Руководство пользователя

КриптоАРМ Mobile 1.0
для ОС Аврора

ООО «Цифровые технологии», 2025 г.

Назначение и условия применения

Приложение КриптоАРМ предназначено для создания и проверки электронной подписи, шифрования и расшифрования документов посредством использования криптопровайдера КриптоПро CSP.

Криптопровайдер (Cryptography Service Provider, CSP) — это независимый модуль, позволяющий осуществлять криптографические операции с помощью функций CryptoAPI.

Поддерживаемые криптопровайдеры

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версии 5.0 R3 и выше.

Поддерживаемые ключевые носители

В приложении поддерживается работа с ключевыми носителями Рутокен ЭЦП 2.0 USB, Рутокен ЭЦП 2.0 Type-C, Рутокен ЭЦП 3.0 NFC, Рутокен ЭЦП 3.0, Рутокен ЭЦП Type-C 3.0, JaCarta-2 ГОСТ через криптопровайдер КриптоПро CSP.

Лицензия на программный продукт

При первой установке приложения активируется лицензия на КриптоПро CSP сроком на 90 дней. Для работы с приложением необходима лицензия (временная, годовая или бессрочная).

Временная лицензия выдаётся пользователю, заполнившему форму на странице для знакомства с продуктом сроком на 30 дней.

После истечения ознакомительного периода для полнофункциональной работы приложения требуется приобретение и установка годовой или бессрочной лицензии. Без установки лицензии операции подписи, расшифрования, установления TLS-соединения выполняться не будут.

Для приобретения лицензии на программный продукт КриптоАРМ можно обратиться в компанию, разрабатывающую приложение.

Системные требования

Для приложения сформулированы минимальные системные требования к конфигурации оборудования под платформу Аврора:

- операционная система: Аврора 4.0 и выше;
- оперативная память: 2Гб и выше;
- встроенная память: 16ГБ и выше;
- разрешение экрана: 720x1280пикс и выше;
- доступ к сети Интернет: рекомендуем;
- фото-камера: рекомендуем, 8МП и выше;
- наличие функции USB-host, NFC.

Функциональность версии

Функциональность версии 1.0.

Приложение текущей версии рассчитано на выполнение операций:

Операция	
Электронная подпись	электронная подпись произвольных файлов размером до 50 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память

	проверка электронной подписи файлов размером до 50 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память
	создание присоединенной и отсоединенной электронной подписи
	создание усовершенствованной подписи
	поддержка стандарта электронной подписи ГОСТ Р 34.10-2012
	добавление электронной подписи (функция соподписи)
Шифрование/ расшифрование	шифрование и расшифрование файлов размером до 50 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память
	шифрование по стандарту PKCS#7/CMS

Управление сертификатами и ключами	отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров
	проверка корректности выбранного сертификата с построением цепочки доверия
	хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.) при условии использования криптопровайдера КриптоПро CSP
	создание запросов на сертификат
	импорт сертификатов с привязкой к закрытому ключу
	экспорт сертификатов
	удаление сертификатов

Работа с журналом событий и уведомлениями	отображение списка событий по уровням детализации
	просмотр уведомлений о событиях
Работа с файлами в каталоге Архив	сохранение всех результатов операций с файлами в каталоге Архив

Установка КриптоАРМ

Установка приложения КриптоАРМ на платформе Аврора

Установка и обновление приложения КриптоАРМ происходит через платформу управления корпоративными мобильными устройствами и приложениями Аврора Центр.

Установка лицензии на программный продукт КриптоАРМ

Для полноценной работы приложения КриптоАРМ необходима лицензия. Существуют бессрочная, годовая и временная лицензии.

Временная лицензия предоставляется с ограниченным сроком действия 30 дней. Для получения временной лицензии необходимо заполнить форму на странице.

Для приобретения годовой или бессрочной лицензии можно обратиться в компанию, разрабатывающую приложение.

Установка лицензии КриптоАРМ

Для установки ключа активации лицензии нужно перейти в раздел **О приложении** (**Ещё** — **О приложении** — **Ввести лицензию**). Ввести ключ активации лицензии и нажать на **Подтвердить**.

При успешной установке обновится информация о статусе и дате истечения лицензии.

Установка КриптоПро CSP

Установка программного обеспечения КриптоПро CSP без ввода лицензии подразумевает использование временной лицензии с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Установка лицензии КриптоПро CSP

Установка ключа активации лицензии производится через пользовательский интерфейс приложения КриптоПро CSP.

Для установки ключа активации лицензии нужно **Открыть** приложение КриптоПро CSP, **Ввести лицензию** — **ОК**.

Описание раздела Документы

Работа с приложением КриптоАРМ начинается с раздела **Документы**.

