Часто задаваемые вопросы ФИС ФРДО (подсистема сбора данных о ДПО)

1. Общие вопросы

1.1 Вопрос: Где можно получить электронную подпись для работы с ФРДО?

Ответ: Список аккредитованных удостоверяющих центров опубликован на сайте Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации https://digital.gov.ru/ru/activity/govservices/2/.

1.2. Вопрос: У нас уже есть электронная подпись, можем ли мы ее использовать для работы с системой ФИС «ФРДО»?

Ответ: Можете, если Вы получали электронную подпись в удостоверяющем центре, аккредитованном в установленном порядке.
Выданная электронная подпись должна соответствовать техническим требованиям для работы с системой ФИС «ФРДО». Данную информацию необходимо уточнить в удостоверяющем центре, в котором Вы получали электронную подпись.

1.3. Вопрос: Как подписать файл электронной подписью?

Ответ: Чтобы подписать файл электронной подписью, на рабочем компьютере должно быть установлено средство электронной подписи КриптоАРМ (в случае использования КриптоПро CSP), ViPNet PKI Client (в случае использования ViPNet CSP) или аналогичное решение в соответствии с использующимися криптопровайдерами.

1.4. Вопрос: Кто должен вносить данные о документах об образовании, выданных упраздненными образовательными организациями?

Ответ: Данные о документах об образовании вносит в систему ФИС ФРДО правопреемник (архив).

1.5. Вопрос: Как подавать сведения за образовательные организации, которые присоединены путем реорганизации?

Ответ: Чтобы подавать сведения о документах об образовании за реорганизованные организации, необходимо создать организацию и связь с ней (по реквизитам ОГРН и КПП, действующих до реорганизации) в личном кабинете правопреемника во вкладке «Организации».

1.6. Вопрос: Как заполнять файл шаблона?

Ответ: Об этом подробно написано в инструкции по заполнению шаблона, которая находится во вкладке «Инструкции» на главной странице сайта https://open-dpo.obrnadzor.gov.ru.

1.7. Вопрос: Можно ли заполнить данные о документах по всем годам в одном шаблоне?

Ответ: Можно, но для удобства дальнейшей работы с внесенными сведениями о документах об образовании рекомендуем заполнять в один шаблон только один год.

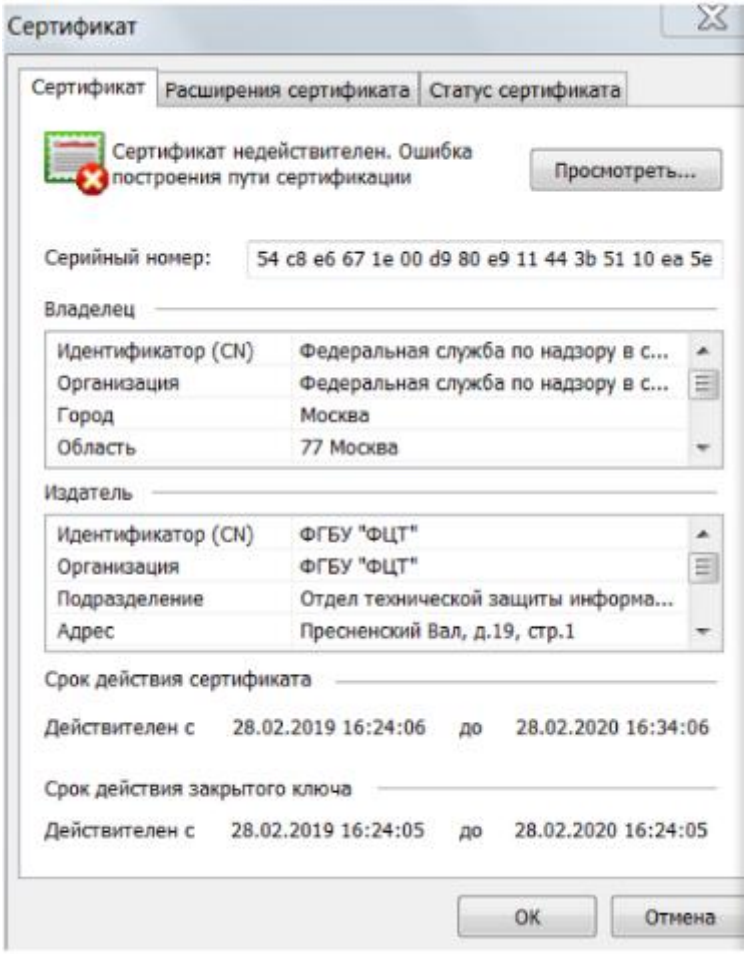
1.8. Вопрос: Какое имя дать заполненному шаблону и пакету?

