Инструкция по подключению клиентов-нерезидентов, пользователей СПТИ к автоматизированной системе «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)»

1. Общая информация

Электронные сообщения между пользователями электронного обмена и Системой передачи финансовых сообщений (СПФС) передаются с использованием автоматизированной системы «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)».

Подключение к ТШ КБР клиента Банка России осуществляется по выделенным каналам, предоставляемым поставщиками услуг связи.

VPN-туннель должен быть развернут к серверу доступа тестового/промышленного ТШ КБР для обеспечения взаимодействия АРМ участника обмена с тестовым/промышленным сегментом ТШ КБР.

Cisco AnyConnect используется для развертывания VPN-туннеля; программное обеспечение можно загрузить непосредственно с тестового/промышленного сервера доступа ТШ КБР. Дополнительно необходимо обеспечить сетевую доступность тестового/промышленного сервера для доступа к ТШ КБР клиента с АРМ участника обмена.

Внутри VPN-туннеля программный продукт (ПП) АРМ КБР-СПФС взаимодействует с сервером ТШ КБР, который получает электронные сообщения от участника обмена и пересылает их в СПФС.

1.1 Настройка VPN-соединения с ТШ КБР

После установления сетевого подключения к ТШ КБР через выделенный канал связи поставщика услуг связи АРМ участника обмена должен иметь сетевой доступ к IP-адресам двух серверов доступа (основного и резервного) тестового/промышленного сегмента ТШ КБР:

- IP-адрес сервера основного доступа тестового сегмента ТШ КБР: 172.16.20.42;
- IP-адрес сервера резервного доступа тестового сегмента ТШ КБР: 172.16.20.74.
- IP-адрес сервера основного доступа промышленного сегмента ТШ КБР: 172.16.20.34;
- IP-адрес сервера резервного доступа промышленного сегмента ТШ КБР: 172.16.20.66.

Кроме того, необходимо обеспечить сетевую доступность тестового/промышленного сервера доступа ТШ КБР с АРМ участника обмена (IP-адреса: 172.16.20.42/172.16.20.74 и 172.16.20.34/172.16.20.66); TCP-порт: 443; UDP-порты: 500, 4500.

Cisco AnyConnect используется для развертывания VPN-туннеля. Чтобы загрузить и установить программное обеспечение Cisco AnyConnect на АРМ участника обмена, вам следует выполнить следующие шаги:

а) Подключитесь к серверу доступа ТШ КБР с помощью Internet Explorer 10 или более поздней версии: https://172.16.20.42 (тестовый сегмент) или https://172.16.20.34 (промышленный сегмент).

б) Нажмите “Continue to this website (not recommended)” (Перейти на этот веб-сайт (не рекомендуется)) (Рисунок 1).

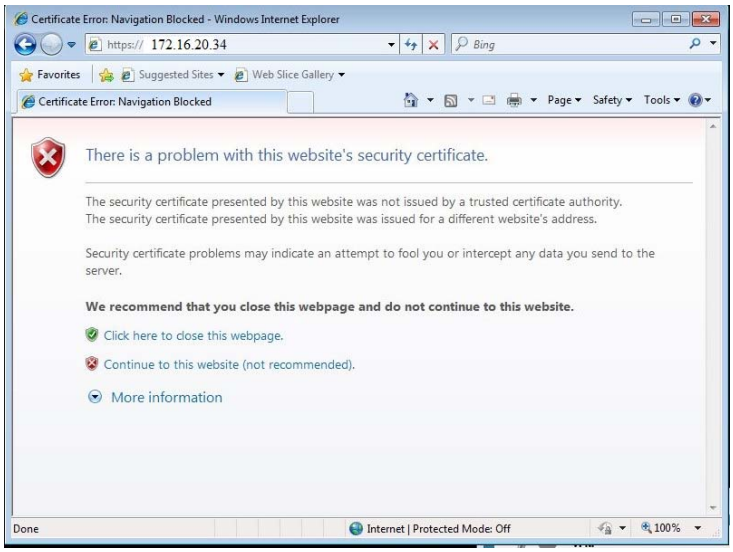

Рисунок 1 – Окно подключения к серверу доступа ТШ КБР

в) Выберите группу для подключения к ACCESS-VPN-TSH-KBR (TEST) / ACCESS-VPN-TSH-KBR (Рисунок 2) и введите, предоставленное Банком России, имя пользователя и пароль канальной учетной записи (xxxxxxxxx-xxxx) для доступа к тестовому/промышленному ТШ КБР