Блок **Профили** предназначен для настройки и управления параметрами операций (подпись, шифрование, выбор сертификатов и т. д.) и перехода в мастер **Подпись и шифрование**, **Проверка и расшифрование**.

Ниже размещён блок **Архив**. Здесь представлен список документов, которые пользователь сохраняет при подписании/шифровании файлов. Для этого необходимо при создании профиля или при работе в мастерах активировать функцию **Сохранять копии документов из результатов операций**. Документы расположены в папке пользователя в каталоге **\Documents\cryptoarmgost**.

В нижней панели расположены кнопки для перехода в разделы **Документы**, **Сертификаты**, **Журнал**. При нажатии на кнопку **Ещё** открывается список всех разделов.

Через drop-down меню можно:

- **Обновить** раздел и список документов в Архиве;
- **Сортировать по: Названию/Дате изменения/Размеру/Типу** — сортировка документов в блоке Архив;
- **Выбрать документы**, которые указаны в блоке Архив;
- **Поиск** — можно ввести название документа или сертификата для его поиска.

Создание профиля подписи

Для подписания и шифрования файлов необходимо создать профиль подписи.

Профиль подписи — шаблон настроек для выполнения операций подписи, архивирования и шифрования для разных ситуаций. Для обмена документами с бухгалтером вы можете установить и использовать один профиль, с партнерами — второй, с клиентами — третий.

Создание профиля подписи

1. Открыть раздел **Документы**.
2. Нажать на кнопку **Создать профиль**.
3. Ввести **Название профиля** и **нажать** на ползунки необходимых операций (Подпись, Архивирование, Шифрование). Ниже откроются настройки для каждого вида операций.
4. Нажать на кнопку **Сохранить** в правом верхнем углу.

Описание полей профиля

- **Название профиля** — название профиля подписи для удобства поиска.
- **Операции** — подпись, архивирование, шифрование, другими словами, операции, которые нужно выбрать.

В зависимости от выбранных параметров станут доступны дополнительные поля:

- **Операция Подпись**, доступные поля:
- **Сохранение результатов** — позволяет создать копии файлов в папке **Архив** на устройстве.
- **Выберите сертификат** — для выбора доступны личные сертификаты с привязкой к закрытому ключу.
- **Стандарт подписи** — **CMS** для создания классической подписи или **CAdES-X Long Type 1** и **CAdES-T** для усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 или CAdES-T требуется заполнить поле **Служба штампов времени (TSP)**. Стандарт подписи CAdES-X Long Type 1 и CAdES-T доступны только при установленных модулях КриптоПро TSP Client и КриптоПро OCSP Client.
- **Вид подписи** — **Присоединённая** или **Отсоединённая**.
- **Кодировка подписи** — сохранение подписи в кодировке BASE64 или DER.
- **Расширение** — выбрать расширение итоговых файлов в формате .sig, .sgn, .sign, .p7s, .bin.
- **Операция Архивирование**, доступная настройка:
- **Сохранение результатов на устройстве** — позволяет создать копии файлов в папку Архив.
- **Операция Шифрование**, доступные поля:
- **Сохранение результатов** — позволяет создать копии файлов в папке **Архив** на устройстве.
- **Выберите сертификаты** — для выбора доступны личные сертификаты и сертификаты других пользователей.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: ГОСТ 28147-89, ГОСТ Р 34.12-2015 Магма, ГОСТ Р 34.12-2015 Кузнечик. Данный параметр доступен для выбора только начиная с версии КриптоПро CSP 5.0.11635.
- **Кодировка файлов** — сохранение зашифрованного файла в кодировке BASE64 или DER.
- **Удалить исходные файлы после шифрования** — исходные файлы в случае успешного завершения операции удаляются из файловой системы.

Редактирование профиля подписи

1. В блоке **Профили** нажать на кнопку **Все**.
2. Вызвать контекстное меню (удерживать название нужного профиля).
3. Нажать на **Редактировать**.
4. Изменить нужные параметры.
5. **Сохранить**.

Удаление профиля подписи

Удаление профиля подписи из списка профилей подписи

1. В блоке **Профили** нажать на кнопку **Все**.
2. Вызвать контекстное меню (удерживать название нужного профиля).
3. **Удалить**.

Для отмены удаления профиля нужно нажать на всплывающее окно сверху **Коснитесь для отмены Удаление профиля**.

Подписание документа

Чтобы подписывать документы электронной подписью, нужно установить в Личное хранилище сертификат с закрытым ключом.

Подписать документы вы можете в мастере **Подписи и шифрования** в разделе **Документы**.

Вы можете подписать документы, выбрав файлы из вкладки Архив или выбрав профиль подписи в блоке **Профили**.

Подпись документа с использованием профиля подписи

1. Открыть раздел **Документы**.
2. Создать профиль подписи, в котором заданы нужные настройки подписи.

