ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«БЕЛОРУССКИЙ МЕЖБАНКОВСКИЙ РАСЧЕТНЫЙ ЦЕНТР»

УТВЕРЖДАЮ

Председатель Правления
ОАО «БМРЦ»
_____О.И.Коробьин
04.11.2019

Кредитный регистр

КЛИЕНТСКАЯ ЧАСТЬ ПОДСИСТЕМЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Руководство пользователя

ЕУЯФ.92000-01 90 01

СОГЛАСОВАНО

Заместитель начальника
Управления «Кредитный регистр»
Национального банка
Республики Беларусь
_____Е.Ф.Пастухович
04.11.2019

2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В документе описывается ПО «Клиентская часть подсистемы информационного взаимодействия» АИС КР, которое устанавливается на рабочие места Участников Кредитного регистра, в том числе администраторов Кредитного регистра для обеспечения защищенного взаимодействия в процессе выполнения различных запросов к Кредитному регистру (на создание кредитных историй, получение отчетов, служебной информации и т.д.).

Клиентская часть подсистемы информационного взаимодействия обеспечивает выполнение предобработки сообщения формата XML – запроса, включающей синтаксический контроль и формирование ЭЦП, выполнение отправки запроса по защищенному каналу MQ на сервер приложений АИС КР, ожидания и получения сообщения MQ – ответа от сервера приложений, его синтаксический контроль и проверку ЭЦП.

Клиентская часть подсистемы информационного взаимодействия поставляется в виде инсталляционного пакета – AISCO_Client.msi, а также в виде обновлений *.msp, которые устанавливается на все рабочие места Участников Кредитного регистра (см. инструкцию по инсталляции [1]).

В состав инсталляционного пакета AISCO_Client.msi включены библиотеки функций, которые предоставляют пользователю Кредитного регистра открытый интерфейс для создания прикладных приложений (программ), непосредственно формирующих и выполняющих запросы к Кредитному регистру, а также сервисные программы для настройки и обеспечения функционирования ПО АИС КР. Такие приложения для автоматизации процесса выполнения запросов создаются пользователем самостоятельно либо используются поставляемые ПК АИС КР (например, ПК «Работа с кредитной историей. Участник АИС КР»). Какие ПК АИС КР необходимо устанавливать на рабочем месте пользователя Кредитного регистра, определяется Участником Кредитного регистра совместно с администратором Кредитного регистра. Для программиста клиентского ПО АИС КР поставляется информация об использовании предоставляемого интерфейса подсистемы информационного взаимодействия (описание требований приведено в [2]).

В состав комплекта установки AISCO_Client.msi также входит набор общих схем XSD для создания исходящих сообщений – запросов и проверки входящих сообщений – ответов, представляемых в формате XML. Требования к форматам сообщений XML приведены в [3].

В настоящем документе приведено описание механизма защищенного взаимодействия и логики выполнения запросов, описаны настройки параметров и действия пользователя для обеспечения функционирования ПО АИС КР.

При необходимости внесения изменений в настройки ПО клиентской части подсистемы информационного взаимодействия действия должны выполняться с правами администратора ОС Windows, а в ОС Windows 7 (и выше)

с включенным UAC – с повышением привилегий администратора ОС (т.е. в режиме «Запуск от имени администратора»).

В настоящем документе приняты следующие сокращения и определения:

MQ; MQSeries – коммуникационные средства гарантированной доставки сообщений – программные продукты IBM MQ;

АС МБР – автоматизированная система межбанковских расчетов;

ЗАО – закрытое акционерное общество;

Кредитный регистр (АИС КР) – автоматизированная информационная система Национального банка Республики Беларусь, обеспечивающая формирование кредитных историй, их хранение и предоставление кредитных отчетов;

носитель ключа ЭЦП (носитель ключа) – внешнее устройство eToken Pro либо iKey 1000/1032 (или раздел реестра ОС, куда ключ может быть занесен с внешнего устройства);

маршрут – набор параметров в разделе реестра ОС Windows HKLM\SOFTWARE\BTC\Router\<маршрут> (в 64-разрядных ОС – HKLM\SOFTWARE\Wow6432Node\BTC\Router<маршрут>), используемых в транспортной подсистеме защищенного взаимодействия, входящей в состав клиентской части подсистемы информационного взаимодействия АИС КР;

ОАО «БМРЦ» – открытое акционерное общество «Белорусский межбанковский расчетный центр»;

ОС – операционная система;

ПК – программный комплекс;

ПО – программное обеспечение;

ППО – прикладное программное обеспечение;

реестр ОС; реестр MS Windows – в настоящем документе – это раздел реестра операционной системы Windows HKLM\SOFTWARE\BTC (в 64-разрядных ОС – HKLM\SOFTWARE\Wow6432Node\BTC), который содержит параметры для ПО АИС КР. (Далее при указании имени раздела указывается его имя только для 32-разрядных ОС – предполагается, что имя для 64-разрядных ОС дополнительно включает Wow6432Node\);