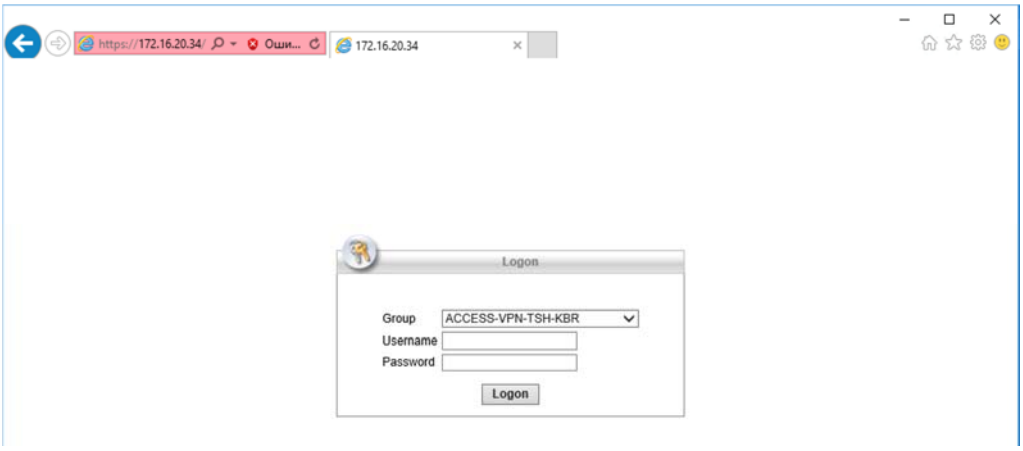

Рисунок 2 – Окно аутентификации на сервер доступа ТШ КБР

г) После ввода имени пользователя и пароля на экране появится уведомление пользователя. Нажмите «Продолжить» в нижней части уведомления.

д) Если появляется сообщение "'Security Warning: Untrusted Server Certificate" (Предупреждение системы безопасности: сертификат ненадежного сервера) (Рисунок 3), все равно нажмите "Continue" (Подключиться).

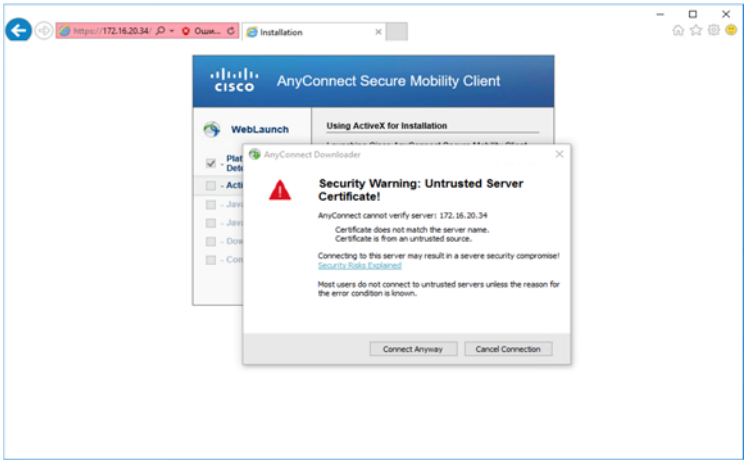

Рисунок 3 – Предупреждение системы безопасности

Если содержимое ActiveX отключено в веб-браузере участника обмена, могут отображаться следующие предупреждения. Нажмите "Yes" (Да) на экране AnyConnect Secure Mobility Client (Рисунок 3.1).

Рисунок 3.1 – Интерфейс вкладки ActiveX в AnyConnect Secure Mobility Client

На появившемся экране нажмите «Установить элемент управления ActiveX» (Рисунок 3.2).

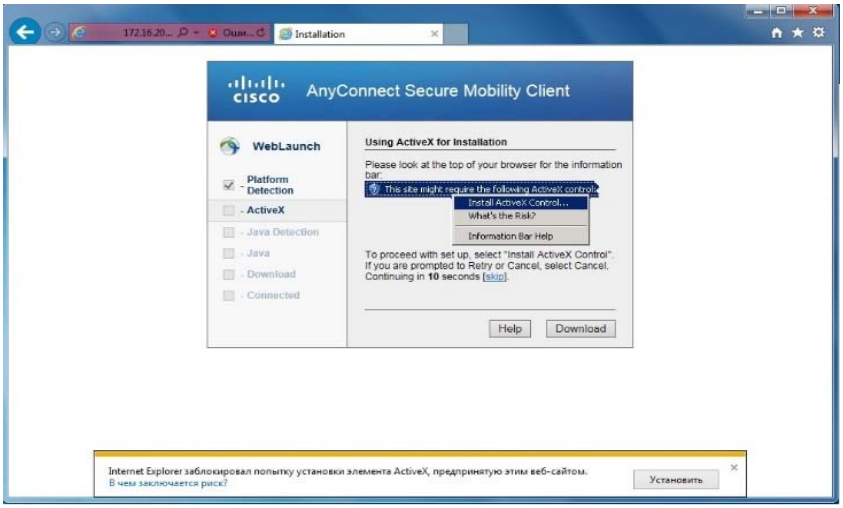

Рисунок 3.2 - Интерфейс вкладки ActiveX в AnyConnect Secure Mobility Client

е) После установки Cisco AnyConnect будет автоматически установлено VPN-соединение с сервером доступа ТШ КБР (Рисунок 4).

