Инструкция по работе с автоматизированной системой «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)»

(версия 1.0 от 15.01.2019)

1. Введение

1.1. Назначение

1.1.1 ТШ КБР предназначен для обеспечения централизованного доступа участников обмена к платёжной системе Банка России и пользователей СПФС к СПФС путем обмена электронными сообщениями.

1.1.2 Обмен ЭС через ТШ КБР можно осуществлять по протоколам HTTP, WMQ с использованием, как специализированных программных комплексов в режиме «система-система» (например СПО УТА, АРМ КБР-Н и т.д.), так и через Web-браузер из состава используемой на технических средствах участника обмена операционной системы для работы по протоколу HTTPS в режиме «клиент-система».

1.2. Уровень подготовки сотрудников участника обмена

Сотрудники участника обмена должны уметь работать с операционными системами семейства Microsoft Windows, Web-браузером, специальными программными комплексами, взаимодействующими с ТШ КБР (СПО УТА, АРМ КБР-Н и т.д.).

1.3. Программные средства, устанавливаемые на автоматизированном рабочем месте участника обмена

1) Операционная система MS Windows (не ниже версии 7);

2) Web-браузер для установки ПО «Cisco AnyConnect»: рекомендуется Internet Explorer (версии 10 и выше);

3) ПО «Cisco AnyConnect» предназначено для установки VPN-соединения, скачивается с сервера доступа ТШ КБР;

4) Web-браузер «Internet Explorer» (версии 11 и выше), Web-браузер «Google Chrome» (версии 66 и выше) или «Mozilla FireFox» (версии 56 и выше) для работы с личным кабинетом ТШ КБР (при обмене ЭС с ТШ КБР в режиме «клиент-система»);

5) Специальное программное обеспечение «Универсальный транспортный адаптер» (СПО УТА) (версия 2.3.1.272) или АРМ КБР-Н (последней версии) (при обмене ЭС с ТШ КБР в режиме «система-система»).

1.4. Общий порядок действий участника обмена при настройке подключения к ТШ КБР

1) Установить системное, общее и специальное программное обеспечение на ПЭВМ участника обмена;

2) Настроить специальное программное обеспечение на ПЭВМ участника обмена для взаимодействия с промышленным и тестовым ТШ КБР;

3) Обеспечить взаимодействие по локальной вычислительной сети ПЭВМ участника обмена с сервером доступа ТШ КБР (промышленным и тестовым);

4) Установить на ПЭВМ участника обмена ПО «Cisco AnyConnect» (скачивается с сервера доступа ТШ КБР).

2. Настройка подключения

2.1 Установка системного, общего и специального программного обеспечения на ПЭВМ участника обмена

Установка системного, общего и специального программного обеспечения (далее – ПО) на ПЭВМ участника обмена выполняется специалистами участника обмена в соответствии с руководствами на данное ПО. Специальных требований к установке данного ПО, необходимых для обеспечения взаимодействия с ТШ КБР, не предъявляется.

2.2 Настройка специального программного обеспечения на ПЭВМ участника обмена для взаимодействия с промышленным и тестовым ТШ КБР

Основные параметры настройки специального программного обеспечения на ПЭВМ участника обмена, необходимые для осуществления взаимодействия с промышленным ТШ КБР, приведены в таблице 1.

Таблица 1 Основные параметры настройки СПО, необходимые для осуществления взаимодействия с промышленным ТШ КБР по протоколу http.

Параметр	Значение
URL отправки собщений	http://172.16.18.211:7777/in
Корневой каталог сканирования	определяется участником обмена
URL приема сообщений	http://172.16.18.211:7777/get
Реквизиты для аутентификации на веб-сервере: Имя пользователя	имя прикладной учетной записи, выданной Банком России для взаимодействия с промышленным ТШ КБР
Реквизиты для аутентификации на веб-сервере: Пароль	пароль прикладной учетной записи, выданной Банком России для взаимодействия с промышленным ТШ КБР

Таблица 2 Основные параметры настройки СПО, необходимые для осуществления взаимодействия с промышленным ТШ КБР по протоколу MQ.

Параметр	Значение
Имя менеджера очередей	FRONTGATE
Имя соединения	172.16.18.211(1414)
Имя клиентского канала	KBR.SVRCONN
Очередь назначения (куда)	FROM.KBR
Очередь получения (от кого)	INBOX.012345678901, где 012345678901 - двенадцать цифр УИС
Реквизиты для аутентификации: Имя пользователя	имя прикладной учетной записи, выданной Банком России для взаимодействия с промышленным ТШ КБР
Реквизиты для аутентификации: Пароль	пароль прикладной учетной записи, выданной Банком России для взаимодействия с промышленным ТШ КБР

Основные параметры настройки специального программного обеспечения (СПО) на ПЭВМ участника обмена, необходимые для осуществления взаимодействия с тестовым ТШ КБР, приведены в таблице 3.

Таблица 3 Основные параметры настройки СПО, необходимые для осуществления взаимодействия с тестовым ТШ КБР.

Параметр	Значение
URL отправки собщений	http://172.16.19.211:7777/in
Корневой каталог сканирования	определяется участником обмена
URL приема сообщений	http://172.16.19.211:7777/get
Реквезиты для аутентификации на веб-сервере: Имя пользователя	имя прикладной учетной записи, выданной Банком России для взаимодействия с тестовым ТШ КБР
Реквезиты для аутентификации на веб-сервере: Пароль	пароль прикладной учетной записи, выданной Банком России для взаимодействия с тестовым ТШ КБР

Таблица 4 Основные параметры настройки СПО, необходимые для осуществления взаимодействия с тестовым ТШ КБР по протоколу MQ.

Параметр	Значение
Имя менеджера очередей	FRONTGATE
Имя соединения	172.16.19.211(1414)
Имя клиентского канала	KBR.SVRCONN
Очередь назначения (куда)	FROM.KBR
Очередь получения (от кого)	INBOX.012345678901, где 012345678901 - двенадцать цифр УИС
Реквизиты для аутентификации: Имя пользователя	имя прикладной учетной записи, выданной Банком России для взаимодействия с тестовым ТШ КБР
Реквизиты для аутентификации: Пароль	пароль прикладной учетной записи, выданной Банком России для взаимодействия с тестовым ТШ КБР

2.3 Обеспечение взаимодействия по локальной вычислительной сети ПЭВМ участника обмена с сервером доступа ТШ КБР и установка на ПЭВМ участника обмена ПО «Cisco AnyConnect»

Телекоммуникационное взаимодействие ПЭВМ участника обмена с ТШ КБР осуществляется с использованием технологии виртуальная частная сеть (VPN), которая реализуется средствами программного обеспечения (ПО) «Cisco AnyConnect».

ПО «Cisco AnyConnect» выполняет следующие задачи:

- устанавливает VPN-соединение с сервером доступа ТШ КБР;

- осуществляет автоматическое восстановление VPN-соединения при его разрыве.

Скачивание ПО «Cisco AnyConnect» на ПЭВМ участника обмена выполняется с сервера доступа ТШ КБР.

Перед установкой ПО «Cisco AnyConnect» участник обмена должен обеспечить взаимодействие по локальной вычислительной сети по протоколу HTTPS:

- с ПЭВМ участника обмена, осуществляющего обмен ЭС через сервер доступа тестового ТШ КБР – IP-адрес: 172.16.20.42;
- с ПЭВМ участника обмена, осуществляющего обмен ЭС через сервер доступа промышленного ТШ КБР – IP-адрес: 172.16.20.34.

Установка ПО «Cisco AnyConnect» на ПЭВМ участника обмена выполняется в следующем порядке:

1) Подключиться к серверу доступа ТШ КБР с использованием Web-браузер Internet Explorer (версии 10 и выше) по адресу:

- «https://172.16.20.42» - основной тестовый сервер доступа ТШ КБР;
- «https://172.16.20.34» - основной промышленный сервер доступа ТШ КБР.

Для тестового ТШ КБР основным сервером доступа является 172.16.20.42, резервным - 172.16.20.74.

