

УТВЕРЖДАЮ
Исполнительный директор
некоммерческой организации
«Гарантийный фонд Приморского края»


К.В. Плетцер

«01» августа 2022 г.

ПОЛОЖЕНИЕ об организации электронного документооборота в некоммерческой организации «Гарантийный фонд Приморского края»

1. Общие положения

1.1. Настоящее Положение устанавливает единые требования к организации работы с документами, получаемыми и отправляемыми с помощью системы электронного документооборота в некоммерческой организации «Гарантийный фонд Приморского края».

1.2. Положение разработано на основании требований следующих нормативных документов:

- Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи";
- Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) "Об информации, информационных технологиях и о защите информации";
- Гражданского кодекса РФ;
- Налогового кодекса РФ;

1.3. В настоящем Положении используются следующие понятия и сокращения:

Фонд – некоммерческая организация «Гарантийный фонд Приморского края».

Электронный документооборот (далее - ЭДО) - единый программно-аппаратный комплекс по работе с электронными документами.

Электронный документ (далее — ЭД) — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком, с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Сервис ЭДО - сервисы электронного обмена документами, в том числе «Корус Сфера Курьер» и «Контур.Диадок».

Система электронного документооборота (далее – СЭД) - это организация обмена электронными документами посредством сервисов ЭДО.

Электронная подпись (далее – ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Усиленная квалифицированная электронная подпись (далее – УКЭП) — цифровой аналог собственноручной подписи работодателя и/или работника, которая позволяет идентифицировать лицо, подписавшее электронный документ и подлинность подписанного документа и ключ проверки данной электронной подписи указан в квалифицированном сертификате.

Подписанный электронный документ (далее — ПЭД) — электронный документ с присоединенной электронной подписью, которая была создана на основе ЭД и ключа электронной подписи.

Сертификат ключа проверки электронной подписи (далее — сертификат) — электронный документ или документ на бумажном носителе, выданный аккредитованным

удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Учетная запись сервиса ЭДО – личный аккаунт уполномоченного сотрудника в сервисах электронного обмена документами, в том числе информационных систем «Корус Сфера Курьер» и «Контур.Диадок» с использованием конфиденциального Логина и Пароля уполномоченного сотрудника.

2. Организация электронного документооборота

2.1. Электронный документооборот включает в себя:

- формирование ЭД;
- проверку ЭД;
- отправку и получение ЭД;
- подтверждение получения ЭД;
- учет ЭД (регистрация входящих и исходящих ЭД);
- хранение электронных документов (ведение архива электронных документов).

2.2. Обмен электронными сообщениями и документами при осуществлении электронного документооборота осуществляют уполномоченные сотрудники, на основании приказа исполнительного директора Фонда.

2.3. Электронный документооборот осуществляется посредством обмена электронными сообщениями и документами в сервисах ЭДО.

2.4. При отправке ЭД уполномоченный сотрудник:

- формирует документ в одном из текстовых редакторов (Microsoft Word, Exel, Adobe),
- заносит информацию об исходящем ЭД в соответствующие Журналы регистрации,
- используя личную учетную запись, входит в сервис ЭДО,
- прикрепляет ЭД в исходящее сообщение,
- подписывает документ квалифицированной ЭП,
- осуществляет отправку ЭД.

2.5. При получении ЭД уполномоченный сотрудник:

- используя личную учетную запись, входит в сервис ЭДО,
- осуществляет распаковку ЭД из сообщения отправителя,
- проверяет действительность сертификата УКЭП отправителя,
- проверяет содержимое ЭД на предмет комплектности и правильности оформления,
- заносит информацию о входящем ЭД в соответствующие Журналы регистрации.

3. Требования к входящим электронным документам

3.1 Каждый входящий ЭД должен быть пописан УКЭП отправителя.

3.2 В случае поступления подписанного УКЭП пакета документов, в том числе, подписанного УКЭП архива документов, каждый документ, содержащийся в пакете документов, считается подписанным УКЭП отправителя, кроме случаев когда в составе пакета ЭД находится документ, подписанный ЭП иного лица.

3.3 Если входящий пакет ЭД содержит документ, подписанный ЭП иного лица (не отправителя), такой документ считается подписанным лицом, первоначально подписавшим документ. При этом, скан копия такого документа должна содержать все необходимые для идентификации подписавшего его лица атрибуты, такие как: ФИО, должность, параметры сертификата ЭП.

3.4. Все входящие ЭД, в том числе, в виде таблиц или текстовых документов (Exel, Word), должны находиться в формате не позволяющем произвести редактирование файла.

4. Хранение электронных документов

- 4.1. Уполномоченный сотрудник после использования ЭД в работе обеспечивает их хранение в соответствии с внутренним распорядительным документом Фонда.
- 4.2. Архив электронных документов должен храниться на отдельном от рабочих компьютеров сервере.
- 4.3. Все электронные документы должны храниться в том же формате, в котором они были сформированы, отправлены и получены.
- 4.4. Срок хранения электронных документов составляет 10 лет, но не менее срока договора поручительства, увеличенного на 5 лет.
- 4.5. Электронный архив подлежит защите от несанкционированного доступа, непреднамеренного уничтожения и (или) искажения, путем размещения копии архива на отдельном, отключенном от сети интернет и локальной сети, компьютере, обеспеченном контролем доступа (логин и пароль), а также антивирусной защитой.

5. Обеспечение информационной безопасности электронных документов

- 5.1. Соблюдение требований информационной безопасности при организации электронного документооборота обеспечивает:
 - конфиденциальность информации (получить доступ к информации может только определенный круг лиц);
 - целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);
 - аутентификацию (когда передаваемую информацию может получить только то лицо, кому оно предназначена, а отправителем является именно тот, от чьего имени она отправлена).
- 5.2. Требования по информационной безопасности при организации электронного документооборота реализуются посредством применения программно-технических средств и организационных мер.
 - 5.2.1. К программно-техническим средствам относятся:
 - программные средства, специально разработанные для осуществления электронного документооборота (сервисы ЭДО);
 - система паролей и идентификаторов для ограничения доступа пользователей к техническим и программным средствам системы электронного документооборота;
 - средства защиты от программных вирусов.
 - 5.2.2. К организационным мерам относятся:
 - задание режима использования пользователями паролей и идентификаторов (логин и пароль в личном аккаунте сервиса ЭДО);
 - допуск к осуществлению документооборота только определенных лиц на основании приказа исполнительного директора Фонда;
 - поддержание программных средств в исправном состоянии;
 - обучение работников Фонда;
 - защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).