3. В разделе **Документы** выбрать нужный профиль подписи. При выборе профиля в мастере автоматически заполняются **Настройки операций**, сохранение результатов на устройстве.
4. **Добавить** документы.
5. Нажать кнопку **Выполнить**.
6. Ввести пароль и нажать на **Ок**.

Подпись документа с использованием мастера Подпись и шифрование

1. Нажать на иконку **Подпись и шифрование**.
2. Нажать на **Подпись** в **Настройках профиля**.
3. Настроить нужные параметры (операции, сохранение результатов на устройстве, сертификат подписи, параметры подписи).
4. Вернуться на предыдущий экран.
5. **Выбрать сертификат**. Откроется список личных сертификатов. Выбрать нужный и нажать на кнопку **Выбрать** (если не было выбрано при настройке параметров).
6. **Добавить документы**.
7. Нажать кнопку **Выполнить**.
8. Ввести пароль и нажать на **Ок**.

Создание усовершенствованной подписи

Усовершенствованная квалифицированная электронная подпись поможет доказать юридическую значимость документа в спорных ситуациях. Например, когда помимо авторства и целостности документа (которые дает обычная КЭП) необходимо подтвердить, что сертификат был действителен в момент подписания документа.

Формат усовершенствованной подписи предусматривает включение в электронную подпись информации о времени создания подписи (TSP) и о статусе сертификата электронной подписи (OCSP) в момент подписания.

1. Открыть раздел **Документы**.
2. Создать профиль подписи или открыть мастер **Подписи и шифрования**. Указать следующие параметры подписи:

- стандарт — CAdES-X Long Type 1 либо CAdES-T, вид, кодировку, формат файла подписи, сохранение результатов в **Архив**;
- опция **Штамп времени на подпись** включена, отключить нельзя;

- заполнить в поле **Служба штампов времени (TSP)** адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: \<протокол>://\<сервер>[:порт][/путь];
- заполнить в поле **Служба онлайн статусов (OCSP)** адрес службы OCSP. Чаще всего адрес прописан в самом сертификате, которым создаётся подпись.

3. Добавить документы.
4. Нажать на кнопку **Выполнить**.
5. Ввести пароль и нажать на **Ок**.

Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут подписанные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — информация о подписи и сертификате подписи;
- **Открыть** — файл откроется в мастере **Проверка и расшифрование**;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: информация о подписи и сертификате подписи.

Шифрование документа

Чтобы шифровать документы, нужно установить в хранилище Другие пользователи сертификат электронной подписи.

Зашифровать документы вы можете в мастере **Подписи и шифрования** в разделе **Документы**.

Вы можете зашифровать документы, выбрав файлы из блока **Архив** или выбрав профиль подписи в блоке **Профили подписи**.

Шифрование документа с использованием профиля подписи

1. Открыть раздел **Документы**.
2. Создать профиль подписи, в котором заданы нужные настройки шифрования.
3. В разделе **Документы** выбрать нужный профиль подписи. При выборе профиля в мастере автоматически заполняются **Настройки операций**, сохранение результатов на устройстве.
4. **Выберите сертификаты** из списка сертификатов других пользователей (если не было указано в настройках профиля).
5. **Добавить документы**.
6. Нажать кнопку **Выполнить**.

Шифрование документа с использованием мастера Подпись и шифрование

1. Нажать на мастер **Подпись и шифрование**.
2. Нажать на **Подпись** в **Настройках профиля**.
3. Изменить операцию **Подпись** на операцию **Шифрование**.
4. Настроить нужные параметры (сохранение результатов на устройстве, алгоритм шифрования и кодировка файлов, выбор сертификата и удаление исходных файлов после шифрования).
5. Вернуться на предыдущий экран.
6. **Выберите сертификаты** (если не было сделано на предыдущем шаге).
7. **Добавить документы**.
8. Нажать кнопку **Выполнить**.

Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут зашифрованные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — название, дата создания и изменения, тип документа, формат, размер, путь;
- **Открыть** — файл откроется в мастере **Проверка и расшифрование**;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;

- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: название, дата создания и изменения, тип документа, формат, размер, путь.

Архивирование документа

Архивировать документы можно в мастере **Подписи и шифрования** или создав профиль подписи с операцией Архивирование.

Для архивирования документов дополнительных настроек нет.

Архивирование документа через мастер Подпись и шифрование

1. Открыть раздел **Документы**.
2. Нажать на мастер **Подпись и шифрование**.
3. Нажать на **Подпись** в **Настройках профиля**.
4. Выбрать операцию **Архивирование**.
5. При необходимости выбрать **Сохранять копии документов из результатов операций**.
6. Вернуться на предыдущий экран.
7. **Добавить документы**.
8. Нажать на **Выполнить**.

