Подключение к Системе
Банк-клиент «ELBRUS Internet»

Шаг 1

После заключения с банком Соглашения об общих правилах и условиях предоставления банковских услуг с использованием системы Банк-клиент, получите в обслуживающем подразделении банка ПИН-конверт с регистрационными данными (имя пользователя и пароль) и устройство для хранения ключа АСП USB-token.

Шаг 2

Проверьте соответствие вашего компьютера требованиям к программному обеспечению и аппаратным средствам.

Требования к аппаратным средствам

- IBM-совместимый компьютер с классом процессора не ниже Pentium 4 и объемом ОЗУ не менее 512 Мбайт, порт USB v1.1 (или выше), манипулятор «мышь»;
- не менее 100 Мбайт свободного дискового пространства;
- постоянное подключение к сети Интернет, возможность работы по протоколу HTTPS (порт 443);
- Устройство USB-token (выдается Банком);
- рекомендуемое для работы с Системой разрешение экрана – 1024x768 точек и выше.
- Мобильный телефон, подключенный к услугам оператором сотовой связи (обязателен в случае использования услуги SMS-OTP).

Требования к программному обеспечению

- Операционная система Microsoft Windows 7/8/10 - в случае использования в качестве средства подписи устройство USB-token
- Актуальные версии браузеров: Internet Explorer; Mozilla Firefox; Opera; Yandex; Google Chrome;
- На компьютере Пользователя интернет-браузер должен поддерживать выполнение сценариев JavaScript;
- Для загрузки/установки/обновления СКЗИ необходимы права «Локальный администратор», «Опытный пользователь»;
- На компьютере должен быть установлен КриптоПлагин (доступен для загрузки при авторизации в Системе при наличии прав подписи);
- Для работы с Устройством USB-token необходимо скачать и установить драйвер устройства с сайта Банка:
- Наличие лицензионного регулярно обновляемого антивирусного программного обеспечения;
- Отсутствие на компьютере Пользователя ранее установленных копий ПО КриптоПро CSP версий ниже 3.6

Шаг 3

Скачайте и установите программы для работы с устройством USB-token:

- USB-token Client-x32 — для Windows 7/8/10 (32-бит).
- USB-token Client-x64 — для Windows 7/8/10 (64-бит).

Устройство USB-token имеет стандартный пароль доступа — 1234567890. В целях безопасности смените стандартный пароль сразу после получения устройства USB-token до сохранения ключа. При создании пароля к устройству USB-token необходимо учитывать, что процедура восстановления пароля возможна только при форматировании устройства, при этом ключи будут потеряны, и необходимо проходить процедуру регистрации заново.

Информация о процедуре смены пароля на USB-token указана в разделе «Вопросы и ответы».

Шаг 4

Установите продукты КриптоПРО для поддержки шифрации передаваемых данных по алгоритму ГОСТ.

Скачайте и установите дистрибутив Крипто Про CSP 4.0:

http://elba.raiffeisen.ru/CSPSetup4.zip

В процессе установки программа потребует ввести серийный номер КриптоПро CSP 4.0, который вам направлен по системе. Для просмотра входящего сообщения с серийным номером КриптоПро необходимо войти в систему, используя имя пользователя и пароль, затем на главной странице перейти к секции «Письма/Письма из банка» и открыть сообщение с темой «Привязка ключа СКЗИ к пользователю».

Шаг 5

Войдите на сайт системы — https://elbrus.raiffeisen.ru

1. В полях **«Имя пользователя»** и **«Пароль»** необходимо ввести данные, указанные в ПИН-конверте, полученном в офисе банка и кликните по кнопке «Войти»
2. В случае первого входа система автоматически предложит изменить пароль для входа
3. В поле **«Старый пароль»** необходимо ввести Пароль, полученный в банке, в полях **«Новый пароль»*** и **«Подтверждение»** ввести новый пароль, который будет использоваться при последующих сеансах работы