СКЗИ – система криптографической защиты информации;

СМДО – система межведомственного документооборота государственных органов Республики Беларусь;

узел-клиент АИС КР; клиент АИС КР – рабочее место пользователя Участника Кредитного регистра с установленным ПО клиентской части информационного взаимодействия и другими ПК для выполнения запросов к Кредитному регистру. При установке ПО каждому узлу-клиенту присваивается уникальный идентификатор в АИС КР (см. инструкцию по инсталляции [1]). Узел-клиент АИС КР подключается к узлам-серверов – серверам приложений АИС КР, основному и резервному, по каналам MQ с уникальными именами. Узел-клиент АИС КР одновременно работает только с одним выбранным

сервером приложений. На одном узле-клиенте АИС КР могут выполнять свои обязанности несколько пользователей Участника Кредитного регистра, каждый со своим ключом ЭЦП (либо с одним, в случае организации так называемого серверного решения для потоковой обработки);

узел-сервер АИС КР; сервер приложений АИС КР – сервер Windows Server 2012 R2 с менеджером сервера IBM MQ и ПО серверной части информационного взаимодействия, выполняющий автоматическую обработку запросов (посредством служб Windows) и непосредственно взаимодействующий с сервером базы данных АИС КР – хранилищем данных Кредитного регистра. В состав АИС КР входит дополнительный резервный сервер приложений АИС КР (работающий в том же штатном режиме, что и основной). Серверы приложений АИС КР имеют уникальные идентификаторы узлов-сервера (AISCOSRV и AISCOSR2). При установке ПО клиентской части информационного взаимодействия выполняется настройка для взаимодействия узла-клиента с узлами-серверов (см. инструкцию по инсталляции [1]);

Управление «Кредитный регистр» – Управление «Кредитный регистр» Национального банка Республики Беларусь;

ЭЦП – электронная цифровая подпись.

В настоящем документе определены следующие роли:

администратор Кредитного регистра – работник Управления «Кредитный регистр» Национального банка Республики Беларусь, осуществляющий регистрацию, предоставление и изменение полномочий Участников Кредитного регистра;

администратор безопасности ОАО «БМРЦ» – работник Управления защиты информации в автоматизированных информационных системах (УЗИ АИС) ОАО «БМРЦ», в обязанности которого входят функции по управлению ключами СКЗИ и по регистрации/синхронизации/удалению каналов MQ Участников Кредитного регистра;

участник Кредитного регистра (Участник) – банк или организация, рабочие места которого зарегистрированы (либо будут зарегистрированы) администратором Кредитного регистра для получения доступа к функциям Кредитного регистра;

пользователь Кредитного регистра (пользователь) – работник Участника Кредитного регистра, который использует Кредитный регистр при выполнении должностных обязанностей.

разработчик ОАО «БМРЦ» – работники ОАО «БМРЦ», выполняющие работы по разработке (включая анализ требований, проектирование, приемочные испытания и внедрение) программного обеспечения Кредитного регистра;

служба сопровождения ОАО «БМРЦ» – работники ОАО «БМРЦ», которые выполняют работы по сопровождению ПО Кредитного регистра (включая услуги по технической поддержке участникам Кредитного регистра).

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ КЛИЕНТСКОЙ ЧАСТИ ПОДСИСТЕМЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Клиентская часть подсистемы информационного взаимодействия АИС КР представляет собой набор динамически подключаемых библиотек (dll, 32-bit) для ОС Windows, содержащих функции, предназначенные для выполнения запросов к Кредитному регистру и обеспечения защиты данных. Клиентская часть подсистемы информационного взаимодействия представляет собой только открытый интерфейс для использования в прикладных программах, непосредственно формирующих запросы – сообщения XML и получающих необходимые сведения из ответов – сообщений XML.

В состав клиентской части подсистемы информационного взаимодействия входят сервисные программы для настройки параметров и обеспечения функционирования ПО АИС КР. Требования к системному, специализированному ПО и устройствам описаны в инструкции по инсталляции [1].

1.1 Состав и назначение программных модулей

Клиентская часть подсистемы информационного взаимодействия включает в себя следующие программные компоненты:

– модуль выполнения запросов – библиотека вычисления/проверки подписи электронных документов АИС КР (клиентская) (DocSignc.dll);

– библиотека сохранения сообщений АИС КР с уникальными именами в архивные каталоги (savefile.dll);

– программа настройки параметров подключения к серверу приложений (SetAISCOServer.exe);

– программные компоненты информационной безопасности:

1) комплекс средств криптографической защиты информации;
2) комплекс управления ключами СКЗИ;
3) комплекс защиты соединений MQSeries;
4) подсистема защищенного взаимодействия;

– комплекс получения обновлений ППО.

