



**Инструкция по настройке WEB-доступа к Личному кабинету
(lk.cbch.ru)**

Москва, 2023 г.

Оглавление

1. Общие положения.....	2
2. Технические условия.....	2
3. Установка корневого сертификата.....	2

1. Общие положения

1.1. В целях выполнения требований действующего законодательства Российской Федерации в сфере информационной безопасности, доступ внешних пользователей (далее – Клиентов) в Личный кабинет общества с ограниченной ответственностью «Спектрум кредитное бюро» (далее – ООО «СКБ») осуществляется по технологии ГОСТ TLS.

1.2. В настоящей Инструкции определяются условия и требования для получения WEB-доступа к Личному кабинету ООО «СКБ».

2. Технические условия

2.1. На автоматизированном рабочем месте Клиента должны быть установлены:

– криптопровайдер **«Крипто-Про CSP»**, установка и настройка криптопровайдера «Крипто-Про CSP» осуществляется в соответствии с технической и эксплуатационной документацией к нему (в том числе, размещенной на официальном сайте разработчика <https://cryptopro.ru/products/csp/>);

– WEB-браузер с поддержкой криптографических алгоритмов ГОСТ:

✓ «Yandex»

✓ «Chromium-gost»

2.2. Сайт Личного кабинета ООО «СКБ» использует защищенное соединение для обмена информацией поэтому, когда вы переходите на сайт (по протоколу HTTPS), серверу нужно подтвердить подлинность этого сайта. Для этого необходимо предоставить специальный сертификат безопасности.

2.3. Для обеспечения доверия к сертификату безопасности ООО «СКБ» на автоматизированном рабочем месте Клиента необходимо установить корневой сертификат удостоверяющего центра, выпустившего данный сертификат. В данном случае необходим сертификат уполномоченного лица ЦУС VPN Удоверяющего центра ООО «КРИПТО-ПРО» (серийный номер сертификата: 0275eeaf00e2ac32964460adb4ae807d0f), скачать данный сертификат можно с официального сайта <http://vpncr.crypto.ru/dist.htm>.

3. Установка корневого сертификата

3.1. Установка корневого сертификата в системное хранилище сертификатов ОС:

– двойным кликом мыши откройте файл корневого сертификата и во вкладке «Общее» нажмите кнопку «Установить сертификат...» (рис. 1):

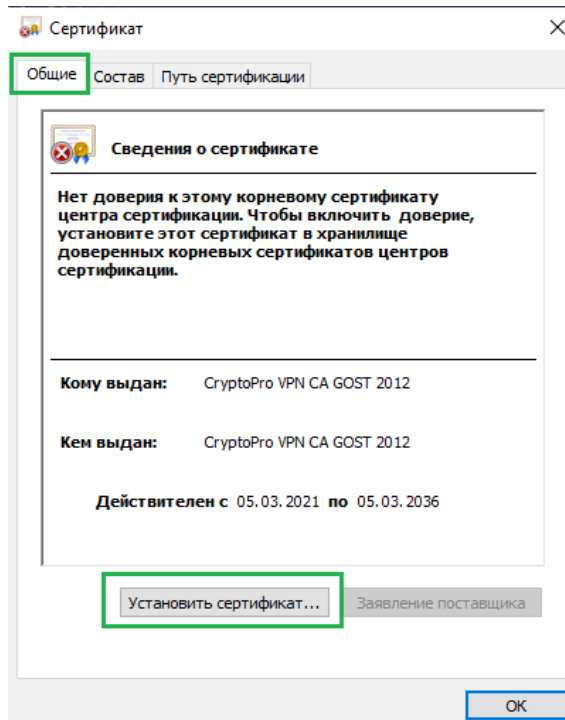


Рис. 1 – открытый файл сертификата (вкладка «Общее»)

- выберите расположение – «**Текущий пользователь**» (рис. 2), нажмите «**Далее**»:

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

Текущий пользователь

Локальный компьютер

Для продолжения нажмите кнопку "Далее".

Рис. 2 – выбор расположения хранилища сертификатов

- укажите вариант «**Поместить все сертификаты в следующее хранилище**» (т.е. вручную) и нажмите кнопку «**Обзор**» (рис. 3):

Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

Автоматически выбрать хранилище на основе типа сертификата

Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Доверенные корневые центры сертификации

Обзор...

