#  Приложение № 7

к Правилам предоставления электронных банковских услуг юридическим лицам (их филиалам и представительствам), индивидуальным предпринимателям, частным нотариусам, частным судебным исполнителям, адвокатам, профессиональным медиаторам посредством системы "ЖССБ-ONLINE"

в АО "Отбасы банк"

*(изменен в редакции согласно решению Правления от 17.03.2021 г., протокол №40)*

*(изменен в редакции согласно решению Правления от 10.10.2023 г., протокол №159)*

ПАМЯТКА ПО БЕЗОПАСНОСТИ ПРИ РАБОТЕ

С КЛЮЧАМИ ЭЦП УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

1. Подготовка персонального компьютера пользователя
	1. Данная памятка является инструкцией по установке и настройке системы интернет-банкинг для Клиентов АО "Отбасы банк" на Вашем рабочем месте. *(изменен в редакции согласно решению Правления от 17.03.2021 г., протокол № 40)*
	2. Для работы в системе интернет-банк, необходимо осуществить предварительную подготовку персонального компьютера (далее – ПК) пользователя.
	3. Минимальные системные требования к ПК пользователя:
* операционная система: Windows 7, Linux, Mac OS 10;
* браузер Microsoft Internet Explorer 11.0, Google Chrome 66.0 и выше, Mozilla Firefox 43.0 и выше, Opera 53.0 и выше;
* доступ в интернет;
* NCALayer (последняя версия).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*ВНИМАНИЕ!*

*Если на Вашем рабочем месте уже установлен ЭЦП удостоверяющего центра, Вы можете перейти к пункту 5 данной инструкции и следовать указанным действиям.*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

1. Для начала работы, просим обратить внимание на то, что первичная настройка рабочего места требует наличие у Вас прав администратора на Вашем ПК или ноутбуке.
2. В случае если у Вас нет прав администратора, либо Вы не знаете, о чём идёт речь, для корректной установки системы рекомендуем вызвать IT-специалиста Вашей компании, либо обратиться в Банк к ответственному специалисту филиала для получения консультации в целях корректной установки системы.
3. Для подготовки рабочего места к работе в системе необходимо провести его настройку: установить ПО NCALayer, Java апплет, получить и установить ЭЦП, настроить веб-браузер и проверить доступ к системе.
4. ЭЦП - это аналог собственноручной подписи, который используется для придания электронному документу такой же юридической силы, как если бы этот документ был на бумажном носителе с подписью и скрепленной печатью.
5. Для получения ЭЦП, которая необходима для входа/авторизации и подписания электронных документов в системе, Вам необходимо подать онлайн заявку на выпуск регистрационного свидетельства на сайте Национального удостоверяющего центра Республики Казахстан: [www.pki.gov.kz.](http://www.pki.gov.kz/) Заявку рекомендуется подавать с личного компьютера в целях безопасности.
6. Дальнейшие действия производятся согласно размещенного на Интернет-ресурсе Банка www.hcsbk.kz "Руководства пользователя по получению регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан".
7. Соберите необходимый пакет документов и обратитесь в НАО Государственная корпорация "Правительство для граждан" (ЦОН) для подтверждения поданной заявки.
8. ЭЦП состоит из двух сертификатов (ключей):
* для авторизации - AUTH\_RSA;
* для подписи документов- GOST - для юр. лиц, RSA - для частных лиц и индивидуальных предпринимателей.
1. Настройка NCALayer в ОС Windows
2. Рекомендуем всегда ставить последнюю версию NCALayer и его последнее обновление.
3. Скачайте "NCALayer" с официального сайта pki.gov.kz. Распакуйте архив и откройте папку "NCALayer\_Windows". Запустите файл "NCALayerInstall.exe". Установите программу, следуя указаниям инсталлятора. Проставьте галочки для автоматического запуска программы "NCALayer" при загрузке операционной системы.
	1. Продолжите установку до соответствующего сообщения об успешной установке программы. Поставьте галочку "Запустить NCALayer" и нажмите кнопку "Завершить".
	2. По завершению установки NCALayer, автоматически откроется окно браузера по умолчанию, с рекомендациями по установке корневых сертификатов и использованию регистрационных свидетельств.
	3. Сразу после завершения установки "NCALayer", программа выполнит установку необходимых для работы корневых сертификатов удостоверяющего центра РК в системное хранилище сертификатов операционной системы. Окно с запросом на установку корневых регистрационных свидетельств удостоверяющего центра РК будет появляться два раза. На запрос установки корневых регистрационных свидетельств удостоверяющего центра РК необходимо ответить **"Да"**.
	4. Системное хранилище сертификатов используют браузеры Edge, Opera, Google Chrome.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*ВНИМАНИЕ!*