Для промышленного ТШ КБР основным сервером доступа является 172.16.20.34, резервным - 172.16.20.66.

Для осуществления подключения на сетевом оборудовании в сторону ТШ КБР должны быть открыты порты взаимодействия TCP 443, UDP 500, 4500

Внимание. Если VPN-соединение устанавливается с ПЭВМ участника обмена, к которому подключение осуществляется через RDP, необходимо **НЕ РАЗРЫВАТЬ** RDP-соединение в течение 5 минут с момента запуска установления VPN-соединения. Так же перед закрытием RDP сессии рекомендуется убедиться в том, что VPN соединение установлено.

2) В открывшемся окне (рисунок 1) нажать ссылку «Continue to this website (not recommended)»;

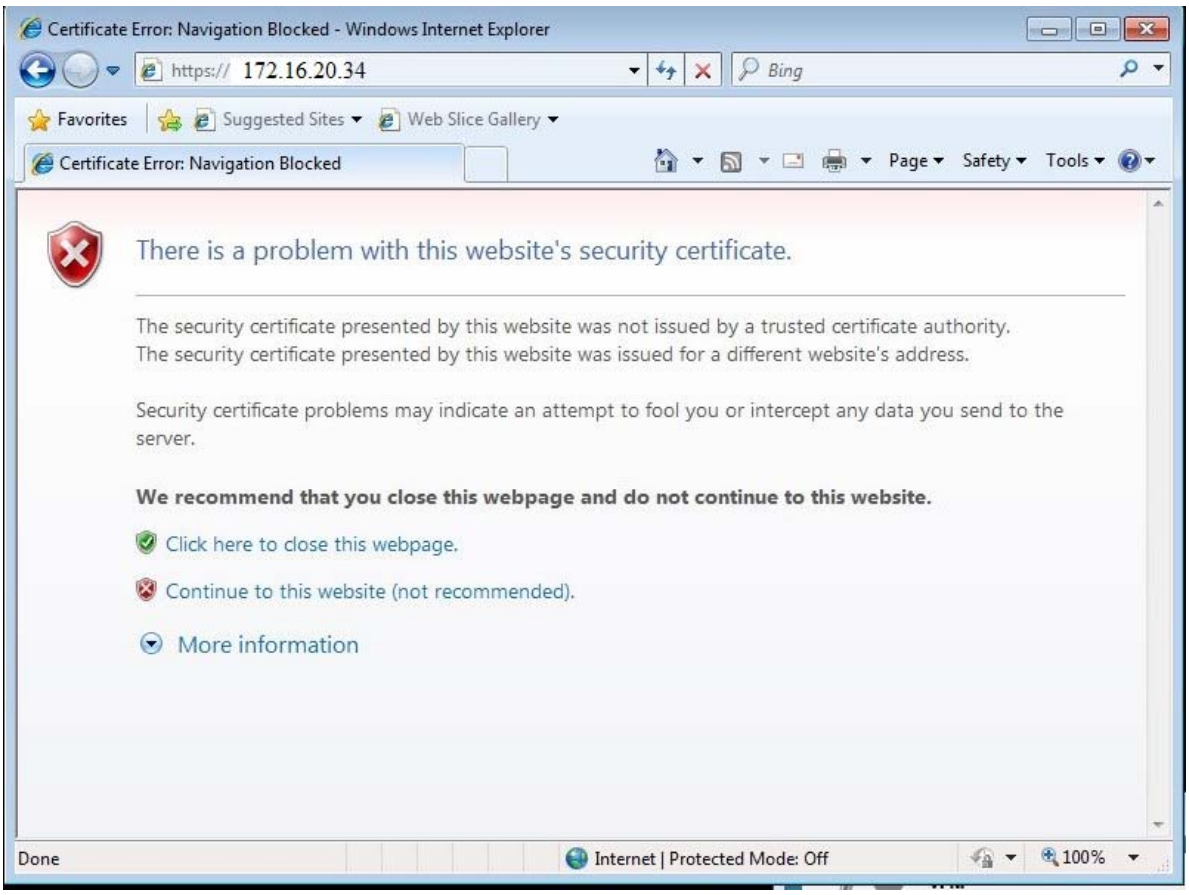


Рисунок 1

3) В открывшейся форме авторизации (рисунок 2) выбрать группу (Group), определяющую подключение к тестовому или промышленному ТШ КБР:

- ACCESS-VPN-TSH-KBR – для подключения к промышленному ТШ КБР;
- ACCESS-VPN-TSH-KBR(TEST) – для подключения к тестовому ТШ КБР.

Также, в этом окне, необходимо ввести логин (Username) и пароль (Password) канальной учётной записи для доступа к тестовому/промышленному ТШ КБР, выданные Банком России.

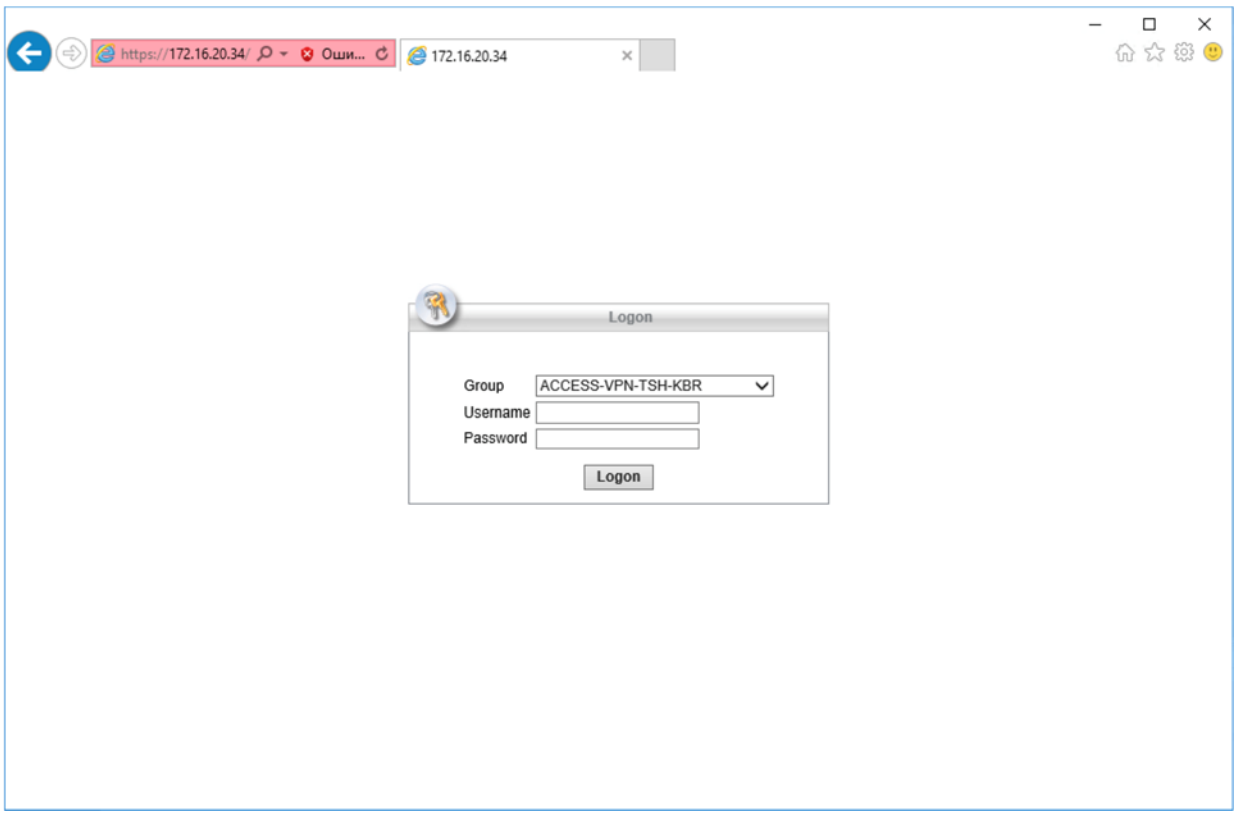


Рисунок 2

4) После ввода логина и пароля на экране появится информационное уведомление для пользователя. Внизу уведомления нужно нажать кнопку «Continue»;