Рис. 3 – выбор хранилища для расположения корневого сертификата вручную

- в появившемся окне выберите хранилище – «**Доверенные корневые центры сертификации**» (рис. 4):

Выбор хранилища сертификата

Выберите хранилище сертификатов, которое вы хотите использовать.

- Доверенные корневые центры сертификации
- Доверительные отношения в предприятии
- Промежуточные центры сертификации
- Доверенные издатели
- Сертификаты, к которым нет доступа

Показать физические хранилища

OK Отмена

Рис. 4 – выбор хранилища из списка

- в итоге будет выбрано нужное хранилище, нажмите «**Далее**» (рис. 5):

Хранилище сертификатов:

Доверенные корневые центры сертификации

Обзор...

Далее Отмена

Рис. 5 – выбор хранилища – «Доверенные корневые центры сертификации»

- на завершающем этапе установки сертификата нажмите «**Готово**»;
- далее появится стандартное предупреждение системы безопасности ОС, появляющееся при добавлении корневого сертификата, и для корректного добавления сертификата в системное хранилище ОС, а также последующего его использования необходимо согласиться с установкой сертификата и нажать «**Да**» (рис. 6):

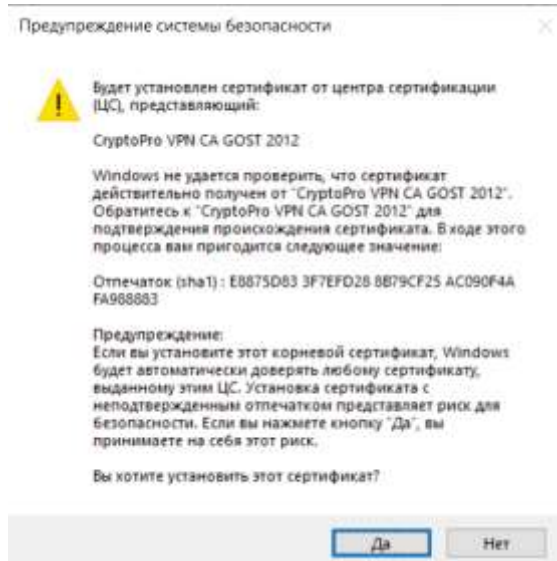


Рис. 6 – окно предупреждения системы безопасности

3.2. В случае корректной установки корневого сертификата при переходе на сайт Личного кабинета ООО «СКБ» в адресной строке WEB-браузера (справа) будет отображаться значок закрытого замочка:

- отображение в браузере «**Yandex**» (рис. 7):

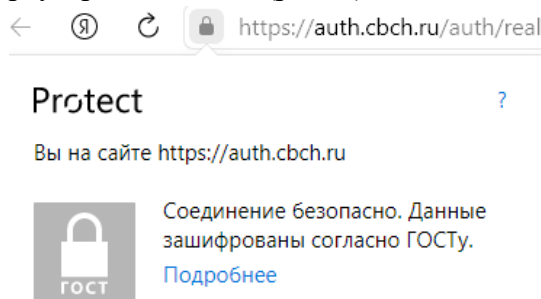


Рис. 7 – защищенное подключение в браузере «Yandex»

- отображение в браузере «**Chromium-gost**» (рис. 8):

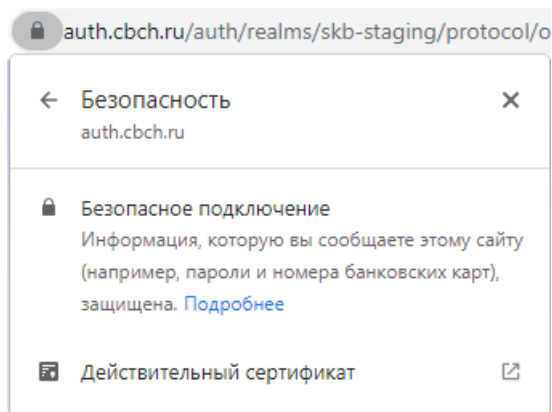


Рис. 8 – защищенное подключение в браузере «Chromium-gost»