**Вопрос.**

**Требования к информации, размещаемой на официальном сайте образовательной организации, предусматривают, что ряд размещаемых электронных документов должен быть подписан электронной подписью. Как это осуществить?**

**Ответ.**

Данный вопрос не так прост. Есть некоторые проблемы, как с юридической, так и с технической точки зрения.

**1. Нормативно-правовой аспект**

Приказ Рособрнадзора от 14.08.2020 № 831 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации» (далее – приказ РОН № 831), изданный в соответствии с постановлением Правительства РФ от 10.07.2013 № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации», устанавливает, что ряд материалов размещается на официальном сайте образовательной организации в виде электронных документов, подписанных электронной подписью (далее – ЭП) в соответствии со статьей 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

Уточнений по виду используемой электронной подписи приказ РОН № 831 не дает. В то время, как статья 5 Федерального закона № 63-ФЗ гласит, что видами ЭП, отношения в области использования которых регулируются указанным Федеральным законом, являются *простая* ЭП и *усиленная* ЭП. Усиленная ЭП, в свою очередь, подразделяется на усиленную *неквалифицированную* ЭП и усиленную *квалифицированную* ЭП, каждая из которых имеет свои особенности.

Статья 6 Федерального закона № 63-ФЗ конкретизирует использование ЭП различных видов. Так, информация в электронной форме, подписанная *простой или усиленной неквалифицированной ЭП*, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Информация в электронной форме, подписанная *усиленной квалифицированной ЭП*, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Если в соответствии с законодательством или правилами делового оборота документ должен быть заверен *печатью*, электронный документ, подписанный *усиленной* ЭП и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному *собственноручной подписью и заверенному печатью*.

Таким образом, статья 6 Федерального закона № 63-ФЗ не снимает имеющуюся в приказе РОН № 831 неопределенность в отношении вида используемой ЭП.

Постановление Правительства РФ от 10.07.2013 № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации», в соответствии с которым издан приказ РОН № 831, утратило силу с 01.03.2022 в связи с началом действия постановления Правительства РФ от 20.10.2021 № 1802 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, а также о признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации» (далее – постановление № 1802). Постановление № 1802 устанавливает уже более конкретные требования: информация размещается в форме электронного документа, подписанного *простой ЭП* в соответствии с Федеральным законом № 63-ФЗ.

Использование простой ЭП регулируется статьей 9 упомянутого Федерального закона.

Электронный документ считается подписанным *простой ЭП* при выполнении в том числе *одного* из следующих условий:

1) простая ЭП содержится в самом электронном документе;

2) ключ простой ЭП применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия должны предусматривать, в частности:

1) правила определения лица, подписывающего электронный документ, по его простой ЭП;

2) обязанность лица, создающего и (или) использующего ключ простой ЭП, соблюдать его конфиденциальность.

К сожалению, постановление № 1802, сняв неопределенность по виду используемой ЭП, добавило другую. Использование простой ЭП подразумевает наличие нормативно установленных правил или соглашений по использованию простой ЭП.

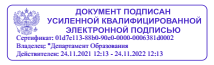
Обычно предполагается, что простая ЭП существует в рамках некой информационной системы. При этом пароль пользователя, разместившего документ, считается его ключом простой ЭП. А логин – ключом проверки. То есть, по логину определяется лицо, подписывающее документ, а соблюдение конфиденциальности пароля приравнивается к соблюдению конфиденциальности ЭП. Или заключается соглашение о том, что подписанием документа простой ЭП считается его направление с определенной электронной почты. При этом уточняется, от каких лиц и с каких адресов будут направляться сообщения. В таком случае ключом ЭП будет пароль к электронному почтовому ящику, ключом проверки ЭП – адрес электронной почты.

Однако в случае с сайтом эти механизмы не работают. Возможность заключения соглашения отсутствует – сайт изначально адресован неопределенному кругу лиц. Пара логин-пароль также утрачивает смысл: оператором, располагающим логином и паролем, как правило, является не лицо, подписывающее документ, а технический специалист, нередко являющийся сотрудником сторонней организации.