*Программа автоматически будет свернута в системный трей. Программу нельзя закрывать пока Вы используете функционал подписания.*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

1. Установка программы Java
	1. Для установки ПО Java необходимо запустить веб-браузер, перейти по адресу <http://www.java.com/ru/> и нажать кнопку "Загрузить Java бесплатно".



* 1. Далее нажать кнопку "Согласиться и начать бесплатную загрузку".
	2. В окне установки необходимо нажать кнопку "Install", после чего начнется процесс установки компонентов платформы Java на рабочее место, по завершении которого в новом окне необходимо нажать кнопку "Close".
1. Установка сертификата ЭЦП удостоверяющего центра
	1. После получения сертификата, производим импорт сертификат в браузеры, установленные на ПК. Находим на компьютере полученный файл, имеющий название "AUTH\_RSA" и двойным щелчком начинаем импортировать файл, запускаем Мастер импорта сертификатов.
	2. Продолжаем импорт, для чего нажимаем кнопку "Далее":
	3. Для подтверждения действия о внесении Вашего ЭЦП в хранилище сертификатов необходимо нажать кнопку "Далее" и в поле "Пароль" ввести пароль ЭЦП.
	4. Выбираем пункт Автоматически выбрать хранилище на основе типа сертификата и нажимаем кнопку "Далее".
	5. Далее нажимает кнопку Готово.
	6. Нажимаем кнопку ОК, выйдет информация об успешном импорте и подтверждаем кнопочкой ОК. Процесс завершен.
2. Вход в систему
	1. Запустите браузер и наберите в адресной строке: https[://dbo.hcsbk.kz](http://www.nova-24.kz)/. При успешном соединении будет загружена страница авторизации пользователя интернет-банкингом для

Клиентов **АО "Отбасы банк**".*(изменен в редакции согласно решению Правления от 17.03.2021 г., протокол № 40)*

* 1. В открывшемся окне необходимо указать предоставленные банком Логин и Пароль. Данные поля чувствительны к регистру вводимых символов.
	2. Далее нажмите кнопку "Войти".
	3. В открывшемся окне Вам необходимо выбрать тип "Хранилище ключей" из списка "Локальный компьютер".
	4. Нажмите кнопку "Далее".
	5. В поле "Путь к хранилищу ключей" необходимо указать путь, где расположены Ваши ключи ЭЦП. Выберите ключ аутентификации (AUTH\_RSA) и нажмите кнопку "Открыть".
	6. В появившемся диалоговом окне введите Ваш пароль на ЭЦП.
	7. Нажмите кнопку "Далее".
	8. Выбрать Ваш сертификат

|  |
| --- |
| Интернет-банк**Выбор регистрационного свидетельства для подписи**Регистрационное свидетельство \*ТЕСТОВ ТЕСТ ▼ПОДТВЕРДИТЬ Назад Отмена |