Комплекс средств криптографической защиты информации включает в себя следующие программные компоненты:

– библиотеки криптографических функций (avcsk.dll, avassign.dll – библиотеки, разработанные ЗАО «Авест»; библиотека avassign.dll);

– библиотеки работы с носителями ключа (FDT_et.dll, FDT_ik.dll);

– служба защищенного хранения данных для доступа к ключам СКЗИ на носителях (HKService.exe);

– базовая библиотека криптографических функций (Crypto.dll);

– библиотека функций ЭЦП (FDT_SG.dll);

– библиотека сжатия данных (ZIPbase.dll);

– библиотеки обработки сообщений XML (Crypt_Doc.dll, Doc_XML.dll, sc_csp.dll);

Комплекс управления ключами СКЗИ:

– библиотека обработки запросов к хранилищу ключевой информации (SC_KeyMgrF.dll);

– библиотека функций запросов ключевой информации из локального хранилища (KeyFunc.dll);

– библиотека взаимодействия с хранилищем ключевой информации (KeySql.dll, содержит сообщения об ошибках);

– программа регистрации ключей СКЗИ (RegCenter.exe, содержит вспомогательные модули для перекодировки и преобразования: BasicInteraction.dll, FITS.Interop.dll – и библиотеки DevExpress);

Комплекс защиты соединений MQSeries:

– модуль аутентификации каналов, реализованный как программа выхода security exit (CSQAUTH.dll);

– модуль канального шифрования, реализованный как программа выхода send/receive exit (CSQCPHR.dll);

– библиотека функций регистрации каналов (RegAuth.dll);

– программа регистрации каналов (RegAuth.exe);

– библиотека административных уведомлений (KC_AdmNotify.dll);

Подсистема защищенного взаимодействия:

– библиотека базовых функций (Basic.dll);

– библиотека менеджера памяти (MemMgr.dll;

– библиотека менеджера сообщений (MsgMgr.dll);

– библиотека для отображения в системном журнале сообщений, записанных функциями библиотеки MsgMgr.dll (errmes.dll);

– библиотека базовых функций работы с MQSeries (MQBasec.dll);

– библиотека шифрования данных встроенными алгоритмами Windows (WinCrypt.dll);

– программа настройки таблицы маршрутизации (TransportParam.exe, BTCutils.dll – библиотека вспомогательных функций);

Комплекс получения обновлений ППО:

– библиотека обработки запросов на получение обновлений (UpdtChk.dll);

– программа загрузки обновлений (SoftUpdate.exe);

– служба автоматического обновления ППО (UpdateService.exe);

– программа настройки параметров автоматического обновления (UpdateParams.exe).

Примечание – Компоненты информационной безопасности в составе клиентской части подсистемы информационного взаимодействия АИС КР заимствованы из АС МБР, включая соответствующую документацию.

Библиотеки функций подсистемы информационного взаимодействия могут быть интегрированы как в автоматизированное рабочее место конечного пользователя, так и во взаимодействующую с АИС КР автоматизированную систему. В составе установочного комплекта поставляются примеры scan.exe и stop.exe (с исходным кодом) для организации собственной потоковой обработки. Использование примеров программ scan.exe и stop.exe недопустимо в производственной эксплуатации.

Дополнительно, по запросу организации – Участника Кредитного регистра, для реализации потоковой обработки запросов удаленных пользователей (так называемого серверного решения), поставляются инструкции по занесению ключа ЭЦП в память компьютера и программные модули: программа записи ключевой информации из носителя ключа в память компьютера (KeyToMem.exe) и библиотека для работы с носителем ключа, сохраненного в памяти компьютера (FDT_Mem.dll). По вопросам получения дополнительного ПО следует обращаться к администратору Кредитного регистра.

2 ОБЩЕЕ ОПИСАНИЕ

2.1 Описание механизма защищенного взаимодействия

Взаимодействие пользователей с Кредитным регистром осуществляется посредством обмена сообщениями MQ – запросами и ответами – XML-сообщениями установленного формата. В составе комплекта установки пользователю поставляются набор общих схем XSD для запросов к Кредитному регистру и соответствующих ответов Кредитного регистра.

Выполнение запроса к Кредитному регистру включает выполнение «неразрывных» операций подписи (вычисления ЭЦП) запроса, отправки его на сервер приложений АИС КР, ожидания и получения от сервера приложений ответа и проверки ЭЦП ответа. Средством выполнения запросов является распределенная подсистема информационного взаимодействия АИС КР, состоящая из клиентской и серверной части, соответственно устанавливаемых на клиентских рабочих местах и на сервере приложений АИС КР.

В АИС КР функционируют два сервера приложений, взаимодействующие с базой данных Кредитного регистра. В зависимости от настроек выполнение запросов клиента АИС КР может осуществляться через основной сервер приложений AISCOSRV либо через резервный сервер приложений AISCOSR2.

2.1.1 Защита соединений IBM MQ

Транспортная среда подсистемы информационного взаимодействия строится на основе сервера IBM MQ, установленного на сервере приложений АИС КР, и клиентов IBM MQ, устанавливаемых на компьютерах пользователей АИС КР. Передача и прием сообщений Кредитного регистра осуществляется в виде сообщений MQ посредством клиентских каналов и очередей MQ.