В имеющейся ситуации единственным выходом представляется использование программных и технических средств, позволяющих на базе усиленной квалифицированной ЭП разместить ЭП внутри документа. Но здесь возникают проблемы технического характера.

**2. Технический аспект**

Во-первых, надо понимать, что наличие в документе подобного значка:



не означает фактическое наличие электронной подписи. Закон подразумевает возможность проверки ЭП внутри документа. А здесь имеется только картинка.

Во-вторых, если документ был подписан на одном компьютере, то это вовсе не означает, что на другом компьютере ЭП будет проверена и подтверждена как действительная. Причиной этого является сам механизм проверки ЭП.

Упрощенно говоря, ЭП представляет собой некоторый код («сертификат»), которым удостоверяющий центр, выпустивший его, подтверждает, личность или юридическое лицо владельца ЭП. Удостоверяющий центр, в свою очередь, тоже обладает сертификатом, которым удостоверяются его полномочия от имени удостоверяющего центра более высокого уровня. Нередко такая цепочка бывает довольно длинной, и заканчивается она, так называемым, «корневым сертификатом», сертификатом головного удостоверяющего центра. Но и головных центров несколько. Например, действуют корневые сертификаты Минцифры России, Федерльной налоговой службы, Федерального казначейства. И, если проверяющему компьютеру не удастся выстроить исходную цепочку сертификатов, то, скорее всего, проверка ЭП покажет наличие проблем с подписью. Однако лицо, подписавшее документ, и неизменность документа установить возможно.

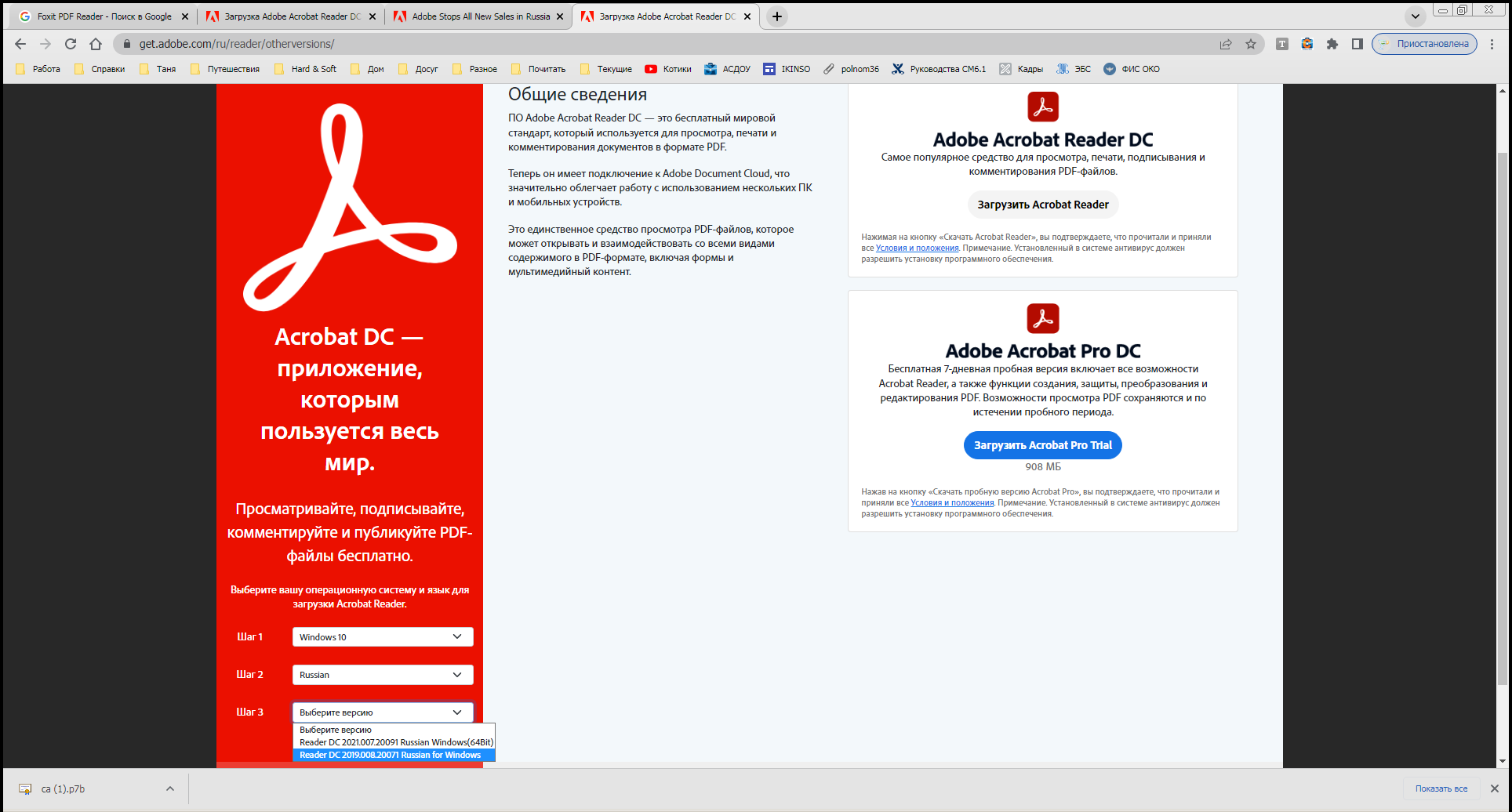
В-третьих, такой механизм подписания подразумевает использование платных программных и технических продуктов. Например, потребуются выпущенный удостоверяющим центром сертификат ЭП на носителе (токене) и комплекс программных средств КриптоПРО.