Архивирование документа с помощью профиля подписи

1. Открыть раздел **Документы**.
2. Выбрать ранее созданный профиль подписи с операцией **Архивирование**.
3. **Добавить документы**.
4. Нажать на **Выполнить**.

Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут заархивированные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — название, дата создания и изменения, тип документа, формат, размер, путь;
- **Открыть** — будет предложено приложение для открытия заархивированного файла;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: название файла, тип документа, формат, размер, дата создания и изменения, путь.

Проверка подписи документа

Для проверки подписи достаточно выделить файл расширением .sig, , .p7s, .sgn, .sign, .bin, который содержит электронную подпись. Никаких дополнительных настроек при проверке подписи производить не нужно.

Проверка подписи документа с помощью мастера Проверка и расшифрование

1. Открыть раздел **Документы**.
2. Выбрать мастер **Проверка и расшифрование**.
3. **Добавить документы**.
4. Результаты проверки будут на экране (**Подпись подтверждена** или **Подпись не подтверждена**).

Проверка подписи документа через контекстное меню

1. Открыть раздел **Документы**.
2. В **Архиве** вызвать контекстное меню у нужного файла.

3. Выбрать **Добавить в** — **Проверка и расшифрование**.
4. Результаты проверки будут на экране (**Подпись подтверждена** или **Подпись не подтверждена**).

Результат выполнения операции

В окне результатов операций мастера **Проверки и расшифрования** будут загруженные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — информация о подписи и сертификате подписи;
- **Копировать в папку Архив** — файл будет скопирован в папку Архив;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: информация о подписи и сертификате подписи.

Расшифрование документа

Для расшифрования у вас в хранилище Личных сертификатов должен быть сертификат с закрытым ключом, который был выбран в качестве сертификата получателя при шифровании.

Для расшифрования нужно выбрать зашифрованные файлы с расширением .enc.

Расшифрование документа с помощью мастера Проверка и расшифрование

1. Открыть раздел **Документы**.
2. Выбрать мастер **Проверка и расширование**.
3. Добавить документ. Начнётся операция расшифрования.
4. Ввести пароль и нажать **Ок**.
5. Результаты проверки будут на экране (расшифрованный файл или **Ошибка**).

Ошибка означает, что на устройстве отсутствует личный сертификат с закрытым ключом, в адрес которого происходило шифрование.

Расшифрование документа через контекстное меню

1. Открыть раздел **Документы**.
2. В **Архиве** вызвать контекстное меню у нужного файла.
3. Выбрать **Добавить в** — **Проверка и расшифрование**.
4. Ввести пароль и нажать **Ок**.
5. Результаты проверки будут на экране (расшифрованный файл или **Ошибка**).

Результат выполнения операции

В окне результатов операций мастера **Проверки и расшифрования** будут расшифрованные файлы. При нажатии на **контекстное меню** можно:

- изучить **Свойства документа** (название документа, тип, размер, дата создания и изменения, путь);
- **Копировать в папку Архив** — файл будет скопирован в папку Архив;
- **Открыть в...** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства.

Соподпись (добавление подписи к файлу)

Чтобы подписывать документы электронной подписью, нужно установить в Личное хранилище сертификат с закрытым ключом.

Вы можете добавлять подпись к уже подписанному файлу.

Для этого в мастер **Подпись и шифрование** загрузите файлы с расширением .sig, , .p7s, .sgn, .sign, .bin с устройства.

Для всех добавленных подписей настройки, такие как кодировка и вид, используются по умолчанию, как для первой подписи.

Стандарт подписи, использование штампов времени, сертификат подписи, каталог для сохранения подписанного документа вы можете настроить в профиле подписи или в настройках операций в мастере.

Добавление подписи с использованием профиля подписи

1. Открыть раздел **Документы**.
2. Выбрать нужный профиль подписи.
3. Выбрать сертификат подписи.
4. Добавить уже подписанные документы с устройства.
5. Нажать на **Выполнить**.
6. **Ввести** пароль.

Добавление подписи с использованием мастера Подпись и шифрование

1. Открыть раздел **Документы**.
2. Нажать на мастер **Подпись и шифрование**.
3. Задать настройки профиля (операция **Подпись** и иные параметры).
4. Выбрать сертификат подписи.
5. Добавить уже подписанные документы с устройства.
6. Нажать на **Выполнить**.
7. **Ввести** пароль.

Добавление подписи к файлу, расположенному в блоке Архив

1. Открыть раздел **Документы**.
2. Вызвать **контекстное меню** подписанного документа.
3. Нажать на **Открыть в**.
4. Выбрать мастер **Подпись и шифрование**.
5. Указать настройки профиля подписи и выбрать сертификат подписи.
6. **Выполнить**.
7. **Ввести** пароль.

Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут подписанные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — информация о подписи и сертификате подписи;
- **Открыть** — файл откроется в мастере **Проверка и расшифрование**;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: информация о подписи и сертификате подписи.

Снятие подписи с файла

Для снятия подписи достаточно выбрать файлы с расширением .sig, .p7s, .sgn, .sign, .bin которые содержат электронную подпись. Никаких дополнительных настроек производить не нужно.

Снятие подписи с файла с помощью мастера Проверка и расшифрование

1. Открыть раздел **Документы**.
2. Открыть мастер **Проверка и расшифрование**.
3. **Добавить документы**.
4. Нажать на файл.
5. В открывшемся окне **Свойства документа** выбрать **Показать оригинал**.

Снятие подписи с файла через контекстное меню

1. Открыть раздел **Документы**.
2. Открыть контекстное меню подписанного документа, расположенного во вкладке **Архив**.

3. Выбрать **Добавить в** — **Проверка и расшифрование**.
4. Нажать на файл.
5. В открывшемся окне **Свойства документа** выбрать **Показать оригинал**.

Результат выполнения операции

При нажатии на **контекстное меню** можно:

- изучить **Свойства документа** (название документа, тип, размер, дата создания и изменения, путь);
- **Копировать в папку Архив** — файл будет скопирован в папку Архив;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства.

Прямые групповые операции

Вы можете выполнять подпись, архивирование и шифрование за одну операцию. Это будут прямые групповые операции. Они выполняются в мастере Подпись и шифрование.

Вы можете комбинировать операции и выбрать одну из комбинаций:

- Подпись и архивирование – документ сначала подписывается, затем архивируется;
- Подпись и шифрование – документ сначала подписывается, затем шифруется;
- Архивирование и шифрование – документ сначала архивируется, затем шифруется;
- Подпись, архивирование и шифрование – документ сначала подписывается, затем архивируется, потом шифруется.

Важно: чтобы подписывать и зашифровывать документы, у вас должна быть действительная лицензия на криптопровайдер КриптоПро CSP.

Чтобы подписывать документы электронной подписью, нужно установить в Личное хранилище сертификат с закрытым ключом.

Чтобы шифровать документы, нужно установить в хранилище Других пользователей сертификат.

Прямые групповые операции в мастере Подпись и шифрование

1. Открыть раздел **Документы**.
2. Открыть мастер **Подпись и шифрование**.
3. Открыть настройки профиля, указать нужные операции и их параметры.
4. Выбрать сертификат/сертификаты (сертификат для подписания документов, сертификат для шифрования документов).
5. Добавить документы с устройства.
6. Нажать на **Выполнить**.
7. Ввести пароль и нажать **Ок**.

Прямые групповые операции в профиле подписи

1. Открыть раздел **Документы**.
2. Выбрать нужный профиль подписи, в котором заданы операции и настройки операций.
3. Выбрать сертификат/сертификаты (сертификат для подписания документов, сертификат для шифрования документов).
4. Добавить документы с устройства.
5. Нажать на **Выполнить**.
6. Ввести пароль и нажать **Ок**.

Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут подписанные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — название, дата создания и изменения, тип документа, формат, размер, путь;
- **Открыть** — файл откроется в мастере **Проверка и расшифрование**;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;

- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: название, дата создания и изменения, тип документа, формат, размер, путь.

Обратные групповые операции

Вы можете выполнять расшифрование, разархивирование, проверку и снятие подписи. Для их выполнения предназначен мастер Проверки и расшифрования.

Важно: чтобы проверять подпись и расшифровывать документы, у вас на устройстве должна быть действительная лицензия на криптопровайдер КриптоПро CSP.

Чтобы расшифровывать документы, нужно установить в Личное хранилище сертификат с закрытым ключом.

По итогам проверки подписанных документов в списке выводится информация о подписи.

Для выполнения обратных операций выбор профиля подписи и настройка параметров операций не требуется.

1. Открыть раздел **Документы**.
2. Открыть мастер **Проверка и расшифрование**.
3. Выбрать документ.
4. Ввести пароль и нажать **Ок**, если файл был зашифрован.

На вкладке Проверка и расшифрование отображаются ход и результаты выполнения операций:

- **Подпись подтверждена** означает успешную проверку подписи — подпись была создана для проверяемого документа, в последующем документ не был изменён.
- **Подпись не подтверждена** означает, что на устройстве отсутствует личный сертификат с закрытым ключом, в адрес которого происходило шифрование, либо подпись не подтверждена.