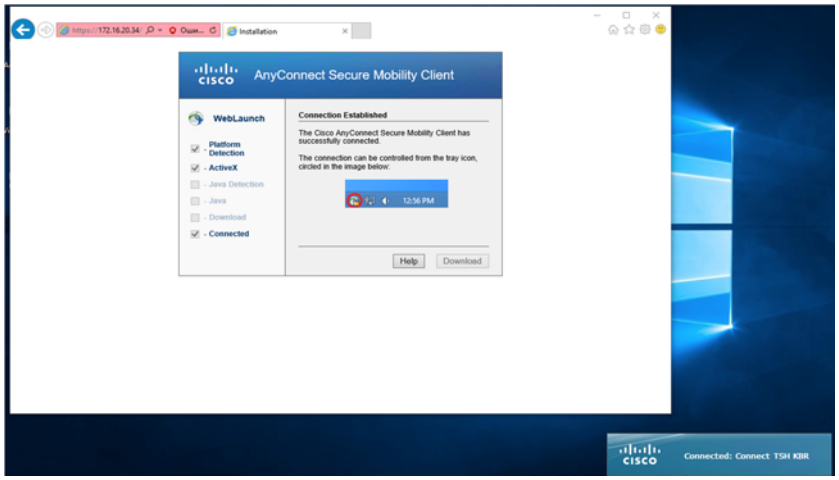

Рисунок 4 – Сообщение об установке VPN-соединения с сервером доступа ТШ КБР

ж) Найдите иконку Cisco AnyConnect на панели задач, нажмите левой кнопкой мыши на иконку и нажмите кнопку Disconnect (Отключить) в окне (Рисунок 5).

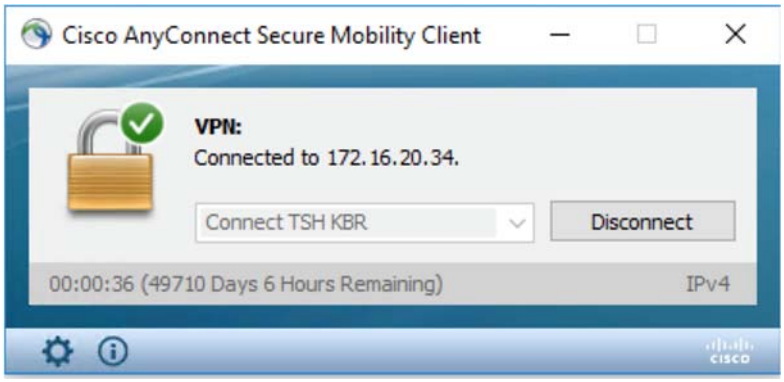

Рисунок 5 – Окно Cisco AnyConnect Secure Mobility Client

з) После отключения нажмите на крестик в правом верхнем углу окна, после чего окно Cisco AnyConnect будет уменьшено на панели задач и будет отображаться в виде иконки  .

и) Установка Cisco AnyConnect на ПК участника завершена.

1.2 Установка VPN-соединения с ТШ КБР

a) Откройте Cisco AnyConnect на АРМ участника обмена (щелкните левой кнопкой мыши по  значку на панели задач).

b) В открывшемся диалоговом окне (Рисунок 6) выберите TEST GO TSH KBR (для тестового сегмента) или PROM GO TSH KBR (для промышленного сегмента) из выпадающего списка для взаимодействия с ТШ КБР и нажмите Connect (Подключиться).

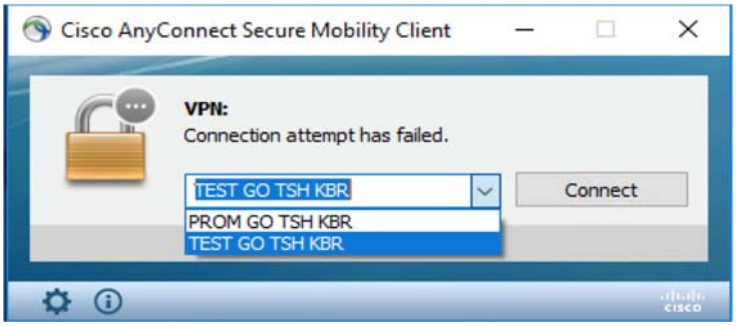

Рисунок 6 – Диалоговое окно Cisco AnyConnect Secure Mobility Client

c) Если появляется сообщение Security Warning: Untrusted Server Certificate (Предупреждение системы безопасности: сертификат ненадежного сервера), все равно нажмите Connect (Подключиться).

d) В открывшемся диалоговом окне (Рисунок 7) в раскрывающемся списке поля Group выберите ACCESS-VPN-TSH-KBR(TEST) / ACCESS-VPN-TSH-KBR, введите имя пользователя и пароль канальной учетной записи (XXXXXXXXXX-XXXX), выданной Банком России для подключения к ТШ КБР тестового/промышленного сегмента и нажать ОК.