На уровне подключения каналов MQ осуществляется взаимная аутентификация сторон узла-сервера – сервера приложений АИС КР и узла-клиента – рабочего места пользователя АИС КР. Процедура взаимной аутентификации реализована в соответствии с протоколом, приведенным в [4]. Подсистема информационного взаимодействия, используя встроенные средства аутентификации, гарантирует, что запрос к Кредитному регистру будет получен только от зарегистрированного рабочего места пользователя АИС КР (клиента АИС КР), и то, что ответ будет выдан сервером приложений АИС КР.

Защита конфиденциальности данных обеспечивается посредством канального шифрования данных, устанавливаемого для всех клиентских каналов MQ (с аутентификацией). Шифруется весь «трафик», включая управляющие сообщения (содержащие, в том числе, имена соединений). Шифрование осуществляется в соответствии со стандартом [5]. Ключом шифрования является сеансовый ключ, вырабатываемый при каждом подключении клиентского канала (общий ключ аутентификации). Описание комплекса защиты соединений MQSeries приведено в [6].

При подключении клиента АИС КР производится процедура регистрации канала MQ, в процессе которой выполняется генерация комплекта ключей для протокола взаимной аутентификации и запись ключевых данных в память компьютеров узла-сервера (на сервере приложений) и узла-клиента (на клиенте АИС КР). Регистрация канала производится администратором безопасности ОАО «БМРЦ», созданный регистрационный файл канала передается для регистрации на узел-клиента – рабочее место пользователя (см. [11]). На рабочем месте пользователя АИС КР используется программа регистрации каналов (RegAuth.exe), описание работы которой приведено в [7].

Для нового клиентского места регистрируются два канала MQ – для подключения к основному серверу приложений и к резервному серверу приложений. Клиент АИС КР настраивается на работу с одним из выбранных серверов приложений, устанавливая его активным в программе настройки параметров подключения к серверу приложений АИС КР (см. 3.7).

В клиентских каналах на стороне сервера приложений АИС КР для разграничения прав доступа к объектам MQ для пользователей Кредитного регистра устанавливается технологический идентификатор MCA-пользователя MCACLNT, для администраторов Кредитного регистра – MCAADMIN.

2.1.2 ЭЦП

Запросы пользователя АИС КР и ответы сервера приложений АИС КР являются электронными сообщениями, содержащими ЭЦП, которая служит для подтверждения целостности и подлинности сообщений. Выработка (подписывание) и проверка ЭЦП осуществляется с использованием встроенных в подсистему информационного взаимодействия сертифицированных средств ЭЦП (разработанных ЗАО «Авест»), которые реализованы в соответствии со стандартами [8] и [9]).

При подключении клиента АИС КР (рабочего места) для каждого пользователя АИС КР создается личный ключ ЭЦП. Соответствующий сертификат открытого ключа ЭЦП помещается на серверы приложений АИС КР для проверки ЭЦП XML-запросов. Сертификаты открытых ключей серверов приложений АИС КР поставляются на все узлы-клиенты АИС КР для проверки ЭЦП XML-ответов.

При установке клиентского рабочего места осуществляется запрос локальной базы сертификатов открытых ключей СКЗИ (см. 3.6.2). Локальная база сертификатов открытых ключей СКЗИ клиента АИС КР включает сертификаты открытых ключей ЭЦП серверов приложения АИС КР и всех открытых ключей ЭЦП группы пользователей СКЗИ (заданной при установке ПО).

Управление ключами ЭЦП, генерация, создание заявок на регистрацию осуществляется непосредственно на рабочем месте пользователя АИС КР с использованием программы регистрации ключей СКЗИ. Описание работы программы приведено в [10].

Операции с ключами ЭЦП (новый ключ, смена, удаление) осуществляются в соответствии с заявками (на бумажных носителях или в электронном виде через СМДО), приведенными в [11], при непосредственном взаимодействии с администратором безопасности ОАО «БМРЦ».

2.1.3 Права для выполнения запросов

При выполнении запросов в базе данных Кредитного регистра выполняется авторизация каждого пользователя АИС КР (по идентификатору ключа ЭЦП) с точностью до предоставляемых прав на выполнение каждого типа запроса. Права предоставляются администратором Кредитного регистра в соответствии с заявкой на предоставление/удаление полномочий по доступу к ресурсам Кредитного регистра, приведенной в [11].

2.2 Описание логики выполнения запросов

Для выполнения запроса прикладные программы клиента АИС КР (поставляемые либо собственные программы для автоматизированной потоковой обработки) вызывают функции библиотек клиентской части подсистемы информационного взаимодействия. Основной функцией является функция ExecDataProc из библиотеки базовых функций Basic.dll или пара функции: Send и Receive – при разделенном процессе отправки запроса и получения ответа. В качестве входных параметров на вход функций передаются: информация о логическом маршруте, указатель на передаваемые данные запроса в памяти и их размер и/или указатель на буфер для получаемых данных ответа.

