продуктов. Через 2 года эти сертификаты проверяются на соответствие текущей политике поддержания гарантий безопасности. По истечении срока поддержания гарантий безопасности NIAP перемещает список сертификатов в список архивных продуктов.

На портале общих критериев перечислены сертификаты, которые признаны участниками Соглашения о признании общих критериев (CCRA). Портал общих критериев может поддерживать продукты в списке сертифицированных продуктов в течение 5 лет и сохраняет записи для архивных сертификатов.

В таблице ниже показаны сертификаты, которые в настоящее время проходят проверку в лаборатории или которые были сертифицированы как соответствующие общим критериям.

Текущий статус

- Проверки при участии NIAP, которые опубликованы как проводимые в настоящий момент, перечислены в списке продуктов, проходящих проверку (NIAP).
- Завершенные и пересмотренные проверки перечислены в списке совместимых продуктов (NIAP).

Операционная система/дата сертификации	Идентификатор схемы/ документы	Название/профили защиты
Операционная система: macOS 11 Big Sur *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* macOS 11 Big Sur: Контакты *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров
Операционная система: macOS 11 Big Sur *Дата сертификации:* —	*Идентификатор схемы:* сертификаты пока не получены *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* macOS 11 Big Sur: Safari *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров
Операционная система: iOS 14, iPadOS 14 *Дата сертификации:* 20.08.2021	*Идентификатор схемы:* 11191 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iOS 14 и iPadOS 14: Контакты *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров
Операционная система: iOS 14, iPadOS 14 *Дата сертификации:* —	*Идентификатор схемы:* 11192 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iOS 14 и iPadOS 14: Safari *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров

Операционная система/дата сертификации	Идентификатор схемы/ документы	Название/профили защиты
Операционная система: iOS 13, iPadOS 13 *Дата сертификации:* 05.06.2020	*Идентификатор схемы:* 11060 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iOS 13 и iPadOS 13: Safari *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров
Операционная система: iOS 13, iPadOS 13 *Дата сертификации:* 05.06.2020	*Идентификатор схемы:* 11050 *Документы:* Сертификат Задание по безопасности Руководство Отчет о результатах проверки Отчет о деятельности в отношении гарантий безопасности	*Название:* Apple iOS 13 и iPadOS 13: Контакты *Профили защиты:* профиль защиты для прикладного программного обеспечения

Архивные сертификаты по общим критериям для приложений Apple

Операционная система/дата сертификации	Идентификатор схемы/ документы	Название/профили защиты
Операционная система: iOS 12 *Дата сертификации:* 12.06.2019	*Идентификатор схемы:* 10960 *Документы:* Задание по безопасности Руководство	*Название:* Safari в iOS 12 *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров
Операционная система: iOS 12 *Дата сертификации:* 28.02.2019	*Идентификатор схемы:* 10961 *Документы:* Задание по безопасности Руководство	*Название:* Контакты в iOS 12 *Профили защиты:* профиль защиты для прикладного программного обеспечения
Операционная система: iOS 11 *Дата сертификации:* 09.11.2018	*Идентификатор схемы:* 10916 *Документы:* Задание по безопасности Руководство	*Название:* Safari в iOS 11 *Профили защиты:* профиль защиты для прикладного программного обеспечения, расширенный комплект для веб-браузеров
Операционная система: iOS 11 *Дата сертификации:* 13.09.2018	*Идентификатор схемы:* 10915 *Документы:* Задание по безопасности Руководство	*Название:* Контакты в iOS 11 *Профили защиты:* профиль защиты для прикладного программного обеспечения

Сертификация безопасности для интернет-сервисов Apple

Apple поддерживает сертификацию в соответствии со стандартами ISO/IEC 27001 и ISO/IEC 27018. Благодаря этому клиенты Apple могут выполнить законодательные и контрактные обязательства со своей стороны. Сертификация позволяет покупателям получить независимую оценку информационной безопасности и политик конфиденциальности компании Apple в отношении сертифицированных систем.

Стандарты ISO/IEC 27001 и ISO/IEC 27018 входят в семейство стандартов Системы управления информационной безопасностью (ISMS), которые публикует Международная организация по стандартизации (ISO). В рамках системы управления информационной безопасностью Apple все требования по контролю из Приложения A включены в заявление о применимости в соответствии со стандартами ISO/IEC 27001 и ISO/IEC 27018. Apple ежегодно проходит независимую оценку аккредитованным регистратором.