5) При появлении сообщения «Security Warning: Untrusted Server Certificate» (рисунок 3) нажать кнопку «Connect Anyway»;

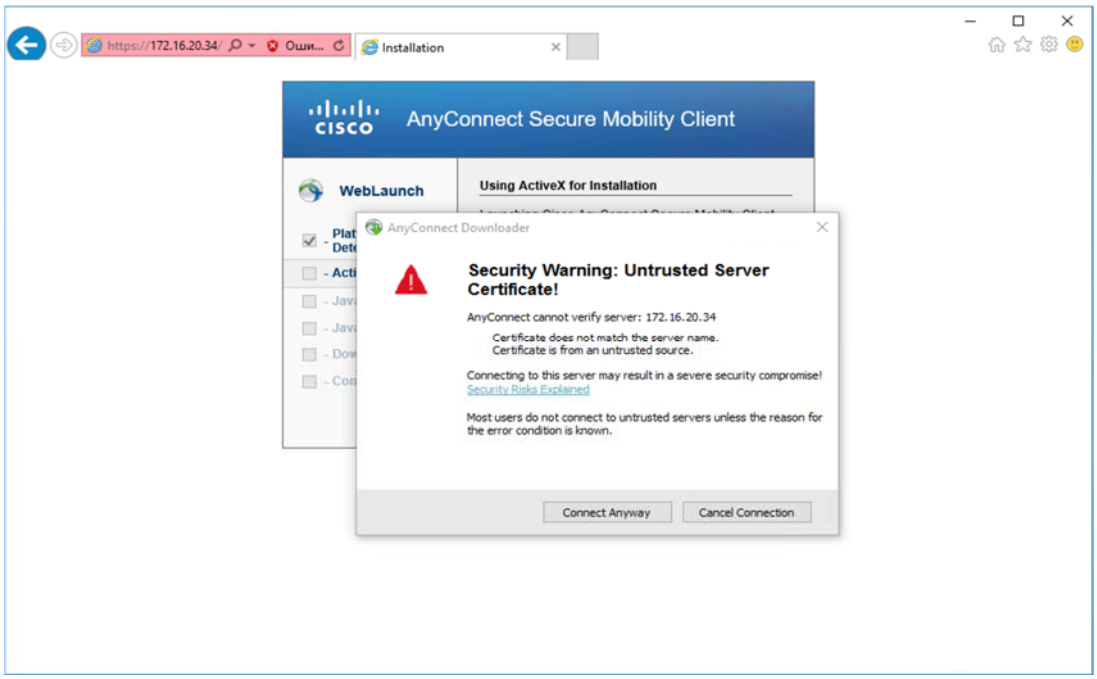


Рисунок 3

6) По окончании установки ПО «Cisco AnyConnect», автоматически будет установлено VPN-соединение с сервером доступа ТШ КБР (рисунок 4);

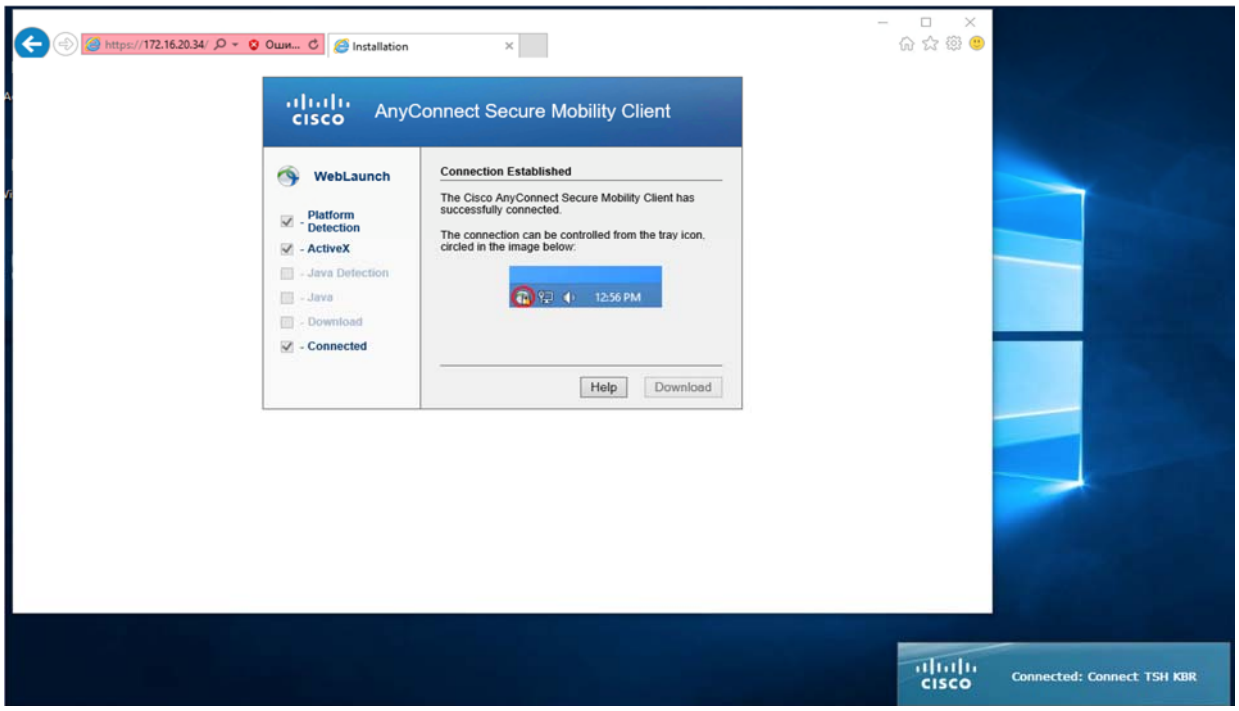


Рисунок 4

7) Далее необходимо найти в трее иконку ПО «Cisco AnyConnect»  , нажать на нее левой кнопкой мыши и в появившемся окне нажать «Disconnect» (рисунок 5);

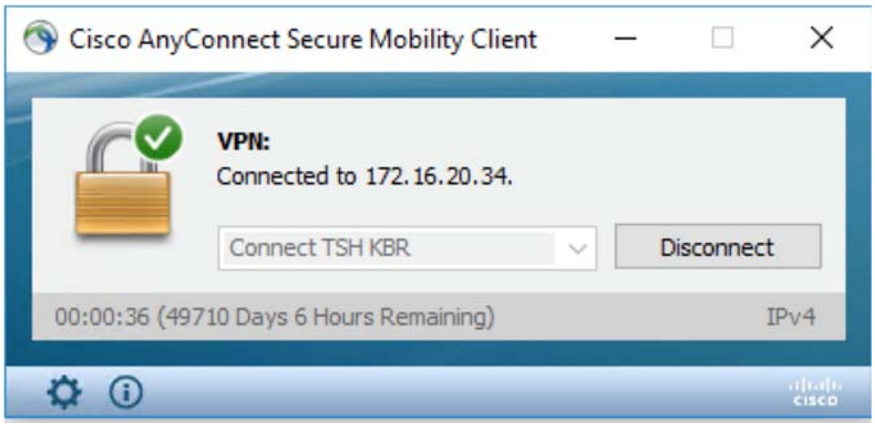


Рисунок 5

8) После разрыва соединения нажать на «крестик» в верхнем правом углу окна, после чего окно ПО «Cisco AnyConnect» будет свёрнуто в трей и обозначено значком  .

9) Установка ПО «Cisco AnyConnect» на ПЭВМ участника обмена **выполнена**.

3. Обмен электронными сообщениями с ТШ КБР

Обмен ЭС через ТШ КБР возможно осуществлять по протоколам HTTP, WMQ с использованием, как специализированных программных комплексов в режиме «система-система» (СПО УТА, АРМ КБР-Н), так и через Web-браузер по протоколу HTTPS в режиме «клиент-система» с использованием личного кабинета в ТШ КБР.