**3. Инструкция по формированию ЭП**

Предполагается, что имеется компьютер, на котором уже установлены комплекс программных средств КриптоПРО и соответствующий сертификат ЭП. В качестве документа, подлежащего подписанию ЭП и размещению на сайте, выберем pdf-файл, как наиболее адекватно отображающий вид оригинала. При этом нет разницы, имеем ли мы дело со сканированным образом документа или документом, сохраненным в pdf-формате.

Для подписания потребуется одна из двух бесплатных программ: Foxit PDF Reader (<https://www.foxit.com/ru/pdf-reader/>) или Adobe Acrobat Reader DC (<https://get.adobe.com/ru/reader/otherversions/>).

Обратите внимание, особенно при использовании Windows 10, по умолчанию скачивается 64-разрядная версия, которая не работает с КриптоПРО. В левом нижнем углу надо выбрать версию программы 2019 года:



Программу нужно скачать и установить.

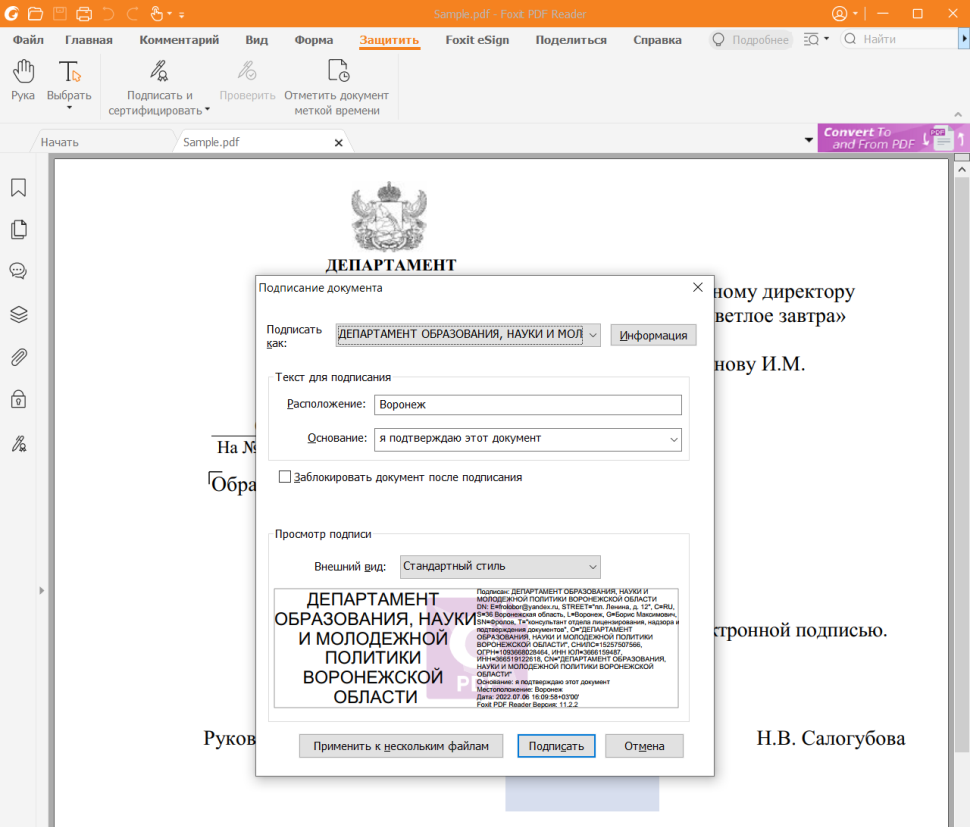
Если вы планируете работать с Adobe Acrobat Reader DC, то вам нужно скачать и установить модуль КриптоПро PDF (<https://www.cryptopro.ru/products/other/pdf>).