В окне результатов операций мастера **Проверки и расшифрования** будут загруженные файлы. При открытии контекстного меню будут доступны следующие функции:

- просмотреть **Свойства документа** — информация о подписи и сертификате подписи;
- **Копировать в папку Архив** — файл будет скопирован в папку Архив;
- **Добавить в** — откроется список мастеров **Подпись и шифрование**, **Проверка и расшифрование**, а также профили подписи;
- **Удалить** — файл будет удалён с устройства. Для отмены нужно нажать на всплывающее окно сверху.

При нажатии на файл откроются **Свойства документа**: информация о подписи и сертификате подписи.

Раздел Сертификаты

Для того чтобы попасть в раздел **Сертификаты**, нужно в нижней панели выбрать раздел **Сертификаты**. При нажатии на кнопку **Ещё** открывается список всех разделов.

Раздел состоит из двух вкладок: **Добавление сертификатов** и список сертификатов одного из хранилищ.

Добавление сертификатов позволяет создать запрос на сертификат или импортировать сертификат из файла.

В правом верхнем меню можно переключаться между списками хранилищ:

- **Личные сертификаты** — для управления личными сертификатами, у которых есть привязка к закрытому ключу;
- **Сертификаты других пользователей** — сертификаты, открытые ключи которых установлены на устройство и в адрес которых можно шифровать документы;
- **Удостоверяющие центры** — для управления доверенными корневыми сертификатами;
- **Списки отзыва** — для управления списками отзыва сертификатов;
- **Запросы** — для управления запросами на сертификат;
- **Ключи** — для отображения ключевых контейнеров.

Через drop-down меню можно:

- **Выбрать сертификаты** — откроется список сертификатов;
- **Поиск** — можно ввести название документа или сертификата для его поиска;
- **Обновить** раздел и список сертификатов.

Установка личного сертификата

Если у вас сертификат на защищённом носителе или в локальном хранилище устройства, то воспользуйтесь инструкцией по установке сертификата из ключевого контейнера.

Если у вас есть сгенерированный закрытый ключ и вы получили сертификат в Удостоверяющем центре, то для установки сертификата воспользуйтесь инструкцией по установке сертификата с привязкой к ключевому контейнеру.

Перед импортом личного сертификата убедитесь, что у вас действительная лицензия на криптопровайдер КриптоПро CSP.

Примечание: для того чтобы сертификат был действительный, у вас должны быть установлены корневые сертификаты УЦ и актуальный список отзыва сертификатов (COC).

Установка сертификата из ключевого контейнера

Данный способ возможен, если сертификат присутствует в контейнере. Иначе функция установки будет недоступна.

1. Подключить защищённый носитель к устройству.
2. Открыть раздел **Сертификаты**.
3. В правом верхнем меню выбрать хранилище **Ключи**.
4. Вызвать **контекстное меню** у нужного контейнера.
5. Выбрать **Установить сертификат**.
6. При необходимости ввести пароль к ключевому контейнеру.

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

Установка сертификата с закрытым ключом из файла .pfx

1. Открыть раздел **Сертификаты**.
2. Нажать на **Импорт из файла**.
3. В файловом менеджере выбрать файл сертификата .pfx.
4. Ввести пароль к контейнеру pfx.
5. Задать новый пароль к ключевому контейнеру.

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

Установка сертификата с привязкой к ключевому контейнеру

1. Открыть раздел **Сертификаты**.
2. Нажать на **Импорт из файла**.
3. В файловом менеджере выбрать файл сертификата .cer или .crt.

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

Установка сертификата с помощью QR-кода

1. Установить КриптоПро CSP 5.0 R2 на компьютер.
2. Запустить утилиту **Инструменты КриптоПро**.
3. В списке выбрать раздел **Сертификаты**.
4. Выделить нужный сертификат и нажать на кнопку **Экспортировать ключи**.

Сертификат подписи должен быть экспортируемым, в противном случае ключ нельзя будет перенести.

5. В появившемся окне **Ввод пароля на PFX** пропустить, вводить не обязательно.
6. Выбрать опцию **Экспортировать PFX в QR-код**.
7. В выпадающем меню **Выберите приложение** указать КриптоАРМ ГОСТ.
8. Ввести пароль на контейнер и нажать на **Ок**.
9. Запустить КриптоАРМ ГОСТ 3 на смартфоне.
10. Открыть раздел **Сертификаты**.
11. Выбрать **Добавить с QR-кода**.
12. При необходимости дать разрешение приложению снимать фото и видео.
13. Отсканировать QR-код с экрана компьютера.

14. Назначить пароль на контейнер.
15. Ввести пароль для контейнера и нажать на **Ок**.
16. Ввести пароль на PFX (см. п. 6, данный пароль может быть не задан при экспорте) и **Далее**.

Сертификат успешно установлен и готов для подписания и расшифрования электронных документов.