ISO/IEC 27001

ISO/IEC 27001 — это стандарт системы управления информационной безопасностью, определяющий требования к созданию, внедрению, поддержке и постоянному улучшению системы управления информационной безопасностью организации. Стандарт ISO/IEC 27001 рассматривает следующие аспекты безопасности, на которые распространяется сертификация ISO/IEC компании Apple:

- политики информационной безопасности;
- организация информационной безопасности;
- управление ресурсами;
- безопасность персонала;
- физическая и экологическая безопасность;
- управление коммуникациями и операциями;
- управление доступом;
- приобретение, разработка и обслуживание информационных систем;
- урегулирование инцидентов в области информационной безопасности;
- управление непрерывностью бизнеса;
- соответствие требованиям.

ISO/IEC 27018

ISO/IEC 27018 — это свод правил по защите информации, позволяющей установить личность (PII), в общедоступных облачных средах. Стандарт ISO/IEC 27018 рассматривает следующие аспекты безопасности, на которые распространяется сертификация ISO/IEC компании Apple:

- согласие и выбор;
- правомерность и указание цели;
- ограничение сбора;
- минимизация объема данных;
- ограничение использования, хранения и раскрытия информации;
- точность и качество;
- открытость, прозрачность и уведомление;
- участие и доступ лица;
- ответственность;
- информационная безопасность;
- соблюдение требований к конфиденциальности.

Сервисы Apple, на которые распространяются ISO/IEC 27001 и ISO/IEC 27018

Сертификаты ISO/IEC 27001 и ISO/IEC 27018 компании Apple относятся к перечисленным ниже сервисам.

- Деловой чат Apple
- Apple Business Manager
- Сервис Apple Push Notification (APNs)
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- Сервисы iWork
- Управляемые Apple ID
- Задания
- Siri

Сертификация

Подтверждение сертификации Apple по ISO/IEC 27001 и 27018 можно посмотреть у нашего регистратора.

Чтобы просмотреть сертификаты Apple, откройте поиск по реестру сертификатов и клиентов на веб-сайте Британского института стандартов (BSI), введите «Apple» в поле «Company» (Компания), нажмите кнопку «Search» (Поиск), затем выберите результаты поиска для просмотра сертификатов.

Примечание. Предоставление информации о продуктах, произведенных сторонней компанией, или о независимых веб-сайтах, не контролируемых и не проверяемых компанией Apple, не означает их рекомендации или одобрения. Apple не несет никакой ответственности за выбор, функциональность или использование сторонних веб-сайтов или продуктов. Apple не делает никаких заявлений относительно точности или надежности сторонних веб-сайтов. За дополнительной информацией обращайтесь к поставщику.

Проект по обеспечению соблюдения требований безопасности для macOS

Проект по обеспечению соблюдения требований безопасности для macOS (mSCP) — это проект с открытым исходным кодом, направленный на реализацию планомерного подхода к созданию руководств по безопасности. Это совместный проект федеральных оперативных специалистов по ИТ-безопасности из Национального института стандартов и технологий (NIST), Национального управления по аэронавтике и исследованию космического пространства (NASA), Агентства оборонных информационных систем (DISA) и Лос-Аламосской национальной лаборатории (LANL). Проект использует набор протестированных и подтвержденных средств контроля для macOS и сопоставляет их с руководствами по безопасности, поддерживаемыми в рамках проекта. Кроме того, проект облегчает создание настраиваемых базовых уровней безопасности для технических средств обеспечения безопасности за счет использования библиотеки протестированных и подтвержденных элементарных действий (настроек конфигурации). В результате проекта индивидуально создаются документация, скрипты, профили конфигурации и контрольный список проверок на основе используемого базового уровня.

mSCP может генерировать материалы, предназначенные для использования совместно с инструментами управления и безопасности, чтобы обеспечить соответствие требованиям. Настройки конфигурации в этом проекте поддерживают следующие базовые уровни руководств.

