ИНСТРУКЦИЯ по установке сертификата

<u> Примечание:</u>

Рекомендуем хранить закрытый ключ на личном защищенном паролем ключевом носителе в сейфе, не передавать его другим сотрудникам, не оставлять без присмотра, а также соблюдать требования:

- Федерального закона «Об электронной подписи»;

- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, в части обращения со средствами криптографической защиты информации;

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г.№ 66, в части эксплуатации средств криптографической защиты информации;

- Эксплуатационной документации к средствам электронной подписи;

- Порядка реализации функций удостоверяющего центра АУ «ЦИТ» Минцифры Чувашии.

СПОСОБ УСТАНОВКИ ЛИЧНОГО СЕРТИФИКАТА № 1:

Запустите КриптоПро CSP, перейдите во вкладку «Сервис» и нажмите кнопку «Установить личный сертификат».

	Безопасность	Winlogon	Настройки TL
Общие	Оборудование	Сервис	Дополнительн
Контейнер з Эти мастера удалить кон	акрытого ключа позволяют протести тейнер закрытого кл	ровать, скопир юча с носителя	ювать или 1.
Про <u>т</u> естиро	вать <u>С</u> копиро	вать	<u>У</u> далить
Личный серт Этот мастер контейнером хранилище.	Просмотреть ификат позволяет связать се і закрытого ключа, уг	сертификаты в ертификат из ф становив этот	з <u>к</u> онтейнере райла с сертификат в
	Установи	ть дичный серт	гификат
Пароли закр	ытых ключей позволяют изменить	пароли (ПИН-к е ранее пароли	оды) закрытых
Эти мастера ключей или	удалить запомненные		

В открывшемся окне с помощью кнопки «Обзор» выберите файл сертификата (файл с расширением «cer» на USB-носителе и наименованием организации в названии), нажмите «Далее». При этом у Вас отобразятся данные по выбранному сертификату. Если сертификат выбран верно нажмите кнопку «Далее», выберите контейнер закрытого ключа этого сертификата через кнопку «Обзор».

Контейнер закрытого ключа	
Введите или укажите контейнер закрытого ключа, который выбранному сертификату	соответствует
Найти контейнер автоматически	
Имя ключевого контейнера:	
\\.\FAT12_F\e97971ae-b942-4544-9c95-98d178294f48	О <u>б</u> зор
введенное имя задает ключевой контейнер:	
Компьютера	
<u> </u>	
В <u>ы</u> берите CSP для поиска ключевых контейнеров:	
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	J ~
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	

После выбора контейнера закрытого ключа нажмите кнопку «Далее», выберите хранилище для хранения ключевого контейнера сертификата и нажмите «Далее».

	Завершение раб установки лично	оты мастера ого сертификата
	Были указаны следующие	е параметры:
	Взять сертификат	~
	из файла	F:\00_test.cer
	имя сертификата	СНИЛС=0000000000, И
	субъект	СНИЛС=0000000000, И
	поставщик	E=uc-info@cap.ru, OFPH=
	действителен с	3 ноября 2018 г. 8:18:34
	действителен по	31 декабря 2018 г. 0:00:(
	серийный номер	67F0 508A 762C CF80 E8 ¥
	<	>
	Убедитесь, что выбраны г нажмите кнопку "Готово"	правильные параметры и для выполнения установки.

Нажмите «Готово».

СПОСОБ УСТАНОВКИ ЛИЧНОГО СЕРТИФИКАТА № 2:

Если вы используете защищенный ключевой носитель (Рутокен или e-token), то сертификат можно установить следующим способом.

Запустите КриптоПро CSP, перейдите во вкладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере».