**3.1. Подписание и проверка подписи в Foxit PDF Reader**

Необходимо открыть подписываемый документ в Foxit PDF Reader.

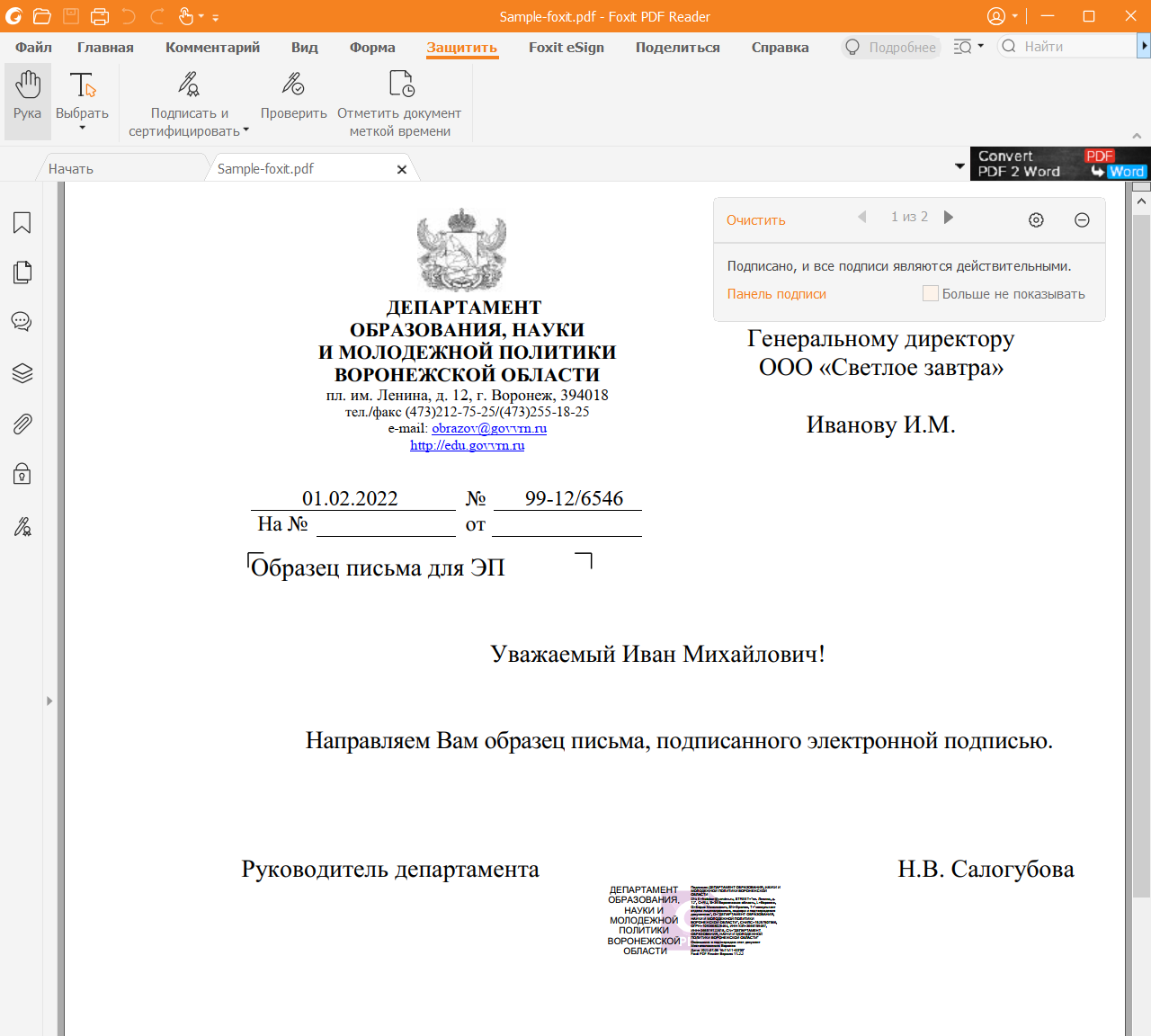
Далее последовательно выбрать пункты меню: «Защитить», «Подписать и сертифицировать», «Разместить подпись». Курсор мыши превратится в крестик, которым надо выделить прямоугольную область там, где планируется разместить подпись.