Организация	Поддерживаемые базовые уровни
Специальная публикация (SP) 800-53 Национального института стандартов и технологий (NIST), Рекомендуемые средства обеспечения безопасности для федеральных информационных систем и организаций, редакция 5	800-53 высокий, 800-53 средний, 800-53 низкий
Специальная публикация (SP) 800-171 Национального института стандартов и технологий (NIST), Защита контролируемой несекретной информации в нефедеральных системах и организациях, редакция 2	800-171
Руководство по технической реализации в области безопасности для macOS 11 компании Apple (macOS 11 STIG) от Агентства оборонных информационных систем (DISA)	STIG
Инструкция комитета по национальной безопасности (CNSSI) 1253, Классификация безопасности и выбор средств управления для систем национальной безопасности	1253

Дополнительная информация:

- Базовый уровень для просмотра всех правил проекта приведен здесь.
- Чтобы узнать больше о проекте и его использовании, см. вики-страницу проекта по обеспечению соблюдения требований безопасности для macOS.
- Чтобы настроить проект для использования, см. Обзор проекта по обеспечению соблюдения требований безопасности для macOS, часть 1, и Обзор проекта по обеспечению соблюдения требований безопасности для macOS, часть 2.
- Если Вы хотите поддержать развитие проекта, см. руководство для участников.

История правок документа

Дата	Сводка
27 октября 2021 г.	Обновленные разделы: • Сертификация безопасности для процессора Secure Enclave • Сертификация безопасности для iOS • Сертификация безопасности для macOS
17 августа 2021 г.	Обновленные разделы: • Сертификация безопасности для процессора Secure Enclave • Сертификация безопасности для чипа безопасности Apple T2 • Сертификация безопасности для iOS • Сертификация безопасности для iPadOS • Сертификация безопасности для macOS • Сертификация безопасности для tvOS • Сертификация безопасности для watchOS • Сертификация безопасности для приложений Apple • Сертификация безопасности • Проект по обеспечению соблюдения требований безопасности для macOS
26 апреля 2021 г.	Добавленный раздел: • Проект по обеспечению соблюдения требований безопасности для macOS Обновленные разделы: • Сертификация безопасности для чипа безопасности Apple T2: новый сертификат FIPS 140-2, 3811. • Сертификация безопасности для процессора Secure Enclave: новый сертификат FIPS 140-2, 3811, и новая таблица дополнительных сертификатов. • Сертификация безопасности для iOS: новые сертификаты FIPS 140-2, 3811, iOS 14 (идентификатор схемы: 11146) на этапе оценки. • Сертификация безопасности для iPadOS: новые сертификаты FIPS 140-2, 3811, iPadOS 14 (идентификатор схемы: 11147) на этапе оценки. • Сертификация безопасности для macOS: новый сертификат FIPS 140-2, 3811. • Сертификация безопасности для tvOS: новые сертификаты FIPS 140-2, 3811. • Сертификация безопасности для watchOS: новые сертификаты FIPS 140-2, 3811. • Сертификация безопасности для приложений Apple: обновление статуса сертификации по общим критериям и новая таблица архивных сертификатов по общим критериям.

Глоссарий

Группа старших должностных лиц по безопасности информационных систем (SOG-IS) — группа, которая регулирует соглашение о взаимном признании между несколькими европейскими странами.

Задание по безопасности (ST) — документ, в котором определена проблема безопасности и указаны требования к безопасности для определенного продукта.

Заявление о применимости (SOA) — документ, в котором описаны меры безопасности, реализованные в контексте системы управления информационной безопасностью, и который выпускается в поддержку сертификации ISO/IEC 27001.

Клиент IPSec VPN — клиент в профиле защиты, который обеспечивает безопасное соединение IPsec между физической или виртуальной серверной платформой и удаленным объектом.

Компонент, переданный на тестирование (IUT) — криптографический модуль, который проходит тестирование в лаборатории.

Криптографический модуль — оборудование, программное обеспечение и (или) прошивка, которые выполняют криптографические функции и соответствуют требованиям заявленного стандарта криптографических модулей.

Международное техническое сообщество (iTC) — группа, которая отвечает за разработку профилей защиты или совместных профилей защиты в рамках Соглашения о признании общих критериев (CCRA).

Национальное партнерство по обеспечению достоверности информации (NIAP) — организация правительства США, которая отвечает за реализацию стандарта оценки по общим критериям в США и управление Схемой оценки и проверки по общим критериям (CCEVS) NIAP.

Национальный институт стандартов и технологий (NIST) — подразделение Министерства торговли США, которое отвечает за развитие метрологии, а также метрологических стандартов и технологий.

