

ПАМЯТКА по настройке программы с использованием Internet-обозревателя

Если на компьютере планируется подписывать платежные документы, тогда необходимо установить криптосистему.

Дистрибутив криптосистемы прилагается на носителе (дискете), выданном в банке, либо может быть скачан с сайта www.capitalbank.ru – пункт «Удаленное обслуживание Банк-Клиент», затем в разделе «Полезная информация» выбрать – «Дистрибутив криптосистемы Агава» – дистрибутив находится в zip-архиве.

Запустите дистрибутив криптосистемы, и следуйте пошаговым инструкциям (лучше соглашаться с предлагаемыми вариантами).

После установки запустите клиентскую программу СКЗИ Агава для настройки.

На вопрос при запуске об использовании токен-контейнера, нажмите "нет"

В главном меню программы СКЗИ Агава выберите пункт "Параметры" – "Расположение контейнера"

В случае расположения ключей например на дискете – укажите "A:\"

В случае расположения ключей на USB-накопителе – укажите букву накопителя

При этом каталог agava_keys должен лежать в корневой папке этого USB-накопителя

Для более безопасной работы рекомендуем установить пароль на ключевой контейнер криптосистемы Агава. Для этого – запустите СКЗИ Агава. Встаньте на ключевой контейнер, правой кнопкой мыши выберите пункт «Установить пароль». Задайте пароль и повторите его для контроля. Теперь при операциях подписания будет выдаваться окно с запросом пароля. Закройте криптосистему Агава.

Для работы с Интернет-Клиентом требуется обозреватель Internet Explorer версии не ниже 6.0 с поддержкой Active-X технологии (32-разрядная версия).

Для входа в систему необходимо:

Создать ярлык на рабочем столе со следующим адресом:

<https://rs-portal.capitalbank.ru/akb.html>

Назвать этот ярлык можно как угодно.

Далее нужно зайти в панель управления в свойства обозревателя.

Закладка "Безопасность"

Выбрать "Надежные узлы". Кнопка "Узлы" –

добавить следующий адрес <https://rs-portal.capitalbank.ru/>

и добавить адрес <http://rs-portal.capitalbank.ru/>

Нажать "Добавить" для добавления.

Галочка "Для всех узлов этой зоны..." – должна быть.

Также необходимо добавить следующий адрес: <http://212.94.116.242/>

Для добавления данного адреса в список надежных узлов необходимо снять галочку,

добавить <http://212.94.116.242/>, затем снова поставить галочку "Для всех узлов этой зоны..."

Нажать "Закреть".

Стоя на пункте "Надежные узлы" нажать кнопку "Другой"

Уйти вниз открывшегося списка.

Снизу вверх проверить все пункты с цветным ромбиком (параметры ActiveX элементов)

– у цветных кубиков должен быть выбран пункт "Включить" (либо "Разрешить")

Нажать "Ок"

В закладке «Конфиденциальность» отключить «Блокирование всплывающих окон», либо оставить эту галочку, но тогда в «Параметрах» блокирования всплывающих окон задать адреса разрешенных веб-узлов: rs-portal.capitalbank.ru и 212.94.116.242 и выбрать уровень фильтрации «Низкий: разрешать всплывающие окна от безопасных узлов».

Закреть параметры конфиденциальности.

Закреть свойства обозревателя через "Ок"

Запустить ярлык для Интернет-клиента на рабочем столе.

При сообщении о заблокированных переходах и невозможности проверить сертификат нажать «продолжить», невзирая на рекомендацию обозревателя.

Перейти по ссылке для ввода пароля.

Ввести пароль и следовать рекомендациям.

Примечание:

Если на компьютере используется антивирусная система, либо система информационной безопасности то необходимо проверить режим блокирования Active-X модулей. И если требуется, то добавить адрес банковского сайта в доверенную зону этой системы.