Для обмена ЭС в режиме «система-система» с помощью специализированного программного обеспечения необходимо произвести настройки специального программного обеспечения с учётом параметров, указанных в п.2.2 настоящей инструкции.

Внимание. В настройках СПО УТА необходимо в обязательном порядке устанавливать параметр «Принимать расширенный список сообщений» в значение «Нет».

Перед началом обмена ЭС необходимо установить VPN-соединение с ПЭВМ участника обмена до сервера доступа тестового/промышленного ТШ КБР с использованием ПО «Cisco AnyConnect».

3.1 Порядок установления VPN-соединения с сервером доступа промышленного ТШ КБР с использованием ПО «Cisco AnyConnect»

1) На ПЭВМ участника обмена открыть ПО «Cisco AnyConnect» (в трее рабочего стола левой кнопкой мыши нажать на значок );

2) В открывшемся диалоговом окне (рисунок 6) в выпадающем списке выбрать контур взаимодействия с ТШ КБР - «PROM GO TSH KBR» (промышленный ТШ КБР) и нажать кнопку «Connect».

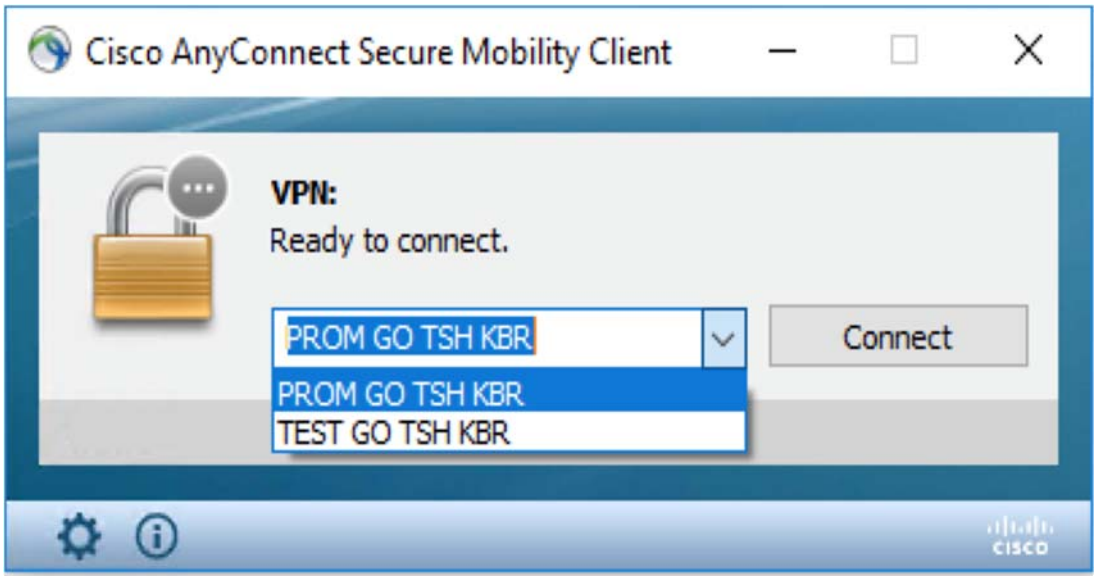


Рисунок 6

3) При открытии окна «Security Warning: Untrusted Server Certificate» нажать кнопку «Connect Anyway»;

4) В открывшемся диалоговом окне (рисунок 7) в выпадающем списке поля Group выбрать «ACCESS-VPN-TSH-KBR», ввести логин (Username) и пароль (Password) канальной учётной записи для доступа к промышленному ТШ КБР, выданные Банком России, и нажать кнопку «ОК»;

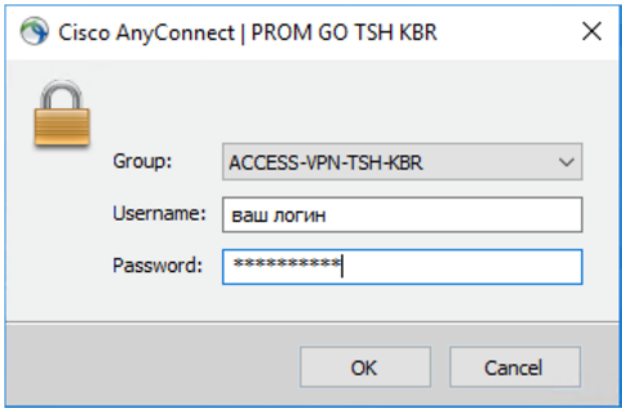


Рисунок 7

5) После успешной аутентификации будет открыто диалоговое окно с сообщением о подключении к серверу доступа промышленного ТШ КБР. В данном окне необходимо нажать кнопку «Accept»;

Важно. При подключении к промышленному ТШ КБР необходимо использовать имя контура «PROM GO TSH KBR» и группу «ACCESS-VPN-TSH-KBR».

3.2 Порядок установления VPN-соединения с сервером доступа тестового ТШ КБР с использованием ПО «Cisco AnyConnect»

1) На ПЭВМ участника обмена открыть ПО «Cisco AnyConnect» (в трее рабочего стола левой кнопкой мыши нажать на значок);

2) В открывшемся диалоговом окне (рисунок 8) в выпадающем списке выбрать контур взаимодействия с ТШ КБР – «TEST GO TSH KBR» (тестовый ТШ КБР) и нажать кнопку «Connect».

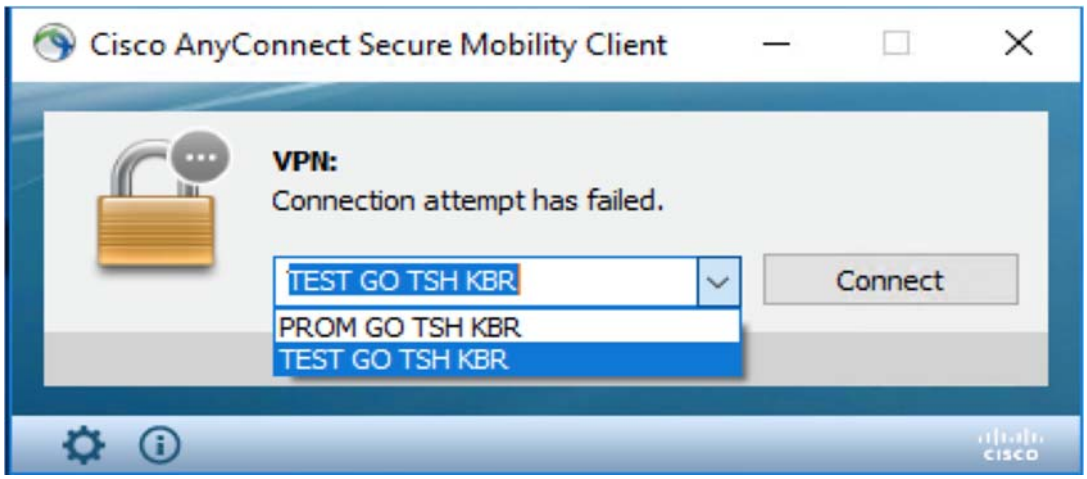


Рисунок 8

3) При открытии окна «Security Warning: Untrusted Server Certificate» нажать кнопку «Connect Anyway»;

4) В открывшемся диалоговом окне (рисунок 9) в выпадающем списке поля Group выбрать «ACCESS-VPN-TSH-KBR(TEST)», ввести логин (Username) и пароль (Password) канальной учётной записи для доступа к тестовому ТШ КБР, выданные Банком России и нажать кнопку «ОК»;

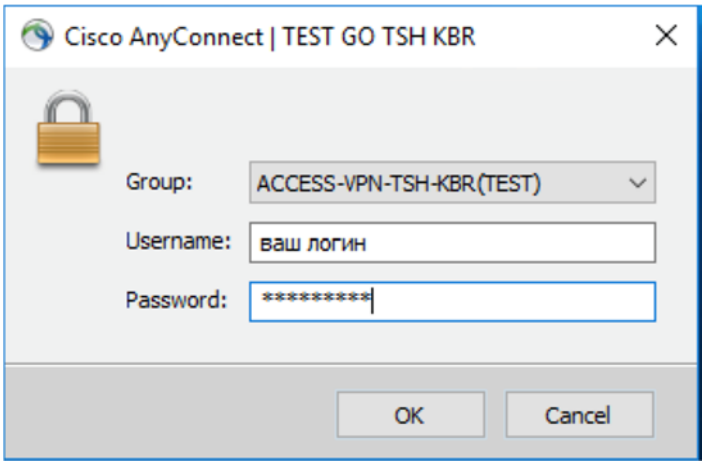


Рисунок 9

5) После успешной аутентификации будет открыто диалоговое окно с сообщением о подключении к серверу доступа тестового ТШ КБР. В данном окне необходимо нажать кнопку «Accept»;

Важно. При подключении к тестовому ТШ КБР необходимо использовать имя контура «TEST GO TSH KBR» и группу «ACCESS-VPN-TSH-KBR(TEST)».

