### **Вход по ЭЦП РУЦ ГосСУОК**

Доступ к Единому порталу электронных услуг (далее ЕПЭУ) осуществляется интерактивно через сеть интернет посредством web–браузера (Microsoft Internet Explorer). Адрес сайта в сети интернет [*https://portal.gov.by*](https://portal.gov.by)

* Для корректной работы должен использоваться браузер Microsoft Internet Explorer версии 9 или выше.
* Для авторизации на ЕПЭУ с использованием ЭЦП РУЦ ГосСУОК необходимо предварительно настроить рабочее месте пользователя в соответствии с инструкцией ([Инструкцией по авторизации с использованием средств электронной цифровой подписи](#настройки)).

При входе на ЕПЭУ пользователь попадает на главную страницу (Рисунок 1):

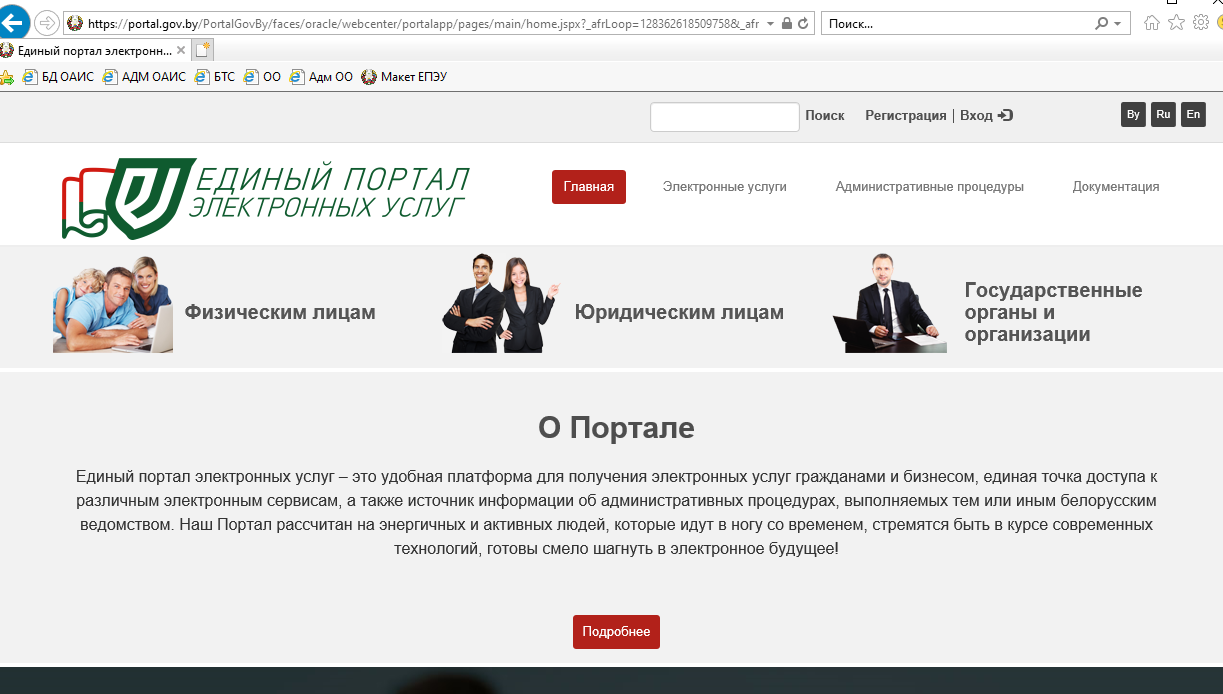


Рисунок 1. Главная страница «Единого портала электронных услуг»

Нажмите на кнопку «Вход».

