



УТВЕРЖДАЮ

Директор ООО «Эксперт»

Перлов Э.Н.

07 июля 2025 г.

Стандартная инструкция по оформлению и передаче электронных документов, подписанных электронной подписью

Данная инструкция разработана в соответствии с положениями Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и регламентирует порядок подготовки и передачи электронных документов, подписанных специальными цифровыми подписями для подтверждения их подлинности.

1. Общие положения

1. Электронные документы подлежат обязательному подписанию электронной подписью (ЭП), если иного не предусмотрено федеральным законом или договором.
2. Подпись производится сертифицированными средствами криптографической защиты информации (СКЗИ), допущенными к использованию в России.
3. Используются следующие типы электронных подписей:
 - простая электронная подпись (ПЭП);
 - усиленная неквалифицированная электронная подпись (УНП);
 - усиленная квалифицированная электронная подпись (УКЭП).

2. Порядок подписания электронных документов

1. Для подписания электронного документа необходима регистрация сертификата ключа проверки электронной подписи (СКЭП) в аккредитованном удостоверяющем центре (УЦ).
2. Документ формируется в цифровом формате (.pdf, .docx, .xls и т.п.) и подписывается соответствующей ЭП с помощью специальных программных средств (например, КриптоАРМ, CryptoPro CSP).
3. Рекомендуются использовать усиленную квалифицированную электронную подпись (УКЭП), обеспечивающую максимальный уровень защиты.

3. Формат представления электронных документов

Электронные документы предоставляются в одном из следующих форматов:

- PDF/A с вложением электронной подписи (*.p7s или *.sig);
- XML с применением XAdES или CAdES стандартов;
- Другие утвержденные Министерством цифрового развития, связи и массовых коммуникаций РФ форматы.

4. Передача подписанных документов

1. Отправка электронных документов возможна следующими способами:
 - через защищенные каналы связи (VPN, HTTPS, FTPS);
 - почтовыми сервисами с защитой конфиденциальности (защищенные email-сервисы);
 - корпоративными информационными системами с возможностью хранения подписанных документов.
2. При передаче обязательно прилагается сертификат ключа проверки электронной подписи (СКЭП), выданный удостоверяющим центром.

5. Хранение и проверка подписанных документов

1. Подписанный документ хранится на сервере организации в электронном архиве не менее установленного срока хранения бумажных аналогов.
2. Проверка подлинности документа осуществляется с помощью специализированных сервисов и программного обеспечения (например, «КриптоПро», «CryptoTrust»).

6. Контроль соблюдения правил использования электронной подписи

Организация обязана контролировать соблюдение порядка формирования и использования электронной подписи, обеспечивать сохранность ключей шифрования и СКЭП.

7. Заключительные положения

Настоящая инструкция вступает в силу с момента утверждения руководителем организации и подлежит регулярному пересмотру каждые 3 года или по мере внесения изменений в законодательство Российской Федерации.