После выделения появится окно формирования подписи:

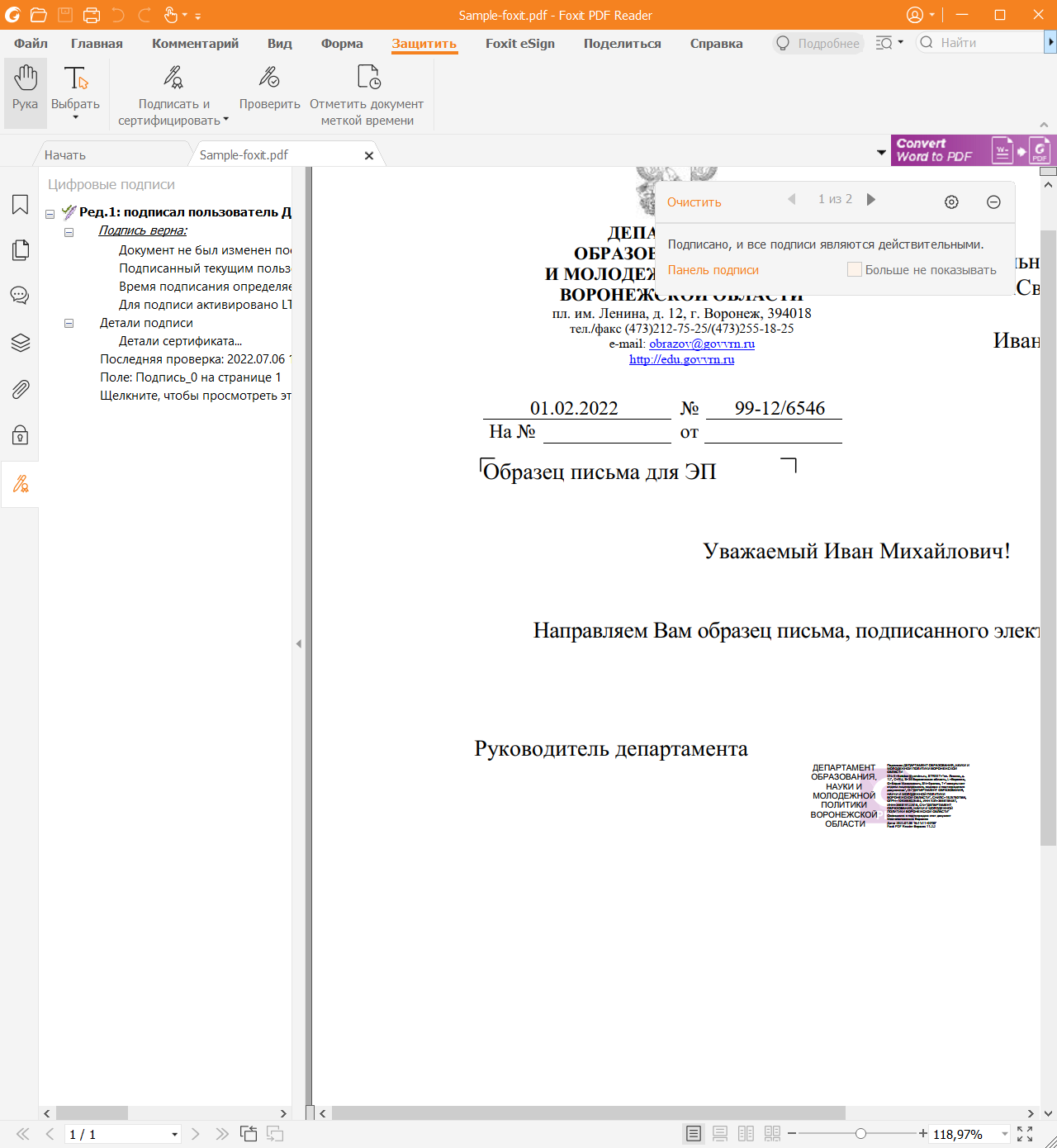


Здесь можно выбрать сертификат ЭП («Подписать как:») и основание (например «Я автор этого документа» или «Я подтверждаю этот документ»). Затем нужно нажать «Подписать».