3.3 Порядок отключения VPN-соединения ПО «Cisco AnyConnect»

1) На ПЭВМ участника обмена открыть ПО «Cisco AnyConnect» (в трее рабочего стола левой кнопкой мыши нажать на значок);

2) В открывшемся диалоговом окне нажать кнопку «Disconnect». После чего VPN-соединения с сервером доступа тестового/промышленного ТШ КБР будет разорвано.

3.4 Обмен ЭС через личный кабинет ТШ КБР

3.4.1 Вход в личный кабинет ТШ КБР

Для входа в личный кабинет ТШ КБР необходимо в адресной строке Web-браузера набрать адрес:

- для промышленного ТШ КБР (https://172.16.18.211:9697)
- для тестового ТШ КБР (https://172.16.19.211:9697)

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 10).

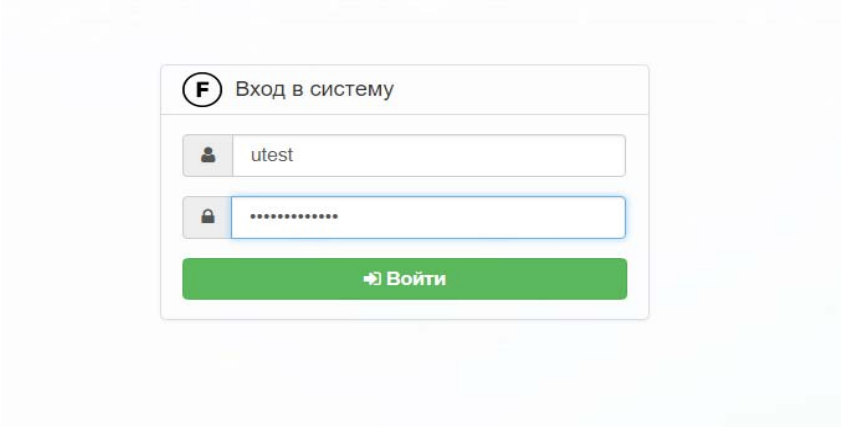


Рисунок 10

В интерфейсе личного кабинета доступны следующие операции:

№ п/п	Имя закладки Web-страницы	Операция
1	Сообщения	просмотр списка, прием и удаление электронных сообщений, предназначенных для участника обмена
2	Отправить	отправка ЭСв платежную систему Банка России
3	Аудит	просмотр истории действий пользователя
4	Смена пароля	смена пароля прикладной и канальной учётных записей пользователя

3.4.2 Смена пароля

Участник обмена при первом входе в тестовый/промышленный ТШ КБР обязан изменить первоначальные пароли для канальной и прикладной учётных записей, выданных Банком России.

Пароль должен соответствовать требованиям информационной безопасности. Длина пароля должна быть не менее 12 символов алфавитно-цифровых и специальных символов в верхнем и нижнем регистрах. Комбинация символов выбирается произвольно и не должна включать в себя легко вычисляемые сочетания (группы одинаковых цифр, имена, фамилии, наименования ПЭВМ участника обмена и т.п.), а также общепринятые сокращения.

Участник обмена должен регулярно (не реже 1 раза в 45 дней) изменять пароль своих учётных записей.

Для смены пароля прикладной учетной записи необходимо перейти на Web-страницу «Смена пароля» и нажать кнопку «Изменить пароль прикладного пользователя».

Для смены пароля канальной учетной записи необходимо перейти на Web-страницу «Смена пароля», из списка выбрать имя канальной учетной записи для которой требуется изменить пароль и нажать кнопку «Изменить пароль».

В открывшемся окне (рисунок 11) необходимо ввести текущий пароль прикладной/канальной учетной записи, новый пароль, подтверждение нового пароля и нажать кнопку «Сменить пароль».

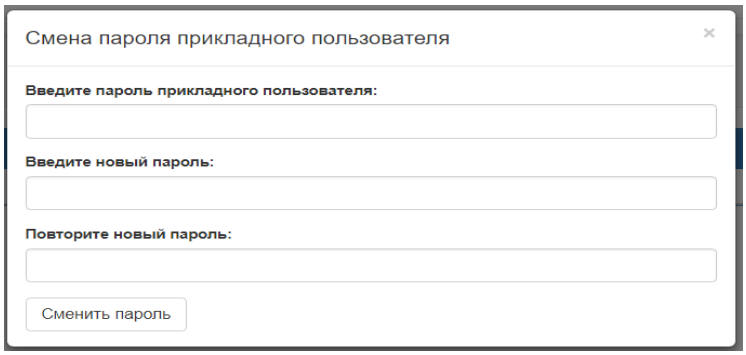


Рисунок 11

Важно. Во избежание блокирования прикладной учетной записи, перед изменением пароля необходимо на ПЭВМ участника обмена остановить работу специализированного программного обеспечения, используемого для обмена ЭС (если оно используется). В случае

блокировки канальной и/или прикладной учётных записей необходимо обращаться:

участникам обмена, расположенным в московском регионе, в Единую службу поддержки пользователей по телефону (495) 957-80-01;

участникам обмена, расположенным в других регионах, в территориальное учреждение Банка России по номеру телефона, указанному в договоре об обмене.

3.4.3 Прием ЭС с использованием личного кабинета ТШ КБР

С использованием Web-страницы «Сообщения» личного кабинета ТШ КБР (рисунок 12) выполняются следующие операции:

- просмотр списка входящих ЭС;
- прием входящих ЭС;
- удаление входящих ЭС.

В верхней левой части окна находятся ссылки на следующие Web-страницы:

- «Входящие» – просмотр списка входящих ЭС, прием и их удаление;
- «Очередь удаления» – просмотр информации об ЭС, находящихся в процессе удаления из личного кабинета участника обмена на ТШ КБР;
- «Исходящие» – просмотр информации об ЭС, находящихся в процессе передачи в ТШ КБР;
- «Отправленные» – просмотр информации об электронных сообщениях, отправленных в ТШ КБР, за период времени, установленный администратором ТШ КБР.