***Пароль должен отвечать следующим требованиям сложности:**

- Пароль должен состоять не менее чем из 8 символов.
- В пароле должны присутствовать символы двух категорий из числа следующих:
  - прописные буквы английского алфавита от A до Z;
  - строчные буквы английского алфавита от a до z;
  - десятичные цифры (от 0 до 9);
  - специальные символы из набора !@#%&*;':",./?
- Пароль не должен содержать последовательность символов, входящую в состав индивидуального имени пользователя (логина)
- Пароль не должен содержать последовательность трех повторяющихся символов

Шаг 6

- при первом входе система автоматически предложит вам скачать и установить КриптоПлагин, после установки которого необходимо перезапустить браузер;
- при нажатии на кнопку «Да», начнется автоматическая загрузка файла BssPluginSetup.exe;
- после установки Плагина и перезапуска браузера криптографические операции будут доступны

Шаг 7

Сгенерируйте ключи АСП:

- Выберите на панели навигации в левой части экрана раздел «Обмен криптоинформацией».

- Перейдите к пункту «Запросы на новый сертификат».
- Для создания ключей АСП пользователя с правом первой подписи, подключите устройство USB-token (для каждого подписанта — отдельное устройство).
- Для пользователей с правами оператора, ключи АСП не формируются.

На панели инструментов выберите меню «Создать новый документ»:

- Заполните поля «Город» и «Адрес электронной почты», нажмите кнопку «Сохранить изменения и закрыть».
- Для хранения ключей АСП в устройстве USB-token выберите из списка ARDS JaCarta 0; AKS ifdh 0, AKS ifdh 1, Aladdin Token JC 0;
- Следуйте инструкциям системы для создания ключей АСП.
- Если для хранения ключей АСП используется устройство USB-token, то укажите ваш пароль доступа, придуманный на Шаге 3 данной инструкции;
- Отметьте документ в списке левой кнопкой мыши и нажмите кнопку «Отправить в банк для обработки». Статус запроса на сертификат должен измениться на «Выгружен».

ВАЖНО! При формировании ключей может появиться уведомление КриптоПро CSP о том, что с 01.01.2019 года меняется формат создания ключей (ГОСТ). В этом случае нужно поставить отметку «*Не напоминать в течение месяца*» и нажать на кнопку «ОК».

Срок действия ключа АСП составляет 1 год. Обновление ключа АСП выполняется дистанционно (необходимо, чтобы на момент обновления еще действовал текущий ключ АСП).

Для этого необходимо перейти в раздел «Запросы на перегенерацию сертификата» и выполнить ряд несложных действий.

Более подробная информация указана в пункте «Перегенерация ключей АСП».

Обращаем ваше внимание, что сертификаты для системы «ELBRUS Internet» невозможно копировать и переносить на другие устройства.

Шаг 8

Передайте в обслуживающее вас подразделение банка «Запрос на сертификат ключа АСП»:

- Выберите документ в списке и откройте его, затем на панели инструментов нажмите кнопку «Печать» и убедитесь, что в появившемся бланке поле «Открытый ключ клиента» заполнено.
- Распечатайте «Запрос на сертификат ключа АСП» на бумажном носителе в 2-х экземплярах, поставьте подпись владельца сертификата, подпись руководителя организации с правом первой подписи и печать организации.
- Предоставьте оба экземпляра запроса на сертификат ключа АСП на бумажном носителе в обслуживающее вас подразделение банка.
- Получите второй экземпляр Запроса на сертификат ключа АСП, подписанный уполномоченным представителем банка.
- После активации ключей АСП банком вы сможете подписывать документы в системе.
- Активация ключей АСП банком производится в течение 2 (двух) рабочих дней после получения сертификата ключа АСП.

Шаг 9

После завершения процедуры подключения убедитесь, что система работает, передав в банк тестовый документ:

- Создайте, подпишите и отправьте письмо в банк, посмотрите выписку по счету. Образец письма:

« (Полное наименование клиента) сообщает, что подключение к системе прошло успешно»

Убедитесь, что письмо было успешно доставлено в банк. Статус документа должен быть «Принят».