* 1. Нажмите кнопку "Подтвердить".
	2. После входа в систему сразу появиться запрос о смене пароля.
	3. Для установки нового пароля необходимо:
* указать новый пароль в поле "Новый пароль";
* повторно ввести новый пароль в поле "Подтверждение пароля".
	1. Пароль пользователя должен соответствовать следующим требованиям:
* Использование не менее восьми символов;
* Использование не менее одной цифры;
* Использование не менее одной строчной и прописной буквы;
* Использование не менее одного специального символа;
* Пароль не должен быть словарным словом, словом из диалекта любого языка или любым словом, написанном в обратном порядке;
* Пароль не должен быть основан на личных данных (например, дата рождения, адрес, имя члена семьи, также написанных в обратном порядке и т.д.);
* Запрет на повторное использование 7 (семи) последних паролей.
	1. После ввода данных следует нажать на кнопку "Изменить".
	2. Откроется форма для ввода старого пароля.

|  |
| --- |
| Смена пароля**Старый пароль** \*\*\*\*\*\*\*\*\*\*\* . ПОДТВЕРДИТЬ Отмена |

* 1. В поле "Старый пароль" необходимо ввести старый пароль и нажать кнопку "Подтвердить".
	2. Если старый пароль был введен верно, то появляется информационное сообщение об успешном изменении пароля.
	3. После успешного входа в систему открывается страница со списком счетов пользователя. Процесс настройки рабочего стола и подключения к системе завершен.
1. Обеспечение безопасности при работе в сервисе интернет - банкинга при использовании ЭЦП удостоверяющего центра
	1. Для обеспечения максимальной защищенности пользователей системы на стороне Клиента Банк рекомендует придерживаться следующих условий:
		1. Запрещается хранение ключей ЭЦП удостоверяющего центра в местах, к которым не ограничен доступ третьих лиц.
		2. Пользователи системы не должны:
* вывешивать на рабочих местах в виде подсказок, записок, сохранять на любых носителях сведения о логинах и паролях, технологических шагах пользователей системы, которые могут стать доступны третьим лицам, не обладающим правами пользователей в системе;
* передавать, пересылать данные о логинах, паролях и ключей ЭЦП удостоверяющего центра третьим лицам;
* использовать личную информацию в пароле (дату рождения, имена, номера телефонов и т.п.), а также пароли, которые использовались ранее в системе или других приложениях.
	1. Если Вам по телефону или по каким-либо другим каналам обращается человек, который представляется работником Банка, ни при каких обстоятельствах не передавайте ему конфиденциальные данные, такие как ключи ЭЦП удостоверяющего центра, логин и пароль для входа в систему. Сообщите в Банк о данном случае, так как работники Банка никогда не будут запрашивать подобные данные.
	2. Если компьютер, с которого производится работа в системе, неожиданно перестал запускаться или выдает непонятные сообщения, рекомендуется незамедлительно связаться с ответственным специалистом филиала Банка и заблокировать работу системы.
	3. При возникновении подозрений, что кто-либо владеет информацией о Вашем пароле, необходимо самостоятельно сменить пароль или обратиться в Банк для блокировки учетной записи пользователя.
	4. Если Вами было получено электронное сообщение с неизвестным вложением или со ссылкой на неизвестный Вам ресурс, необходимо удалить это сообщение, не открывая вложения и не активируя ссылку (особенно если в сообщении указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл), так как эти вложения или ссылки могут содержать как сами вирусы, так и ссылки для скачивания и установки вредоносного кода. Кроме того, рекомендуется после получения такого письма провести полную проверку компьютера антивирусным средством.
	5. При загрузке системы обязательно проверяйте, что соединение установлено именно с сервером Банка и именно по адресу https://dbo.hcsbk.kz/ для удостоверения, что вы работаете с сервисом Банка.
	6. Для защиты компьютера от угроз сети интернет используйте лицензионную антивирусную систему.
	7. Проводите регулярные проверки компьютера, на котором установлена система, на предмет наличия вирусов, с использованием обновленных антивирусных баз (рекомендуемая периодичность проверки не реже 1 раза в неделю, и обновление баз антивирусной системы по мере выпуска обновлений сигнатур).
	8. Блокируйте компьютер и не оставляйте без присмотра носитель ключей ЭЦП удостоверяющего центра.