## **Инструкция по авторизации с использованием средств электронной цифровой подписи**

## **1. Действия по настройкам для авторизации и работы на портале «Единый портал электронных услуг» (**[**https://portal.gov.by**](https://portal.gov.by)**)**

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», убедитесь, что напротив пункта «Фильтрация ActiveX» не стоит галочка.
* **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 6.3.0.791**: проверить версию можно, открыв «Пуск» → «Все программы» → «Авест» → «Avest CSP Bel» → вкладка «Версия».
* **персональный менеджер сертификатов 4.0.6.1061**: 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, то лучше всего воспользоваться обновлением всего комплекта абонента.

1. Проверьте, установлена ли актуальная версия плагина AvCMXWebP.

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 1.1.8, состояние «Включено».

Если плагин в надстройках не отображается или версия ниже, чем 1.1.8, то лучше всего воспользоваться обновлением всего комплекта абонента [ForClient(AvToken\_AvPass).zip](https://nces.by/wp-content/uploads/2017/AvPKIsetup%20%28AvToken_AvPass%29.zip)

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 6.3.0.791)**](http://www.avest.by/crypto/download/csp/setupAvCSPBel6.3.0.791.exe) и [**AvCSP (версия 6.3.0.791)**](http://www.avest.by/crypto/download/csp/setupAvCSP6.3.0.791.exe).
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. [Инструкцию по импорту списка отозванных сертификатов](https://portal.gov.by/i/portalgovby/documents/certificates/insr_import_SOS.rtf).

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 установлен комплект программ для работы с российской криптографией компании ***«КриптоПро***» и с белорусской криптографией компании **«*Авест*»**. В рамках одной ОС Windows возможна работа только одного стороннего криптографического ПО. Криптопровайдеры ЗАО "АВЕСТ" и компании "КриптоПро", с точки зрения системы, оба 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.