Установка корневого и промежуточного сертификатов

Установить корневой или промежуточный сертификат вы можете в хранилище **Удостоверяющие центры** раздела **Сертификаты**.

1. Открыть раздел **Сертификаты**.
2. В правом верхнем меню выбрать хранилище **Удостоверяющие центры**.
3. Нажать на кнопку **Импорт из файла**.
4. Выбрать **Загрузить из файла**.
5. В файловом менеджере выбрать файл сертификата.
6. Подтвердить запрос на установку сертификата.

При успешном импорте сертификат появится в списке хранилища **Удостоверяющие центры**.

Создание запроса на сертификат

Чтобы получить личный сертификат для выполнения криптографических операций, необходимо создать запрос на сертификат и направить его на рассмотрение в Удостоверяющий центр (УЦ).

1. Открыть раздел **Сертификаты**.
2. Нажать на **Запрос на сертификат**.
3. При необходимости выбрать **Шаблон сертификата** — По умолчанию / Сертификат КЭП ИП / Сертификат КЭП физического лица / Сертификат КЭП юридического лица / Шаблон с расширенным списком полей.
4. При необходимости активировать опцию **Создать как самоподписанный**.
5. Заполнить сведения о владельце. Набор полей меняется в зависимости от выбранного шаблона.

6. Указать **параметры ключа**: алгоритм, назначение ключа и возможность его экспортировать (данная опция позволит экспортировать сертификат вместе с закрытым ключом для переноса на другое устройство).
7. При необходимости выбрать **использование ключа** и **назначение сертификата**.
8. Нажать на **Подтвердить**.
9. Нажимать на экран в рандомном порядке, пока ключ не будет создан.
10. Ввести и подтвердить пароль, нажать на **Ок**.

На основе указанных данных формируется запрос на сертификат, который отображается в хранилище **Запросы**. Можно изучить его свойства, экспортировать или удалить.

Созданный файл запроса на сертификат следует направить на рассмотрение в Удостоверяющий центр (УЦ). Полученный из УЦ сертификат следует импортировать для работы в приложении.

Импорт сертификатов других пользователей

Установка сертификата, который был отправлен вам другим пользователем, происходит в хранилище сертификатов других пользователей. Он нужен для шифрования документов в адрес этого сертификата. Такой сертификат импортируется без закрытого ключа.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Сертификаты других пользователей**.
3. Нажать на кнопку **Импорт из файла**.
4. В файловом менеджере выбрать файл сертификата.
5. Подтвердить помещение сертификата хранилище **Других пользователей** (текущее).

При успешном импорте сертификат появится в хранилище сертификатов **Других пользователей**.

Установка списка отзыва сертификатов

Список отзыва сертификатов (COC/CRL) — документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было временно приостановлено.

1. Открыть раздел **Сертификаты**.
2. В правом верхнем меню выбрать хранилище **Списки отзыва**.
3. Нажать на **Импорт из файла**.
4. В файловом менеджере выбрать файл списка отзыва с расширением .crl.
5. Подтвердить добавление сертификата в списки отзыва, нажав на **Выбрать**.

При успешном импорте СОС отображается в хранилище **Списки отзыва** со статусом *Действителен*.

При вызове контекстного меню можно:

- изучить **Свойства списка отзыва** — данные о сертификате;
- **Экспортировать** — экспорт сертификата в файл формата .cer;
- **Удалить** — удаление СОС с устройства.

Экспорт личного сертификата

Для обмена шифрованными данными с другими пользователями необходимо экспортировать сертификат без закрытого ключа.

Экспорт сертификата с закрытым ключом нужен в следующих ситуациях:

- сохранение копии сертификата и связанного с ним закрытого ключа;
- удаление сертификата и его закрытого ключа с устройства для установки на другое устройство.

Экспорт сертификата без закрытого ключа

1. Открыть раздел **Сертификаты** — хранилище **Личные сертификаты**.
2. Вызвать контекстное меню у нужного сертификата.
3. Выбрать **Экспортировать**.
4. Ввести пароль на контейнер.
5. В открывшемся окне выбрать нужные настройки (не экспортировать закрытый ключ, тип кодировки). Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый.
6. **Подтвердить**.
7. Выбрать папку для сохранения экспортируемого сертификата.
8. Назвать файл и **Подтвердить**.

При успешном выполнении операции сертификат экспортируется в файл формата .cer.

Экспорт сертификата с закрытым ключом в контейнер PFX

Важно: вы можете экспортировать сертификат вместе с закрытым ключом, если ключ имеет флаг "экспортируемый". В противном случае эта функция недоступна.