Общие критерии (CC) — стандарт, который устанавливает общие концепции и принципы оценки безопасности информационных технологий и определяет общую модель оценки. Стандарт включает каталоги требований к безопасности на стандартизированном языке.

Полное шифрование диска (FDE) — шифрование всех данных в томе хранилища.

Проверяемые модули (MIP) — список криптографических модулей, которые в настоящий момент проходят проверку по программе проверки криптографических модулей (CMVP). Список ведется CMVP.

Программа проверки криптографических алгоритмов (CAVP) — проект Национального института стандартов и технологий (NIST) по проверке утвержденных (например, одобренных FIPS и рекомендованных NIST) криптографических алгоритмов и их отдельных компонентов.

Программа проверки криптографических модулей (CMVP) — проект правительства США и правительства Канады по проверке соответствия стандарту FIPS 140-3.

Профиль защиты (PP) — документ, в котором определена проблема безопасности и указаны требования к безопасности для определенного класса продуктов.

Процессор Secure Enclave (SEP) — сопроцессор, встроенный в систему на кристалле (SoC).

Сервис Apple Push Notification (APNs) — доступный по всему миру сервис Apple, который обеспечивает доставку push-уведомлений на устройства Apple.

Система на кристалле (SoC) — интегральная микросхема (IC), которая объединяет несколько компонентов на одном чипе.

Система управления информационной безопасностью (ISMS) — набор политик и процедур информационной безопасности, которые устанавливают границы программы безопасности, разработанной для защиты определенного объема информации и систем путем систематического управления информационной безопасностью на протяжении всего жизненного цикла информации или системы.

Совместный профиль защиты (cPP) — профиль защиты, разработанный международным техническим сообществом. Это группа экспертов, которым поручено создание cPP.

Соглашения о признании общих критериев (CCRA) — соглашение о взаимном признании, которое устанавливает политики и требования для международного признания сертификатов, выданных в соответствии со стандартами ISO/IEC 15408 или стандартами оценки по общим критериям.

Управление мобильными устройствами (MDM) — сервис, который позволяет удаленно управлять зарегистрированными устройствами. После регистрации устройства администратор может настраивать параметры и выполнять другие действия с устройством по сети без участия пользователя, используя сервис MDM.

Уровень безопасности (SL) — четыре уровня общей безопасности (1–4), которые определены в ISO/IEC 19790 для описания наборов применимых требований к безопасности. Уровень 4 является самым строгим.

Федеральный стандарт обработки информации (FIPS) — публикации, разработанные Национальным институтом стандартов и технологий для ситуаций, когда это требуется по закону или существуют обязательные требования федерального правительства в отношении кибербезопасности.

Apple Business Manager — простой веб-портал для ИТ-администраторов, который предоставляет организациям быстрый и оптимальный способ развертывания устройств Apple, приобретенных напрямую у Apple либо у авторизованных реселлеров Apple или операторов сотовых сетей. Регистрацию устройств в решении для управления мобильными устройствами (MDM) можно выполнить автоматически. В этом случае не потребуется физически настраивать или подготавливать устройства перед выдачей пользователям.

Apple School Manager — простой веб-портал для ИТ-администраторов, который предоставляет организациям быстрый и оптимальный способ развертывания устройств Apple, приобретенных напрямую у Apple либо у авторизованных реселлеров Apple или операторов сотовых сетей. Регистрацию устройств в решении для управления мобильными устройствами (MDM) можно выполнить автоматически. В этом случае не потребуется физически настраивать или подготавливать устройства перед выдачей пользователям.

corecrypto — библиотека, которая содержит реализации низкоуровневых криптографических примитивов. Учтите, что библиотека corecrypto не предоставляет непосредственно интерфейсы программирования для разработчиков, а используется через API, предоставляемые разработчикам. Исходный код corecrypto является общедоступным, что позволяет проверить его характеристики безопасности и правильность функционирования.

Secure Element (SE) — кремниевый чип, который встроен во многие устройства Apple и поддерживает такие функции, как Apple Pay.

sepOS — прошивка Secure Enclave на основе версии микроядра L4, доработанной компанией Apple.

T2 — чип безопасности Apple, который устанавливается в некоторые компьютеры Mac с процессором Intel начиная с 2017 г.

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

RS028-00499-B