Логический маршрут (маршрут) – это комплект параметров подсистемы защищенного взаимодействия, используемый функциями Basic.dll, устанавливаемый в разделе реестра ОС HKLM\SOFTWARE\BTC\Router. Имя подраздела в этом разделе реестра является именем (идентификатором) маршрута. Параметры маршрута определяют направление для передачи, приема либо обработки данных в распределенной транспортной подсистеме защищенного взаимодействия (тип маршрута определяет работу с файлами, с реестром ОС, сообщениями MQ и др.). Для настройки и просмотра маршрутов используется программа настройки таблицы маршрутизации TransportParam.exe (см. 3.1), ярлык для запуска которой расположен на рабочем столе и имеет наименование «Настройка параметров транспорта».

Основным начальным маршрутом для выполнения запросов АИС КР является маршрут KB (см. настройки маршрута в окне программы TransportParam.exe на рисунке 1). Все настройки маршрута в реестре приведены в таблице А.1 Приложения А. В маршруте KB дополнительно могут быть настроены параметры для внутренних повторов при недоступности менеджера, включая сбои в сети, и параметры для внутренних повторов по истечении интервала ожидания ответов. Данные параметры применяются при передаче запроса для выполнения на сервер приложений по маршруту «Дальнейшая обработка» (см. окно программы TransportParam.exe).

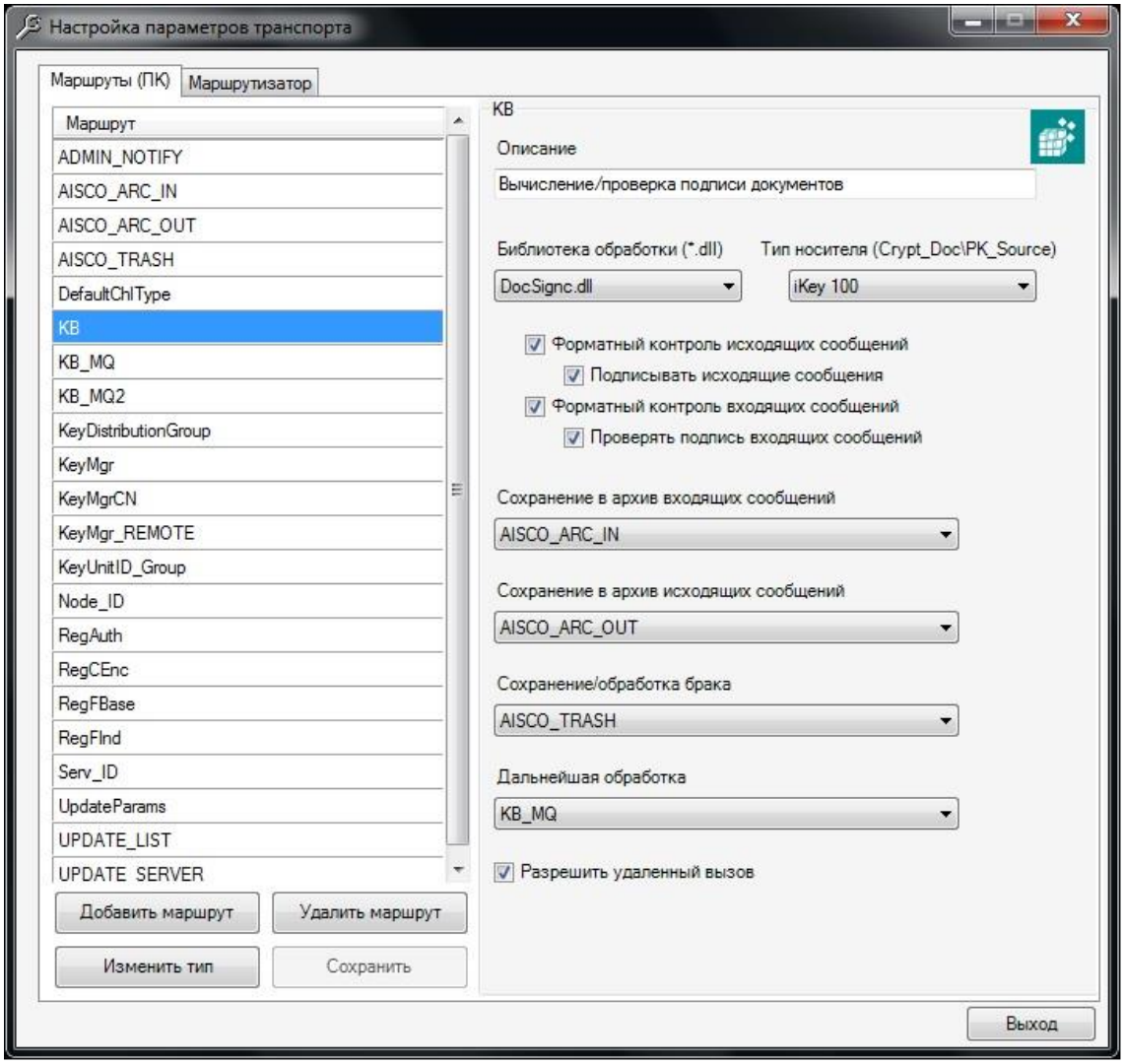

Рисунок 1

Передаваемые данные запроса и получаемые данные ответа представляют собой сообщения формата XML. Сообщения запросов и ответов должны формироваться на основании схем XSD, которые устанавливаются как на узле-клиенте, так и на сервере приложений АИС КР.