В открывшейся странице авторизации, в левой части страницы выберите ссылку «Авторизация с использованием ЭЦП РУЦ ГосСУОК» (Рисунок 2):

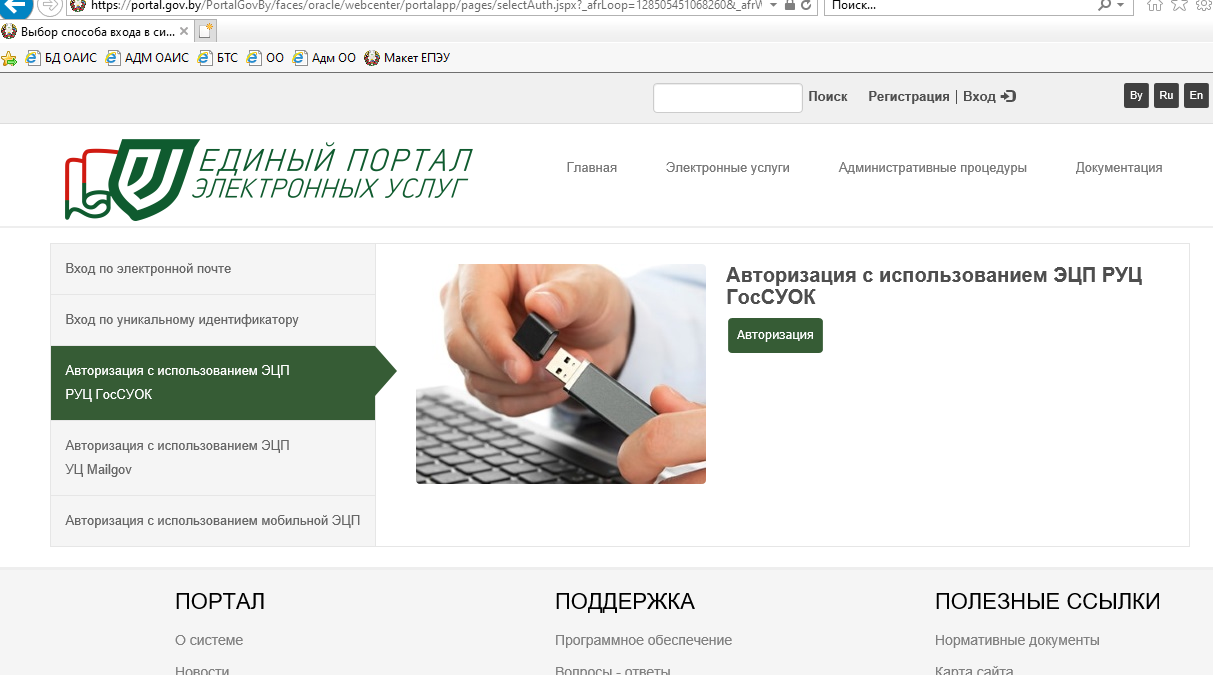


Рисунок 2. Авторизация по ЭЦП РУЦ ГосСУОК

Нажмите на кнопку . Откроется всплывающее окно с доступными сертификатами (Рисунок 3):

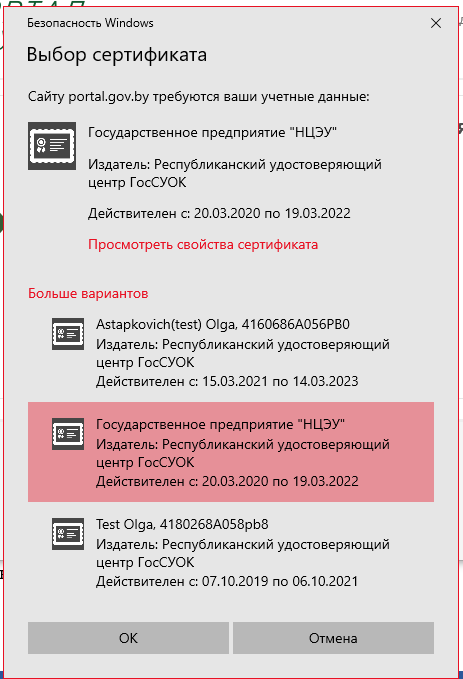


Рисунок 3. Список доступных сертификатов

Выберите нужный сертификат и нажмите **ОК**. Открывается следующее окно с полем для ввода пароля (Рисунок 4):