В открывшемся окне с помощью кнопки «Обзор» выберите USB-носитель и записанный на него контейнер закрытого ключа. Их может быть несколько, поэтому можно посмотреть каждый из них по порядку, выбрав один них и нажав «ОК». Откроется окно с основными сведениями о сертификате (кем и кому выдан, срок действия и серийный номер). Если этот не тот сертификат, что вам нужен, то вы можете нажать кнопку «Назад» и повторить процедуру уже с другим контейнером. Если же все верно, то нажмите кнопку «Установить»:

📀 Сертификаты в контейнере закрытого ключа 🛛 🗙					×
Сертификат для Просмотрите и	і просмотр і выберите	ра сертификат			
Сертификат:	АУ ЦИТ М	Линцифры Чува	шии]
Субъект:	E=	. ИНН=0	02130176633	3, OFPH=11621300	063501, C=RU, S
Поставщик:	OFPH=11	62130063501,	ИНН=002130	176633, C=RU, S:	=21 Чувашская Г
Действителен <u>с</u> :	25 январ	я 2023 г. 8:16:3	37		
Действителен <u>п</u> о:	25 январ	я 2024 г. 8:26:3	37		
Серийный <u>н</u> омер:					
				<u>У</u> становить	С <u>в</u> ойства
					06200
					000000
			< <u>Н</u> азад	Готово	Отмена

УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА

Скачайте корневой сертификат УЦ АУ «ЦИТ» Минцифры Чувашии по ссылке:

http://uc-cit.cap.ru/aia/uc-au-cit2023.crt

Откройте корневой сертификат УЦ АУ «ЦИТ», щелкнув по нему дважды левой кнопкой мыши, и нажмите на кнопку «Установить сертификат»:.

8	Сертификат		\times
06	щие Состав Пут	ъ сертификации	
	Сведения	я о сертификате	
	Этот сертифика	т предназначается для:	
	• Все политин • Все политин	ки выдачи ки применения	
	Кому выдан:	АУ "Центр информационных технологий" Минцифры Чувашии	_
	Кем выдан:	АУ "Центр информационных технологий" Минцифры Чувашии	
	Действите	лен с 21.06.2021 по 21.06.2036	
	Установ	ить сертификат	ика
			ОК

Откроется окно «Мастер импорта сертификатов».

Расположение хранилища необходимо выбрать «Текущий пользователь»:

🔶 😺 Мастер импорта сертификатов	×
Мастер импорта сертификатов	
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений, хранилище сертификатов — это область состемы, предназначенная для хранения сертификатов	
Расположение хранилища • Текуший пользователь Олокальный компьютер	
Для продолжения нажните кнопку "Далее".	
Далее Отмен	a
	_

Рисунок 8

Затем вручную выбрать хранилище сертификатов: «Доверенные корневые центры сертификации»:

Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.
О Автоматически выбрать хранилище на основе типа сертификата
• Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
Обзор

Зыбор :	кранилища сертификата	×
Выбери хотите	те хранилище сертификатов, которое в использовать.	3Ы
····	Личное	^
	Доверенные корневые центры сертис	
	Доверительные отношения в предпри	
	Промежуточные центры сертификаци	
	Объект пользователя Active Directory	
	Ловеренные издатели	~
<	>	
Пока	азать физические хранилища	

Нажать кнопку «Далее»:

х _Ф и	петер инпорто сер ификатов	
Xpa	илище сертификатов	
	(ранилища сертификатов - это системные области, в которых хранятся сертификаты.	
	Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.	
	О Автоматически выбрать хранилище на основе типа сертификата	
	• Поместить все сертификаты в следующее хранилище	
	Хранилище сертификатов:	
	Доверенные корневые центры сертификации Обзор	

Затем нажать на кнопку «Готово»:.

÷ 🌡	Мастер импорта сертификатов	×
	Завершение мастера импорта серти	фикатов
	Сертификат будет импортирован после нажатия кнопк	и "Готово".
	Были указаны следующие параметры:	
	Хранилище сертификатов, выбранное пользователем Содержимое	Доверенные корневые цент Сертификат
	٤	>
		Готово Отмена

В открывшемся после диалоговом окне с предупреждением нажать «Да». Импорт сертификата завершен.