Ответ: Имя шаблона и пакета с заполненными данными о документах об образовании может быть любым, но без использования пробелов и спецсимволов.

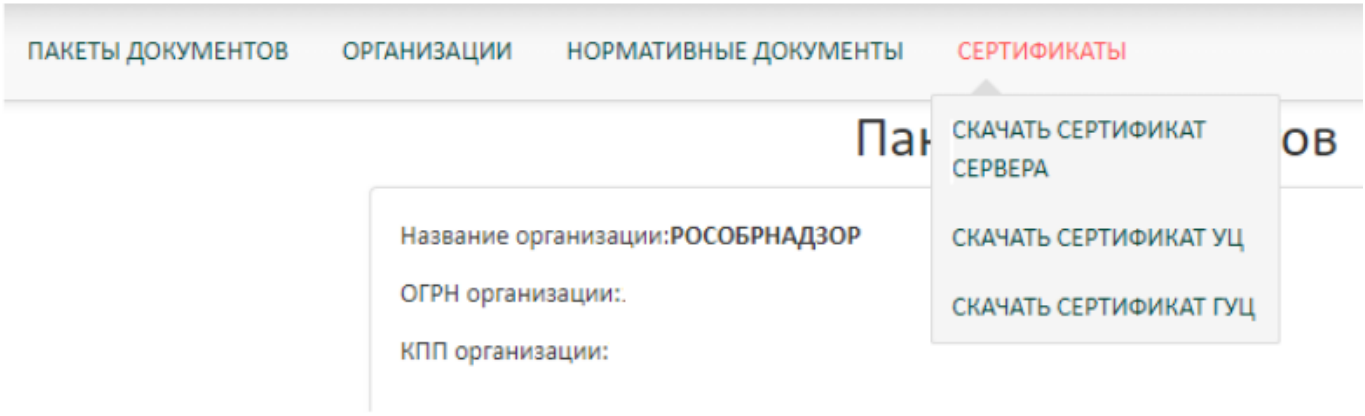
1.9. Вопрос: Что делать, если у выпускника нет отчества, а поле является обязательным полем?

Ответ: Поле «Отчество» можно заполнить словом «Нет».

1.10. Вопрос: Не удается зашифровать файл сертификатом сервера. Выдает ошибку «Сертификат не действителен. Ошибка построения пути сертификации»



Ответ: 1. Для проверки цепочки необходимо установить корневые и промежуточные сертификаты УЦ. Наведя курсор на пункт меню «Сертификаты», в появившемся меню необходимо нажать пункт меню «Скачать сертификат УЦ».



После загрузки файла сертификата его необходимо установить. Также необходимо установить сертификат ГУЦ, нажав на пункт меню «Скачать сертификат ГУЦ», и повторить вышеописанные действия.

2.Дешифрование

2.1 Убедитесь, что файл пакета зашифрован согласно требований к файлу загружаемого пакета, перечисленных в п.п. 3.2 "Руководство оператора".

2.2 Убедитесь, что файл пакета зашифрован на открытом ключе сертификата сервера. Если осуществлено подписание и шифрование через пункт контекстного меню криптопровайдера "Подписать и зашифровать", убедитесь, что на этапе задания параметров шифрования был выбран сертификат сервера, а для подписания был выбран сертификат электронной подписи ответственного за внесение данных об образовании в систему ФРДО.

2.3 Убедитесь, что файл пакета зашифрован на действующем сертификате сервера, обновление сертификата сервера осуществляется раз в год. Для получения актуального сертификата его необходимо скачать с сервера. Действия, необходимые для скачивания, описаны в п.п. 3.2 "Руководство оператора" Рис. 9.

2.4 Сертификат сервера не поддерживает алгоритм использованный при шифровании файла. Необходимо обеспечить шифрование файла по алгоритму ГОСТ 28147-89, подробнее см. пункт 3.2 Руководства оператора.

3. Проверка подписи

3.1 Убедитесь, что файл пакета подписан согласно требований к файлу загружаемого пакета, перечисленных в п.п. 3.2 "Руководство оператора".

3.2 Убедитесь, что файл пакета подписан действительным сертификатом (не истек срок действия сертификата).

3.3 Удостоверьтесь, что подпись файла пакета документов в формате «attached PKCS #7», алгоритм ГОСТ 34.10-2012, выходной файл в формате «der».