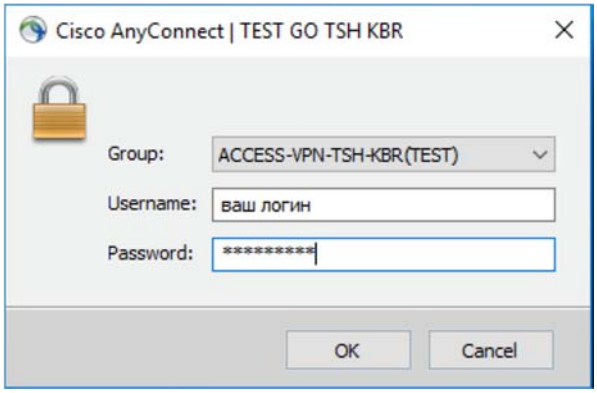

Рисунок 7 – Диалоговое окно аутентификации Cisco AnyConnect для подключения к ТШ КБР

e) После успешной аутентификации появляется диалоговое окно с сообщением о подключении к серверу доступа тестового/промышленного ТШ КБР. Нажмите «Принять».

Важно! При подключении к тестовому ТШ КБР используйте **TEST** GO TSH KBR и группу ACCESS-VPN-TSH-KBR (**TEST**). При подключении клиента к промышленному ТШ КБР используйте **PROM** GO TSH KBR и группу ACCESS-VPN-TSH-KBR.

1.3 Проверка доступности ТШ КБР для заявок, изменение каналов и учетных записей приложений участников обмена в Личном кабинете ТШ КБР

После того, как VPN-соединение **с тестовым сегментом** установлено, ПК участника обмена должен иметь доступ к серверу тестового сегмента ТШ КБР (172.16.19.211) для обеспечения взаимодействия с приложениями.

IP-адрес 172.16.19.211 предоставляет два порта для взаимодействия с ТШ КБР:

– **http**://172.16.19.211:7777 используется для взаимодействия в режиме «Система-Система». Этот адрес указывается в настройках ПП АРМ КБР-СПФС.

– **https**://172.16.19.211:9697 используется для взаимодействия в режиме «Человек-Система». Это Личный кабинет пользователя ТШ КБР, в котором он может изменить пароли канальных и прикладных учетных записей или отправлять и получать сообщения вручную.

После того, как VPN-соединение **с промышленным сегментом** установлено, АРМ участника обмена должен иметь доступ к серверу промышленного сегмента ТШ КБР (172.16.18.211) для обеспечения взаимодействия с приложениями.

IP-адрес 172.16.19.211 предоставляет два порта для взаимодействия с ТШ КБР:

– **http**://172.16.18.211:7777 используется для взаимодействия в режиме «Система-Система». Этот адрес указывается в настройках ПП АРМ КБР-СПФС.

– **https**://172.16.18.211:9697 используется для взаимодействия в режиме «Человек-Система». Это Личный кабинет пользователя ТШ КБР, в котором он может изменить пароли канальных и прикладных учетных записей или отправлять и получать сообщения вручную.

На странице аутентификации необходимо ввести логин и пароль прикладной учётной записи для подключения к тестовому/промышленному ТШ КБР, выданные Банком России, и нажать кнопку “Войти” (Рисунок 8).

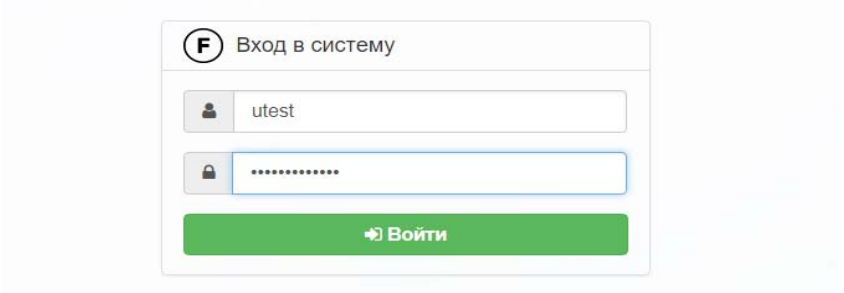

Рисунок 8 – Страница аутентификации «Личный кабинет»

После успешной авторизации участник обмена может изменять пароли канальных и прикладных учетных записей, а также отправлять и получать сообщения в ручном режиме через интуитивно понятный интерфейс.