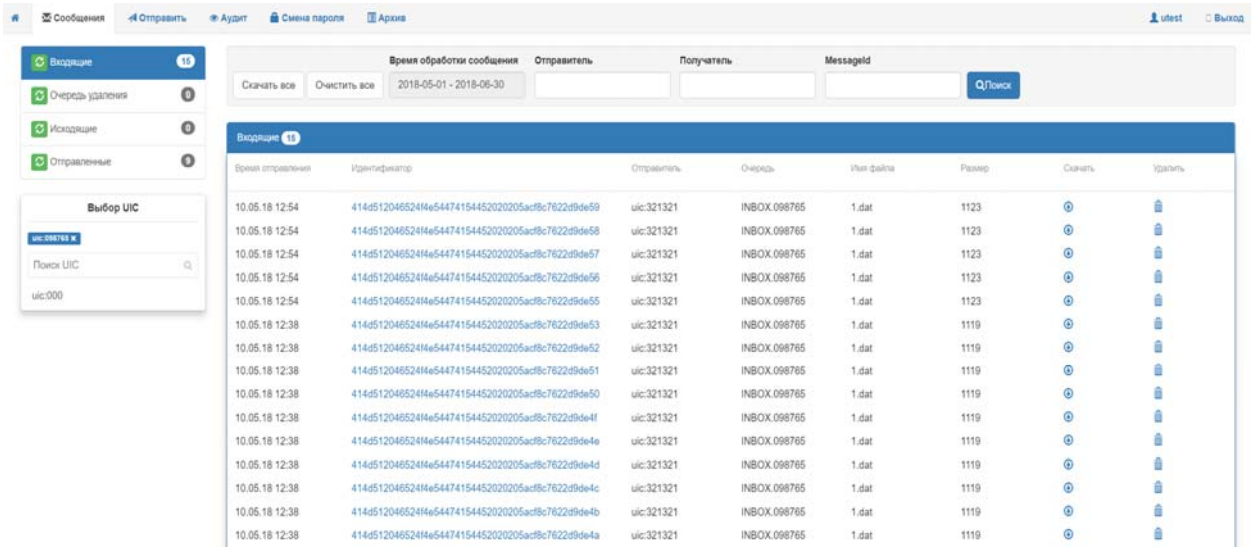


Рисунок 12

Работа с входящими ЭС в личном кабинете ТШ КБР выполняется с использованием Web-страницы «Входящие».

Список входящих ЭС можно отфильтровать по:

- дате и времени поступления ЭС в ТШ КБР – поле «Время обработки сообщения»;
- адресу отправителя ЭС – поле «Отправитель»;
- адресу получателя ЭС – поле «Получатель»;
- уникальному идентификатору ЭС – поле «MessageId».

В области «Выбор UIC» отображается список логических адресов участника обмена (УИС + номер АРМ), закрепленных за прикладной учётной записью. При выборе в списке определенного логического адреса участника обмена в списке входящих ЭС будут присутствовать только ЭС, предназначенные для выбранного логического адреса.

Прием и удаление ЭС выполняется путем нажатия иконок «Скачать»/«Удалить» напротив ЭС.

После удаления ЭС попадает в архив ТШ КБР и хранится там в течении периода времени, установленного администратором ТШ КБР.

3.4.4 Отправка ЭС с использованием личного кабинета ТШ КБР

Отправка ЭС осуществляется с использованием Web-страницы «Отправить» личного кабинета ТШ КБР (рисунок 13).

Интерфейс Web-страницы разделен на две части:

– Область загрузки файлов, обозначенная пунктирной линией и надписью «Загрузите файлы»;

– Очередь отправки, в которой отображается текущее состояние отправки ЭС.

Для отправки ЭС необходимо нажать на область загрузки файлов левой кнопкой мыши и выбрать файлы ЭС, предназначенные для передачи в ТШ КБР, либо «перетащить» (Drag-and-drop) необходимые файлы ЭС из локальной папки на область отправки файлов.

Отправлять ЭС можно по отдельности, нажав кнопку «Отправить» напротив имени файла ЭС, или все сразу, нажав кнопку «Отправить все».

Удаление ЭС выполняется нажатием кнопки «Удалить» напротив имени файла ЭС.

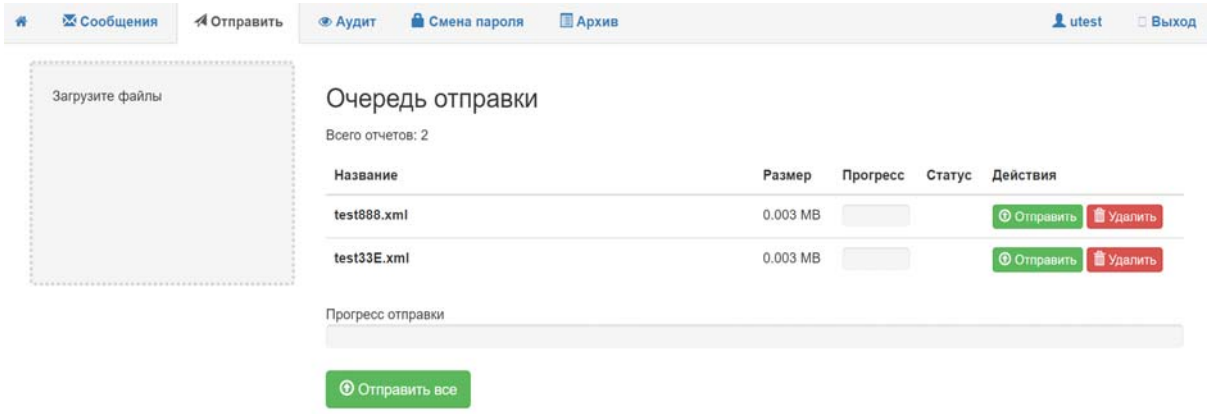


Рисунок 13

3.4.5 Работа с архивом входящих ЭС

После удаления входящего ЭС оно попадает в архив ТШ КБР и хранится там в течении периода времени, установленного администратором ТШ КБР.

Работа с архивом входящих ЭС осуществляется с использованием Web-страницы «Архив» личного кабинета ТШ КБР (рисунок 14).

Получение ЭС из архива осуществляется путем нажатия иконки «Скачать», находящейся напротив имени файла ЭС и его размера.

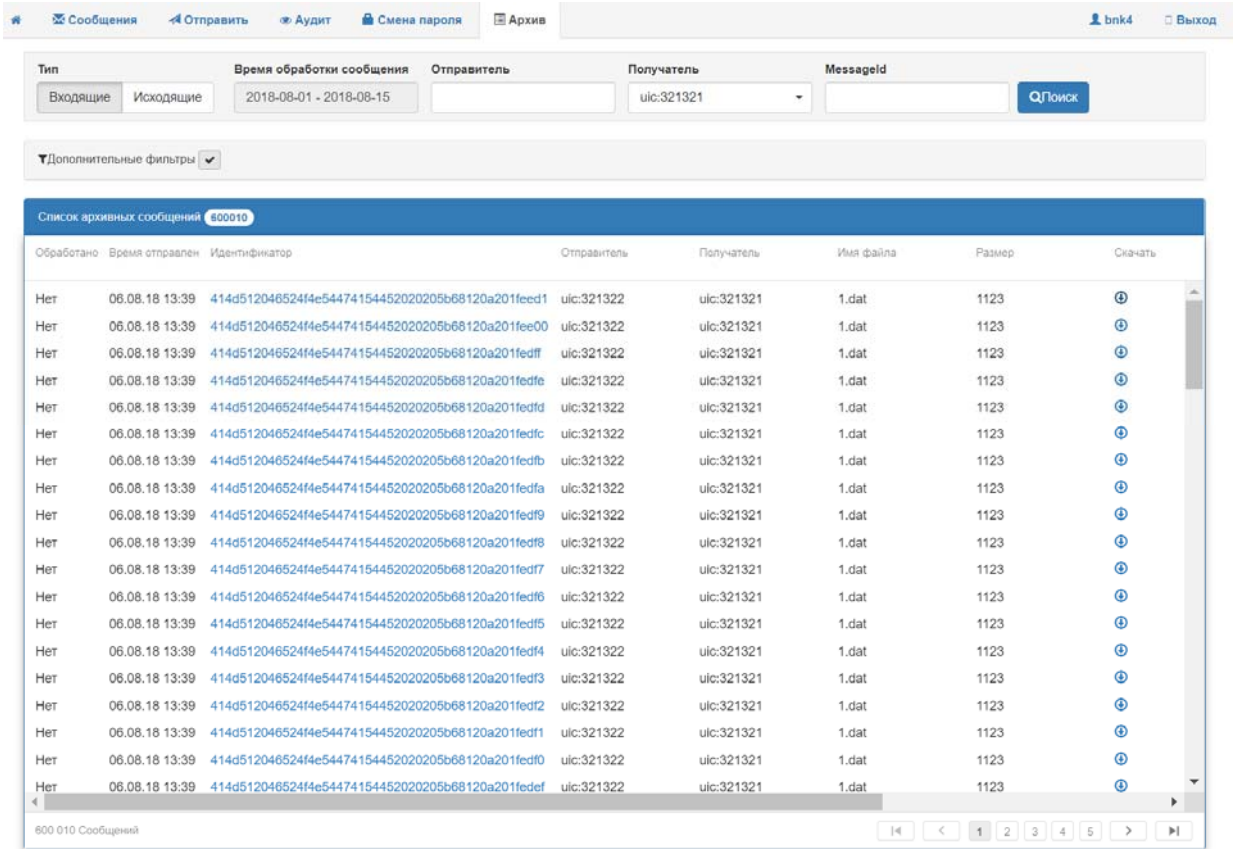


Рисунок 14

3.4.6 Выход из личного кабинета ТШ КБР

Для выхода из личного кабинета ТШ КБР необходимо нажать на надпись «Выход» в правом верхнем углу окна личного кабинета ТШ КБР.