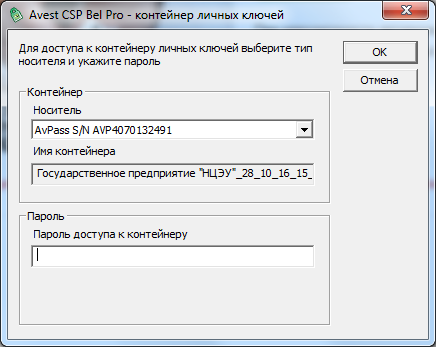


Рисунок 4. Ввод пароля для доступа к контейнеру личных ключей

Введите пароль в соответствующее поле и нажмите **ОК**. Если авторизация прошла успешно, откроется страница Личного кабинета пользователя.

**Инструкция по авторизации на портале «Единый портал электронный услуг» (**[**https://portal.gov.by**](https://portal.gov.by)**)**

**с использованием средств электронной цифровой подписи**

**Действия по настройкам для авторизации и работы:**

1. Проверьте настройки в браузере Internet Explorer

* Вход на портал осуществляется ТОЛЬКО с помощью браузера **Internet Explorer** версии не ниже 9. Проверить версию можно выбрав в строке меню Internet Explorer «Справка» → «О программе»
* **В адресной строке не должно быть префикса** **www**
* **Добавьте портал в надежные сайты**. В строке меню Internet Explorer выберите «Сервис» → «Свойства браузера» → «Безопасность» → «Надежные сайты (узлы)» → «Сайты (узлы)» → «Добавить», внесите URL: <https://portal.gov.by>
* **Включите протоколы безопасности SSL 3.0 TLS 1.0, 1.1, 1.2.** В строке меню Internet Explorer выберите «Сервис» → «Свойства браузера» → «Дополнительно», добавьте галочку напротив пункта SSL 3.0, TLS 1.0, 1.1, 1.2.
* **Отключите защищенный режим**. В строке меню Internet Explorer выберите «Сервис» → «Свойства браузера» → «Безопасность» → «Надежные сайты (узлы)». Снимите галочку с пункта «Включить защищенный режим».
* **Отключите фильтрацию Active X.** В строке меню Internet Explorer выберите «Сервис» → «Свойства браузера» → «Безопасность» → «Надежные сайты (узлы)» → «Другой», убедитесь, что напротив пункта «Включить фильтрацию ActiveX» стоит галочка на «Отключить».
* **Отключить режим совместимости.** В строке меню Internet Explorer выберите «Сервис» → «Параметры просмотра в режиме совместимости», убедитесь, что веб-сайт portal.gov.by **не добавлен** в список веб-сайтов, для которых Вы выбрали просмотр в режиме совместимости.

1. Проверьте, установлена ли актуальная версия криптографического программного обеспечения.

Актуальные версии криптографического ПО на данный момент:

* **криптопровайдер 6.3.0.813**: проверить версию можно, открыв «Пуск» → «Все программы» → «Авест» → «Avest CSP Bel» → вкладка «Версия».
* **персональный менеджер сертификатов Авест для ГосСУОК 5.0.3.1136**: проверить можно, открыв «Пуск» → «Все программы» → «Авест для НЦЭУ» → «Персональный менеджер сертификатов Авест для ГосСУОК» → войти в систему без авторизации → выбрать меню «Справка» → «О программе».

Если на компьютере установлена более старая версия криптопровайдера Avest CSP Bel/Персонального менеджера сертификатов Авест для ГосСУОК, то лучше всего воспользоваться обновлением всего комплекта абонента. Для установки криптопровайдера требуются права администратора.

1. Проверьте, установлена ли актуальная версия плагина **AvCMXWebP 1.1.10**.