На выбранном месте появится подпись и станет доступной ее проверка:



Если в появившемся окне нажать «Панель подписи», то подпись можно проверить детально:

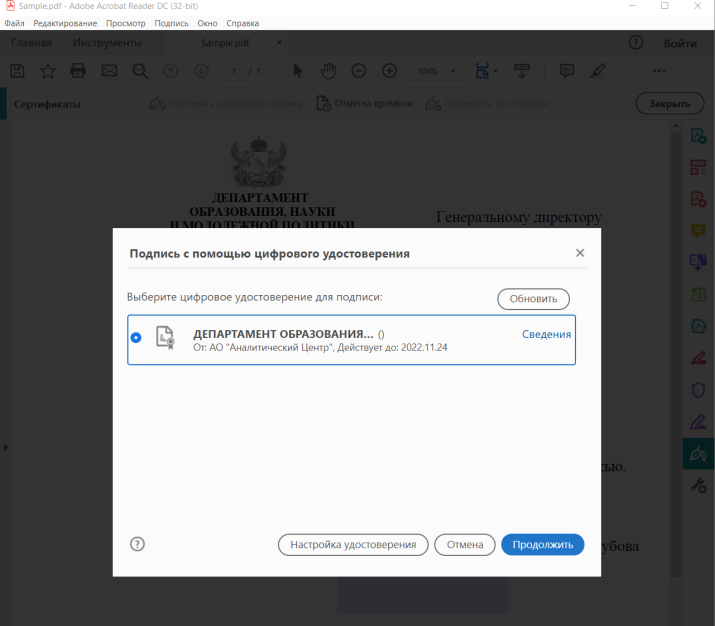
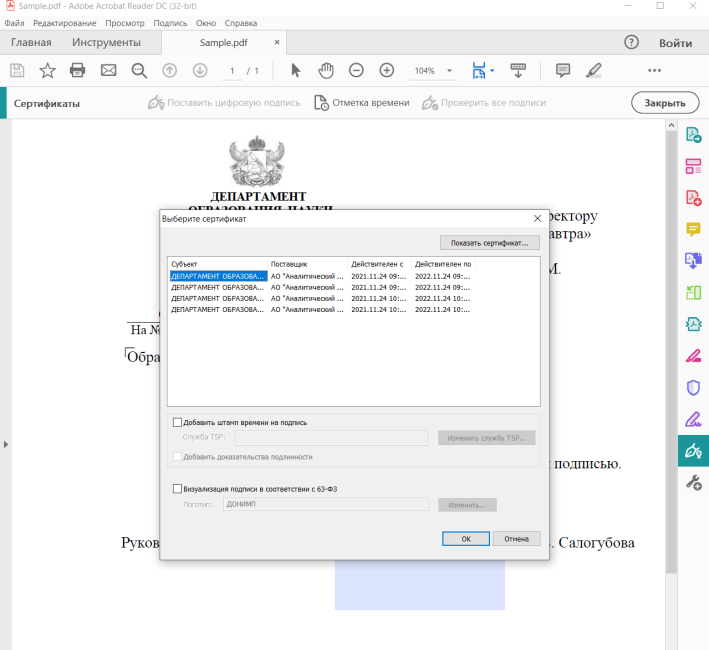