3.5 Автоматизация работы VPN-соединения с сервером доступа ТШ КБР при обмене электронными сообщениями с использованием ПО УТА

3.5.1 Получение командных файлов для автоматизации работы VPN-соединения

1) Установить VPN-соединения с сервером доступа тестового ТШ КБР с использованием ПО «Cisco AnyConnect» в соответствии с разделом 3.2 настоящего документа.

2) С помошью Web-браузера перейти по ссылке «http://172.16.19.211:9898/settings_uta.zip» и скачать архивный файл «settings_uta.zip» (рисунок 15).

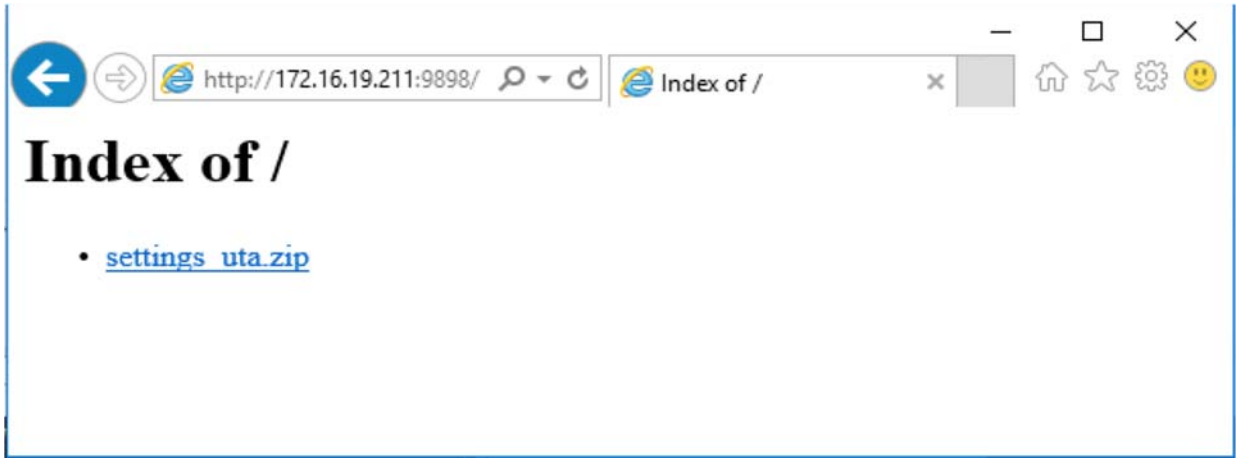


Рисунок 15

3) Распаковать содержимое архивного файла «settings_uta.zip» в директорию «C:\SettingVpnTsh».

Состав архивного файла «settings_uta.zip»:

- «ConnectTEST.bat» – командный файл, выполняющий запуск сценария «Setting.ps1», для автоматического установления VPN-соединения с сервером доступа тестового ТШ КБР с использованием ПО «Cisco AnyConnect»;
- «ConnectUOS.bat» – командный файл, выполняющий запуск сценария «Setting.ps1», для автоматического установления VPN-соединения с сервером доступа промышленного ТШ КБР с использованием ПО «Cisco AnyConnect»;

- «Disconnect.bat» – командный файл, выполняющий запуск сценария «Setting.ps1», для разрыва VPN-соединения, установленного с использованием ПО «Cisco AnyConnect», с сервером доступа тестового/промышленного ТШ КБР;
- «Setting.ps1» – сценарий Windows PowerShell, управляющий работой VPN-соединения с сервером доступа тестового/промышленного ТШ КБР с использованием ПО «Cisco AnyConnect».

Важно. Для корректной работы Windows PowerShell на ПЭВМ участника обмена необходимо выполнить следующие действия:

1) На ПЭВМ участника обмена, в коммандной строке, выполнить команду «PowerShell» с правами администратора;
2) В открывшейся окне (рисунок 16) выполнить команду «set-executionpolicy remotesigned»;
3) Подтвердить изменение политики выполнения сценариев, нажав «Y» и затем Enter;
4) Убедиться, что команда выполнилась без ошибок и закрыть окно.

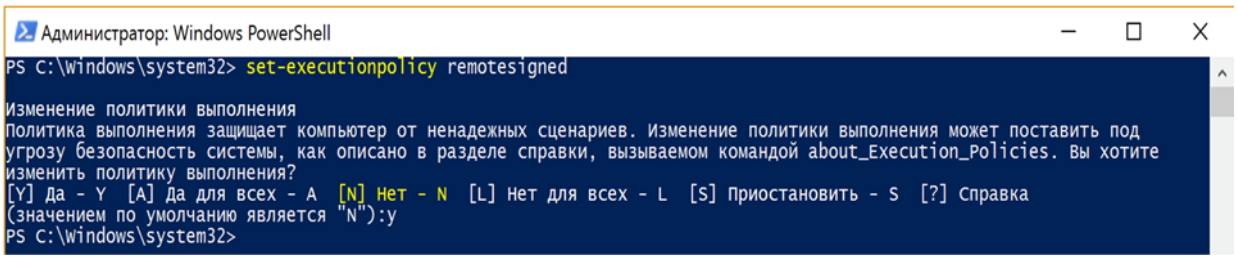


Рисунок 16

3.5.2 Настройка командных файлов «ConnectTEST.bat», «ConnectUOS.bat», «Disconnect.bat»

Перед началом работы в командных файлах «ConnectTEST.bat», «ConnectUOS.bat», «Disconnect.bat» необходимо присвоить значения следующим переменным среды Windows:

1) set **client=KO**;
2) set **TestConType**= «протокол проверки доступности ТШ КБР»;

возможные значения – **icmp** или **tcp.**

Значение переменной среды определят протокол, по которому с ПЭВМ участника обмена будет осуществляться проверка доступности

серверов доступа ТШ КБР. При значении **icmp**, проверка доступности будет выполняться по протоколу ICMP, при значении **tcp –** по протоколу HTTPS. Рекомендуется использовать значение параметра **icmp**.

3) set **OpSystem**= «разрядность операционной системы, установленной на ПЭВМ участника обмена»;

возможные значения – **32** или **64**

4) set **User**= «имя канальной учетной записи для подключения к тестовому/промышленному ТШ КБР»;

В файле «ConnectTEST.bat» указывается имя канальной учетной записи для подключения к серверу доступа тестового ТШ КБР. В файле «ConnectUOS.bat» указывается имя канальной учетной записи для подключения к серверу доступа промышленного ТШ КБР.

5) set **Password**= «пароль канальной учетной записи для подключения к тестовому/промышленному ТШ КБР»;

В файле «ConnectTEST.bat» указывается пароль канальной учетной записи для подключения к серверу доступа тестового ТШ КБР. В файле «ConnectUOS.bat» указывается пароль канальной учетной записи для подключения к серверу доступа промышленного ТШ КБР.

Внимание. Если VPN-соединение устанавливается с ПЭВМ участника обмена, к которому подключение осуществляется через RDP, необходимо **НЕ РАЗРЫВАТЬ** RDP-соединение в течение 5 минут с момента установления VPN-соединения.

3.5.3 Настройки файла сценария «Settings.ps1» в случае использования NAT (натирования адресов) в сети участника обмена

В случае использования NAT (натирования адресов) в сети участника обмена, необходимо произвести изменения в файле скрипта Setting.ps1.