Получив имя маршрута KB, функция Basic.dll (ExecDataProc) передает управление библиотеке вычисления/проверки подписи электронных документов АИС КР (DocSignc.dll), которая установлена в маршруте KB как библиотека обработки (обработчик). В обработчике DocSignc.dll выполняются следующие действия:

1) **выполнение предобработки запроса.** Осуществляется синтаксический форматный контроль и подписывание, т.е. вычисление ЭЦП, в соответствии с установленными опциями в маршруте KB для исходящих сообщений. Если произошла ошибка в процессе предобработки, то сообщение направляется по маршруту «Сохранение/обработка брака» (AISCO_TRASH), если такой маршрут установлен в маршруте KB. Если произошла ошибка в процессе обработки брака,

то обработчик завершает работу и возвращает: код ошибки в процессе обработки брака, если произошла ошибка контроля, или код ошибки вычисления ЭЦП, если произошла ошибка при подписывании;

2) **сохранение сообщения запроса**, прошедшего предобработку, в архиве исходящих сообщений. Выполняется передача сообщения по маршруту «Сохранение в архив исходящих сообщений» (AISCO_ARC_OUT), если в маршруте КВ установлен такой маршрут. Если произошла ошибка при сохранении, то обработчик завершает работу и возвращает код этой ошибки;

3) **передача запроса для выполнения на сервер приложений**. Передача производится по маршруту «Дальнейшая обработка» (KB_MQ#, где # – порядковый номер сервера приложений, для основного – отсутствует), указанному в маршруте КВ (см. окно программы TransportParam.exe на рисунке 2).