Версию плагина AvCMXWebP можно проверить в надстройках Internet Explorer: выберите в строке меню Internet Explorer «Сервис» → «Настроить надстройки» («Надстройки») → «Отображать: Все надстройки» → ищем надстройку AVEST CryptMail X Web Plugin, версия должна быть 1.1.10, состояние «Включено».

Если плагин в надстройках не отображается или версия ниже, чем 1.1.10, то лучше всего воспользоваться обновлением всего комплекта абонента:

- с носителями AvToken или AvPass: [АРХИВ](https://nces.by/wp-content/uploads/gossuok/AvPKISetup(5.3.bel).zip)

- с носителем AvBign: [АРХИВ](https://nces.by/wp-content/uploads/gossuok/AvPKISetup(5.3.bign).zip)

Для установки Комплекта абонента в операционной системе Windows Пользователь должен иметь права не ниже "PowerUser". Запуск файла-установщика производится от имени администратора.

1. Убедитесь, что антивирусное ПО не блокирует доступ к Порталу.

Антивирус — важный элемент безопасности, но он не должен блокировать соединение с надёжными сайтами. Чтобы убедиться, что именно антивирус блокирует соединение с portal.gov.by, **на время** отключите антивирусное ПО и попробуйте зайти на портал. Если с выключенным антивирусом удаётся зайти на портал, значит требуется его дополнительная настройка, добавление сайта portal.gov.by в исключения антивируса.

В некоторых антивирусах (например, ESET NOD 32) понадобится дополнительное отключение фильтрации протоколов TLS и SSL.

1. Если авторизация перестала проходить после обновления Windows или в результате некорректной работы антивируса, требуется переустановить криптопровайдер ["AVCSPBEL" (ВЕРСИЯ 6.3.0.813)](https://www.avest.by/crypto/download/csp/setupAvCSPBel6.3.0.813.zip).
2. Для серверных операционных систем требуется дополнительная настройка.

Скачайте [Файл ключа реестра](https://nces.by/wp-content/uploads/requireSAI_DLL.zip)

Сохраните этот файл на компьютер. Распакуйте архив и запустите файл двойным щелчком мыши (изменения нужно вносить с правами администратора). Разрешите внесение изменений в реестр. Выполните перезагрузку компьютера после внесения всех изменений.

1. Обновите списки отозванных сертификатов.

См. **Приложение 1.**

1. Проверьте, доступен ли порт 4443. Выберите «Пуск» - «Выполнить» или «Поиск» - набрать cmd – наберите **telnet portal.gov.by 4443**

Если откроется пустое окно, то порт открыт. В случае неудачи появится сообщение о том, что соединение с локальным портом установить не удалось. В таком случае необходимо обратиться к системному администратору.

1. Проверьте, включено ли «Состояние безопасной загрузки».

Проверить можно: «Пуск» - «Выполнить» (на Windows 10 нажмите правой клавишей по кнопке «Пуск», в выпадающем меню выберите «Выполнить»), наберите **msinfo32 →** «OK».

В окне «Сведения о системе» найдите элемент «Состояние безопасной загрузки», если значение «Вкл.», необходимо его отключить. На большинстве компьютеров безопасную загрузку можно отключить в меню встроенного ПО (BIOS) компьютера.

**Внимание: Данную настройку рекомендуется выполнять только опытным пользователям, т.к. неправильное изменение параметра может помешать правильному запуску компьютера.**

1. Убедитесь, что на компьютере не установлен комплект программ для работы с российской криптографией компании ***«КриптоПро***». В рамках одной ОС Windows возможна работа только одного стороннего криптографического ПО. Криптографии ЗАО "АВЕСТ" и компании "КриптоПро", с точки зрения системы, являются сторонними.
2. Убедитесь, что на компьютере пользователя не используется **Kerio control**:

(**Kerio Control** (ранее назывался Kerio WinRoute Firewall и WinRoute Pro) — это программный межсетевой экран, разработанный компаниями Kerio Technologies и Tiny Software. Основными функциями программы являются: организация безопасного пользовательского доступа в Интернет, надежная сетевая защита ЛВС, экономия трафика и рабочего времени сотрудников за счёт ограничения нецелевого доступа к различным категориям веб-контента.)