1. Открыть раздел **Сертификаты** — хранилище **Личные сертификаты**.
2. Вызвать контекстное меню у нужного сертификата.
3. Выбрать **Экспортировать**.
4. Ввести пароль на контейнер.
5. В открывшемся окне выбрать нужные настройки (экспортировать закрытый ключ, тип кодировки). Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый. **Задать** пароль к файлу .pfx.
6. **Ввести** пароль к сертификату.
7. Выбрать папку для сохранения экспортируемого сертификата.
8. Назвать файл и **Подтвердить**.

При успешном выполнении операции сертификат экспортируется в файл формата .pfx.

Экспорт сертификата

Сертификаты других пользователей, корневые и промежуточные сертификаты экспортируются без закрытого ключа.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Сертификаты других пользователей** или **Удостоверяющие центры**.
3. Вызвать контекстное меню у нужного сертификата.
4. Выбрать **Экспортировать**.
5. Указать тип кодировки DER или BASE64.
6. **Подтвердить**.
7. Выбрать папку для сохранения экспортируемого сертификата.
8. Назвать файл и **Подтвердить**.

При успешном выполнении операции сертификат экспортируется в файл формата .cer.

Удаление сертификата

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище, из которого необходимо удалить сертификат.
3. Вызвать контекстное меню у нужного сертификата.
4. При необходимости **Удалить связанный с сертификатом контейнер**.
5. Выбрать **Удалить**.
6. Подтвердить удаление.

Сертификат будет успешно удален из хранилища.

Ключевые контейнеры

В программе отображаются ключевые контейнеры, расположенные на устройстве и на отчуждаемых носителях, например, USB-токенах или смарт-картах.

Просмотр сертификата в контейнере

1. При необходимости подключить защищённый носитель к устройству.
2. Открыть раздел **Сертификаты**.
3. Открыть хранилище **Ключи**.
4. Нажать на контейнер.

Откроется информация о сертификате в контейнере.

Установка сертификата из ключевого контейнера

Примечание: данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключить защищённый носитель к устройству.
2. Открыть раздел **Сертификаты**.
3. Открыть хранилище **Ключи**.
4. Вызвать контекстное меню.
5. **Установить сертификат**.
6. При необходимости ввести пароль к ключевому контейнеру.

Удаление сертификата

Важно: удалённый контейнер не подлежит восстановлению! Вам придется перевыпускать сертификат.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Ключи**.
3. Вызвать контекстное меню.
4. **Удалить**.
5. **Удалить связанный с контейнером сертификат**.
6. **Удалить**.

Для отмены удаления коснуться верхней панели.

Журнал

Информация о событиях, происходящих в рамках приложения, записывается в **Журнал** .

События в журнале разделяются по уровням логирования: Информация и Ошибка.

Информация включает в себя все сообщения, информирующие о действиях, например, операция подписи, экспорт сертификата.

Ошибка сообщает об ошибках в работе приложения.

При вызове контекстного меню можно **Экспортировать в файл** и сохранить на устройстве.

Просмотр информации о событии

Для просмотра подробной информации о событии нужно нажать на запись в списке журнала.

При вызове контекстного меню информацию о событии можно **Экспортировать в файл**.

При нажатии на **Поиск** можно осуществлять поиск по ключевым словам.

Через drop-down меню можно:

1. **Выбрать оповещения** — множественный выбор оповещений, которые в дальнейшем можно **Экспортировать**;
2. **Фильтр** — откроется окно выбора следующих параметров:
3. **Выбрать дату** — выбор календарной даты или диапазон дат;
4. **Приложение** — выбор раздела, в котором возникло событие;
5. **Уровень** — выбор уровень логирования (информация или ошибка).

Для отмены параметра фильтрации необходимо нажать на отмену для конкретного параметра.

Работа с защищёнными носителями

В мобильном приложении КриптоАРМ поддерживается работа с ключевыми носителями через криптопровайдер КриптоПро CSP:

- Рутокен ЭЦП 2.0 USB;
- Рутокен ЭЦП 2.0 Type-C;
- Рутокен ЭЦП 3.0 USB;
- Рутокен ЭЦП 3.0 Type-C;
- Смарт-карта Рутокен ЭЦП 3.0 NFC;
- JaCarta-2 ГОСТ.

Подключение защищённых носителей

Важно: устройство должно поддерживать функцию USB-OTG для работы с USB-токенами и функцию NFC для работы со смарт-картами.

Защищённые носители USB и Type-C достаточно вставить в разъем устройства или подключить через переходник.

Для подключения **смарт-карты NFC** необходимо:

- включить функцию NFC на устройстве;
- приложить смарт-карту к задней панели устройства.

Установка ключей

1. Запустить приложение КриптоАРМ.
2. Подключить защищённый носитель.
3. Открыть раздел **Сертификаты** — **Ключи**.
4. **Установить** сертификат через контекстное меню.
5. Открытый ключ установится в хранилище **Личные сертификаты**.