**3.2. Подписание и проверка подписи в Adobe Acrobat Reader DC**

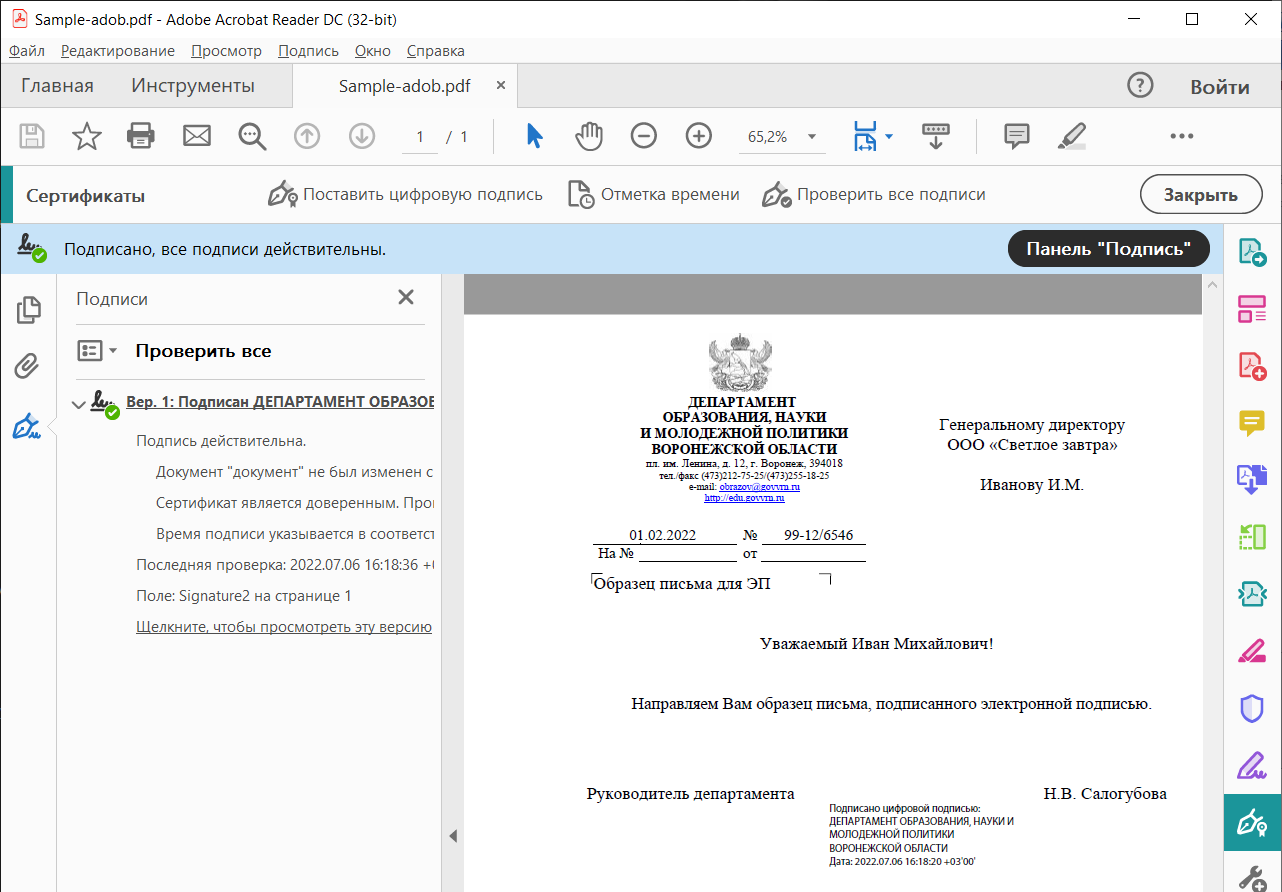
Необходимо открыть подписываемый документ в Adobe Acrobat Reader DC.