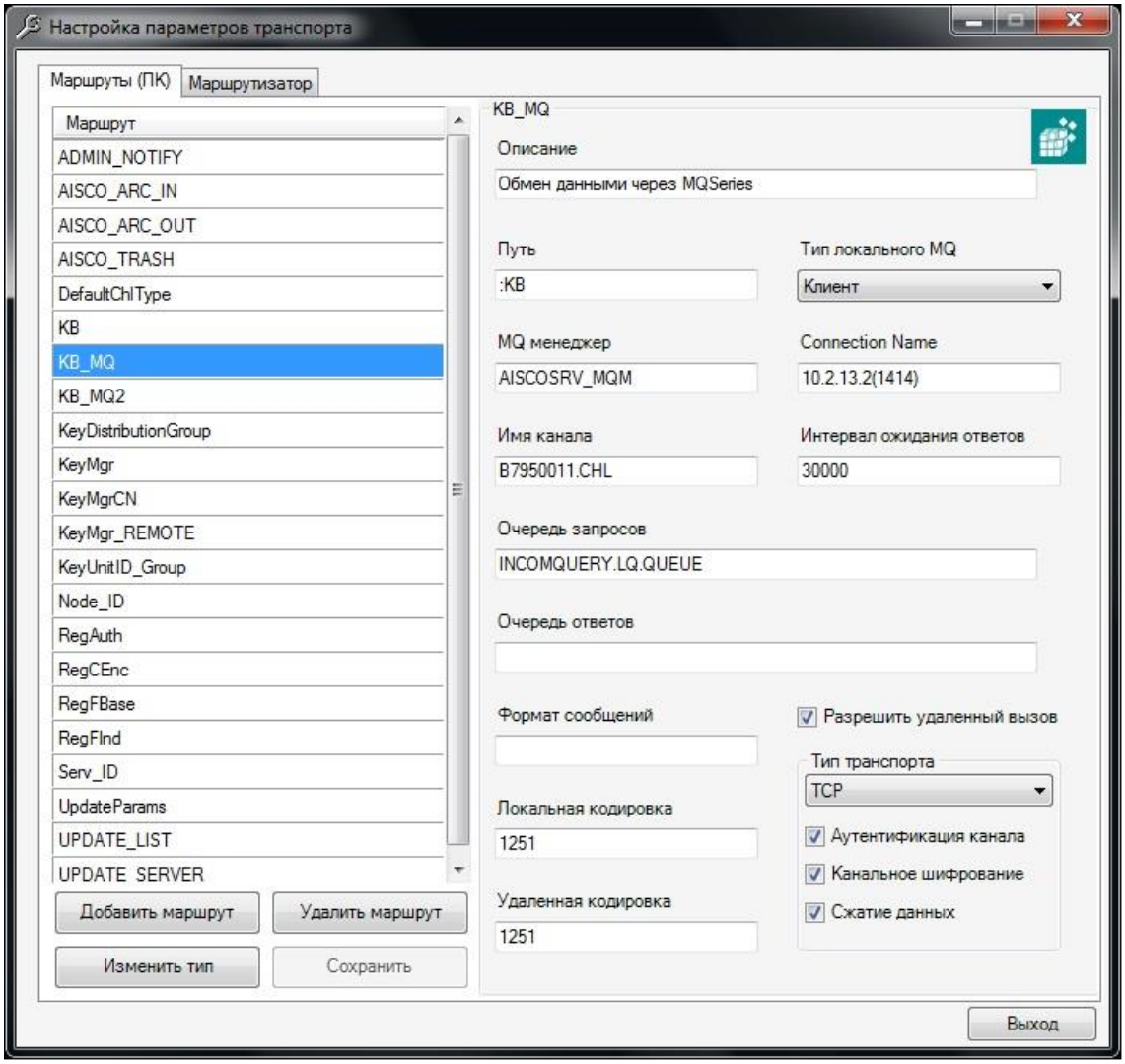

Рисунок 2

В соответствии с параметрами, указанными в маршруте KB_MQ#, выполняется передача данных по шифрованному каналу связи с аутентификацией

на выбранный сервер приложений АИС КР в очередь запросов и получение данных в динамически создаваемую клиентом временную очередь ответов (или в явно указанную очередь ответов). Передача сообщения осуществляется в режиме ожидания ответа с установленным интервалом ожидания ответов (это параметр WaitInterval в маршруте KB_MQ#, см. таблицу А.1 Приложения А).

Если в маршруте KB (см. таблицу А.1 Приложения А) задан параметр WaitRepete со значением неравным 0, то выполняются внутренние повторы (в DocSignc.dll) по истечении интервала ожидания ответов WaitInterval. Общее время ожидания с повторами установлено по умолчанию до 30 минут. Таким образом, клиентское приложение может получить ответ на запрос, время исполнения которого в базе Кредитного регистра больше гарантированного времени поддержания соединения MQ (установленного в KeepAlive для MQ) – больше 5 минут. Для выполнения повторов в пользовательском приложении обработки (без внутренних повторов) с применением опции GET_PREV_ANSWER – получение ответа на предыдущий запрос в ExecDataProc (см. описание в требованиях [2]) требуется удалить параметр WaitRepete.

На сервере приложений выполнение запросов производится обработчиком, установленном для обработки этой очереди запросов службой Router серверной части подсистемы информационного взаимодействия (устанавливается несколько копий службы для одной очереди для ускорения процесса обработки).

Помимо запроса (сообщения XML) в службу Router передаются параметры маршрута KB_MQ#, где в поле «Путь» указывается маршрут с параметрами для обработки на сервере приложений (:KB). Под управлением службы Router выполняются синтаксический контроль и проверка ЭЦП пользователя АИС КР, собственно выполнение запроса на сервере базы данных Кредитного регистра, формирование ответа формата XML, его синтаксический контроль и подписывание ключом ЭЦП сервера приложений АИС КР.

В результате выполнения запроса служба серверной части подсистемы информационного взаимодействия Router кладет сообщение ответа во временную динамическую очередь ответов (или в явно заданную очередь ответов);

4) **получение кода возврата** при получении ответа от сервера приложений или по истечении интервала ожидания ответов. Если код возврата имеет положительное значение, то это означает получение ответа от сервера приложений – сообщения формата XML. Если получен код возврата, имеющий отрицательное значение, то это означает, что ответ не получен по причине ошибки, и в этом случае обработчик завершает работу и возвращает полученный код, т.е. код ошибки;

5) **выполнение обработки ответа от сервера приложений**. Осуществляется синтаксический форматный контроль и проверка ЭЦП в соответствии с установленными опциями в маршруте KB для входящих сообщений. Если произошла ошибка при проверке, то ответ направляется по маршруту «Сохранение/обработка брака» (AISCO_TRASH), если такой маршрут установлен в маршруте KB. Если произошла ошибка в процессе обработки брака,

то обработчик завершает работу и возвращает код этой ошибки, если произошла ошибка контроля, или код ошибки проверки ЭЦП, если произошла ошибка при проверке ЭЦП;

6) **сохранение сообщения ответа**, прошедшего проверку, в архиве исходящих сообщений. Выполняется передача сообщения по маршруту «Сохранение в архив входящих сообщений» (AISCO_ARC_IN), если в маршруте КВ установлен такой маршрут. Если произошла ошибка при сохранении, то обработчик завершает работу и возвращает код этой ошибки.

Итак, в прикладную программу возвращается код завершения обработчика DocSignc.dll как возврат функции библиотеки базовых функций Basic.dll (ExecDataProc). Если код возврата имеет положительное значение, то это означает получение ответа – сообщения формата XML от сервера приложений АИК КР в буфере памяти, размер которого есть значение кода возврата.