1. Если вход на портал осуществляется по каналу связи – откройте файл «hosts» в блокноте (C:\Windows\System32\drivers\etc), добавьте новой строкой данное значение «**192.168.10.177 portal.gov.by**», сохраните измененный файл.

**ПРИЛОЖЕНИЕ 1**

**Способы получения актуальных Списков отозванных сертификатов (СОС):**

1. **Запуск ярлыка «Скачать СОС ГосСУОК» с рабочего стола:**

При установке комплекта абонента AvPKISetup для ГосСУОК на рабочем столе создаётся ярлык, который называется «Скачать СОС ГосСУОК». Если его запустить, он начнёт по очереди скачивать СОС из интернета и импортировать их. После его полной отработки в системе появятся актуальные СОС.

Если на вашем компьютере интернет работает через прокси, то для полноценной работы нужно отредактировать файл, который располагается по пути: c:\Program Files (x86)\Avest\AvPCM\_nces\ get\_crl.bat. Файл get\_crl.bat нужно открыть с помощью блокнота и раскомментировать строки, отвечающие за настройку прокси (удалить слово «rem»):

set PX\_USER=(указать имя пользователя)

set PX\_PASS=(указать пароль)

set http\_proxy=(указать IP-адрес прокси-сервера)

После того, как вы укажете настройки для соединения с интернет через прокси, можно будет сохранить изменения в файле get\_crl.bat и запускать ярлык «Скачать СОС ГосСУОК» с рабочего стола для обновления СОС.

1. **Автоматическое обновление через меню персонального менеджера сертификатов Авест.**

**Внимание: этот способ не поддерживается на ОС Windows ХР**. На Windows ХР не скачиваются СОС, размещённые по URL с https. Это связано с тем, что Windows ХР не поддерживает SNI (стандарт, позволяющий сделать HTTPS намного более масштабируемым).

Запустите Персональный менеджер сертификатов Авест для ГосСУОК, войдите в систему без авторизации, выберите меню «Сервис» → «Обновление СОС и сертификатов УЦ», нажмите «Далее» и дождитесь завершения процесса скачивания актуальных СОС из интернета.

1. **Ручной импорт СОС**

Скачайте тот файл СОС, который истёк и требует обновления, по одной из ссылок и сохраните на компьютер в папку, в которую вы обычно сохраняете файлы (например, Загрузки):

Корневой удостоверяющий центр (КУЦ)

[Список отозванных сертификатов (СОС КУЦ)](https://nces.by/wp-content/uploads/certificates/pki/kuc.crl).

Республиканский удостоверяющий центр (РУЦ)

[Список отозванных сертификатов (СОС РУЦ)](https://nces.by/wp-content/uploads/certificates/pki/ruc.crl);

[Сертификат службы атрибутных сертификатов юридического лица;](https://nces.by/wp-content/uploads/certificates/atrib-cert-ul.cer)

[Cписок отозванных сертификатов для центра атрибутных сертификатов РУЦ](https://nces.by/wp-content/uploads/certificates/pki/cas_ruc.crl).

Скачать СОС по каналам связи можно на следующих ресурсах:

<http://10.102.1.201/instruktsiya-po-ustanovke-avest/>

<http://10.30.254.20/?id=38>.

Запустите Персональный менеджер сертификатов Авест для ГосСУОК, войдите в систему без авторизации, выберите меню «Файл» → «Импорт сертификатов/СОС» → «Обзор…» – укажите путь к скачанному файлу СОС в формате \*.crl и проимпортируйте его, следуя указаниям. Если истёк ещё какой-то СОС, то скачайте его и повторите процедуру.