Далее последовательно выбрать закладку «Инструменты», пункты «Сертификаты», «Поставить цифровую подпись». Также как и в предыдущем случае крестиком надо будет выделить область, где будет размещаться подпись. Откроется окно выбора сертификата. Нужно выбрать необходимый сертификат и нажать «ОК». Затем, в окне подписи, нажать «Подписать».

Появится уведомление, что документ подписан.

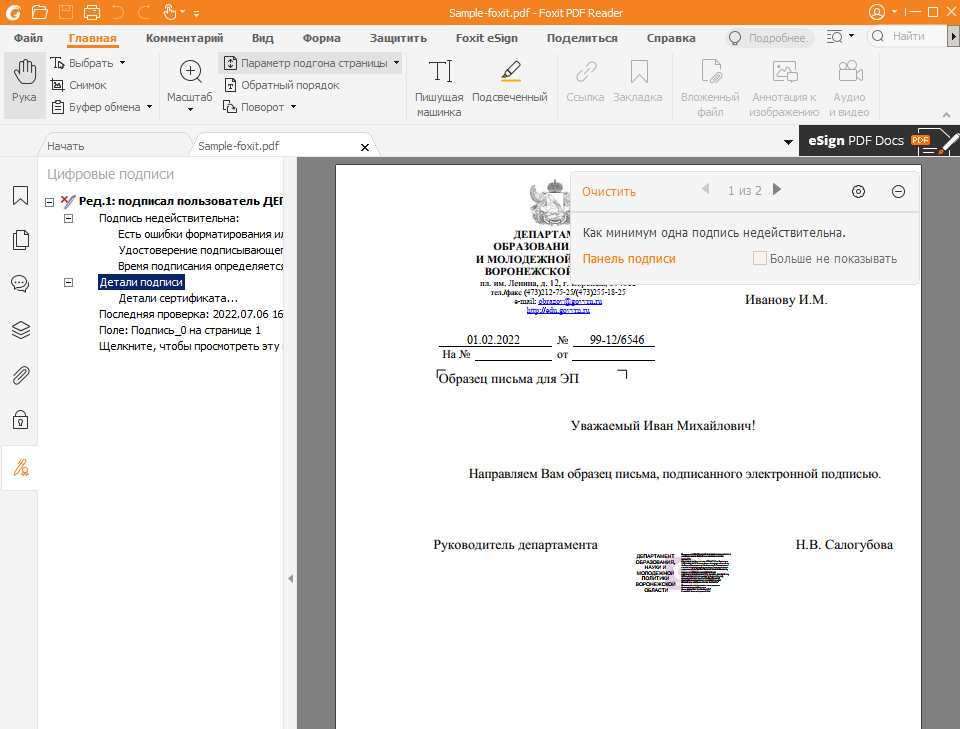


Теперь на панели «Подпись» можно проверить детали подписи.



**4. «Ошибки» подписи**

Откроем любой из свежеподписанных документов на другом компьютере:



Проверка показывает, что подпись недействительна. Второй компьютер не может выстроить цепочку сертификатов, но, тем не менее, документ содержит ЭП, сформированную по правилам и содержащую реквизиты подписавшего лица.

Такой документ будет считаться соответствующим требованиям приказа РОН № 831 и постановления № 1802.

*Ответ подготовлен отделом аккредитации и контроля качества образования*