Для **тестовых** серверов доступа изменить адреса **тестовых** серверов доступа (172.16.20.42, 172.16.20.74.) на натируемые в участника обмена в строке 50 скрипта Setting.ps1 в части описания настроек для тестовых серверов доступа

```
 ##################################################
#           $client = "KO"                       #
#           $zone = "TEST"                         #
##################################################
if($zone -eq 'TEST')
{
$Group = "1"
[string]$ServerInternal="172.16.19.211"
$ServerList=@( "172.16.20.42", "172.16.20.74" )
}
```

Для **промышленных** серверов доступа изменить адреса **промышленных** серверов доступа (172.16.20.34, 172.16.20.66.) на натируемые в сети участника обмена в строке 39 скрипта Setting.ps1 в части описания настроек для промышленных сервером доступа:

```
  ##################################################
#           $client = "KO"                       #
#           $zone = "UOS"                          #
##################################################
if($zone -eq 'UOS')
{
$Group = "0"
[string]$ServerInternal="172.16.18.211"
$ServerList=@( "172.16.20.34", "172.16.20.66" )
}
```

3.5.4 Настройка в ПО УТА автоматизированного управления (включение/отключение) VPN-соединением с сервером доступа тестового/промышленного ТШ КБР

В операционной системе ПЭВМ участника обмена, на котором установлено ПО УТА, в свойствах службы «UTAService» («Панель управления» – «Службы» – «UTAService») во вкладке «Вход в систему» необходимо указать имя и пароль учётной записи, зарегистрированной в операционной системе ПЭВМ участника обмена, от имени которой будет выполняться вход в систему и запускаться служба ПО УТА.

Важно. Если не выполнить данную настройку VPN-соединение с сервером доступа ТШ КБР автоматически устанавливаться не будет.

В настройках ПО УТА в разделе «Настройка событий» необходимо указать следующие параметры:

1) в поле «Программа старта» указать значение «C:\SettingVpnTsh\ConnectTEST.bat» для подключения к серверу доступа тестового ТШ КБР или «C:\SettingVpnTsh\ConnectUOS.bat» для подключения к серверу доступа промышленного ТШ КБР;

2) в поле «Программа завершения» указать значение «C:\SettingVpnTsh\Disconnect.bat»;

3) в поле «Тип запуска приложений» выбрать значение «Запускать программу запуска и завершения».

Пример настройки ПО УТА для подключения к серверу доступа промышленного ТШ КБР приведен на рисунке 17.

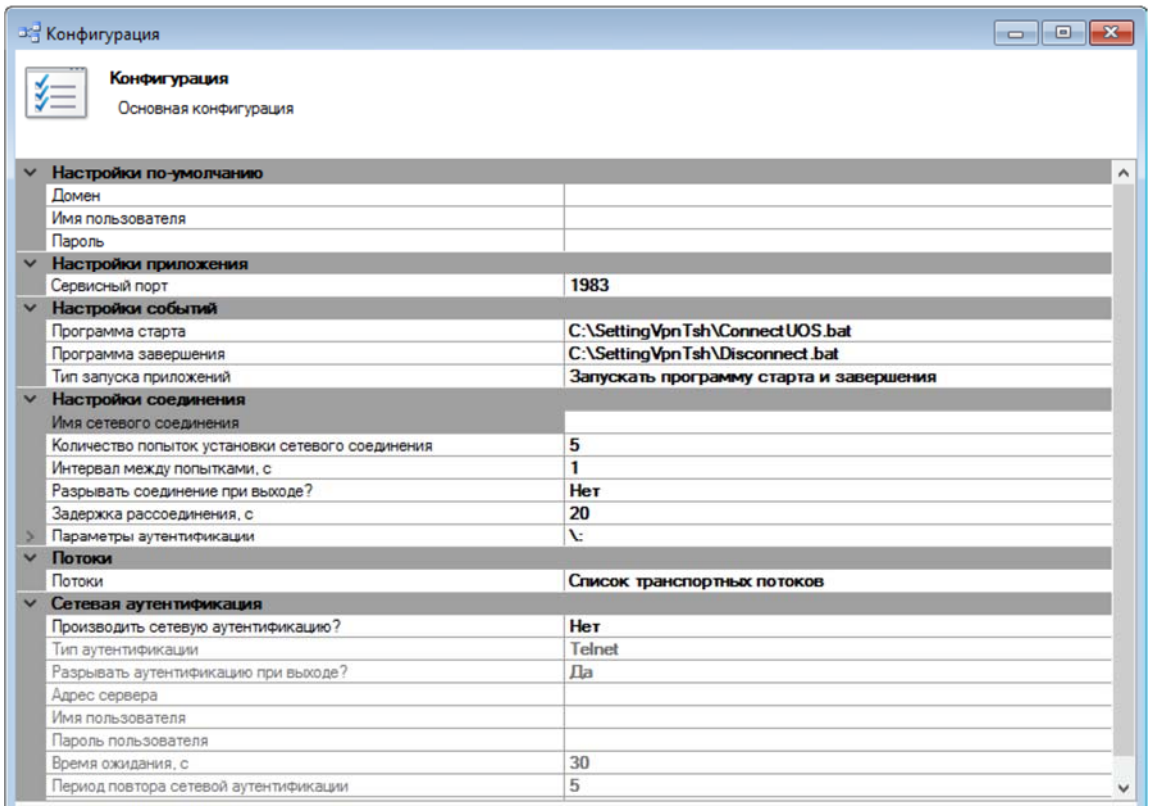
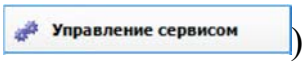


Рисунок 17

После выполнения данных настроек при запуске сервиса ПО УТА (иконка в разделе Управление сервисом) будет автоматически запускаться

процедура установления VPN-соединения с сервером доступа ТШ КБР. При остановке сервиса ПО УТА (иконка в разделе 

) будет автоматически запускаться процедура разрыва VPN-соединения с сервером доступа ТШ КБР.

Результаты установления/разрыва VPN-соединения с сервером доступа ТШ КБР фиксируются в файле «C:\SettingVpnTsh\ConnectUOS.log» (при работе с промышленным ТШ КБР) или «C:\SettingVpnTsh\ConnectTEST.log» (при работе с тестовым ТШ КБР). Пример записи результатов установления/разрыва VPN-соединения с сервером доступа ТШ КБР приведен на рисунке 18 и рисунке 19 соответственно.

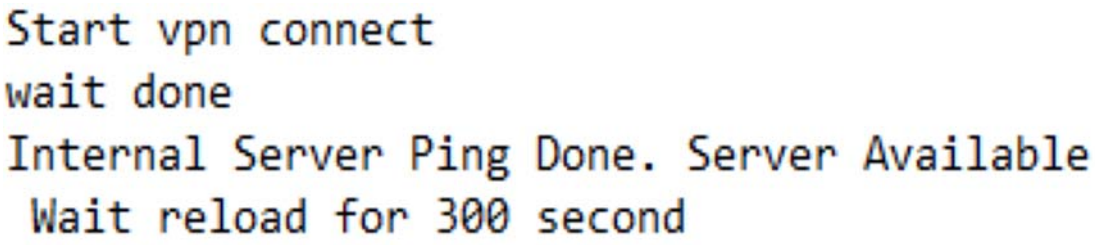


Рисунок 18 VPN-соединение с сервером доступа ТШ КБР установлено

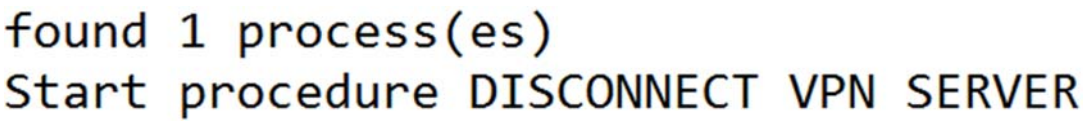


Рисунок 19 VPN-соединение с сервером доступа ТШ КБР разорвано