Если получен код возврата, имеющий отрицательное значение, то это означает, что в буфере памяти нет данных ответа, и в данном случае код возврата – это код сообщения об ошибке. Коды ошибок, сообщения об ошибках и способ программного получения текстов сообщений приведены в разделе 4.

В процессе работы обработчика DocSignc.dll дополнительно осуществляется регистрация ошибок и причин их возникновения в журнал событий Windows «Приложение».

3 НАСТРОЙКА КЛИЕНТСКОЙ ЧАСТИ ПОДСИСТЕМЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Все необходимые параметры первоначально устанавливаются при инсталляции клиентской части подсистемы информационного взаимодействия (см. [1]). Изменять параметры после установки не требуется без явных причин.

Для настройки и просмотра параметров используется программа настройки таблицы маршрутизации TransportParam.exe. Подробное описание работы программы TransportParam.exe, типов маршрутов и их параметров приведено в [12]. Для запуска TransportParam.exe используется ярлык на рабочем столе «Настройка параметров транспорта».

Настройка клиентской части подсистемы информационного взаимодействия должна производиться под учетной записью администратора ОС (с повышением полномочий администратора).

Если в процессе выполнения операций (запросов) пользователь АИС КР получает сообщения об истечении интервала получения данных с сервера приложений, но при отсутствии проблем или ошибок связи, в том числе на сервере приложений, то в соответствующих настройках пользователь может увеличить интервал ожидания ответов и повторить выполняемую операцию (запрос). Настройка осуществляется с помощью программы TransportParam.exe в маршруте KB_MQ# (KB_MQ, KB_MQ2), соответствующем выбранному серверу приложений – для выполнения запросов XML (см. рисунок 2), а также в маршрутах KeyMgrCN и KeyMgr_REMOTE – для выполнения запросов базы открытых ключей.

Также в процессе работы может потребоваться смена типа устройства носителя ключа ЭЦП: в этом случае пользователь устанавливает требуемый **тип носителя**. Если нет необходимости сохранять успешно отправленные запросы и/или обработанные ответы, пользователь может **отключить сохранение сообщений**. Другие параметры для функционирования изменяются только по требованию службы сопровождения ОАО «БМРЦ». Эти настройки осуществляются с помощью программы TransportParam.exe в маршруте KB (см. рисунок 1).

Параметры клиентской части подсистемы информационного взаимодействия устанавливаются в реестре ОС. В основном используются комплекты параметров, так называемые маршруты, которые расположены в подразделах раздела реестра ОС HKLM\SOFTWARE\BTC. Описание маршрутов и их параметров приведено в Приложении А.

3.1 Настройка маршрутов для выполнения запросов

В процессе выполнения запросов к Кредитному регистру используются следующие маршруты:

– KB – основной маршрут, который определяет библиотеку для выполнения запросов при вызове функции Basic.dll (ExecDataProc), одним из параметров которой является данный маршрут;

– KB_MQ# (KB_MQ, KB_MQ2 и т.д.) – маршруты для дальнейшей обработки, которые определяют параметры обмена данными с каждым сервером приложений посредством IBM MQ;

– AISCO_ARC_IN – маршрут для сохранения входящих сообщений XML – ответов Кредитного регистра, который определяет путь сохранения файлов и библиотеку savefile.dll для сохранения файлов с уникальным именами;

– AISCO_ARC_OUT – маршрут для сохранения исходящих сообщений XML – запросов к Кредитному регистру, который определяет путь сохранения файлов и библиотеку savefile.dll для сохранения файлов с уникальным именами;

– AISCO_TRASH – маршрут для сохранения отбракованных входящих либо исходящих сообщений XML, который определяет путь сохранения файлов и библиотеку savefile.dll для сохранения файлов с уникальным именами.

Параметры маршрутов приведены в таблице А.1 Приложения А.

Маршрут KB определяет библиотеку обработки сообщений формата XML DocSignc.dll и ее параметры (см. окно программы TransportParam.exe на рисунке 1):

– опции для выполнения форматного контроля, вычисления и проверки ЭЦП исходящих и входящих сообщений (запросов и ответов);

– маршруты для сохранения исходящих сообщений (запросов) и входящих сообщений (ответов), маршрут для сохранения/обработки брака (запросов и ответов);

– маршрут для дальнейшей обработки, используемый для передачи запроса для выполнения на сервер приложений АИС КР;

– тип используемого носителя ключа ЭЦП.

Из параметров может изменяться пользователем тип носителя ключа ЭЦП при смене типа носителя после установки. Кроме того, пользователь может не устанавливать опции сохранения в архивные каталоги, если это не требуется, например, в случае, когда собственное ПО обеспечивает сохранение в архивные каталоги.

При переходе на работу с другим сервером приложений соответствующий маршрут для дальнейшей обработки KB_MQ# (KB_MQ или KB_MQ2) автоматически (без участия пользователя) корректируется программой настройки параметров подключения к серверу приложений (см. 3.7).

Опции для форматного контроля, выработки и проверки ЭЦП отменяются только в случае выполнения тестирования (по требованию службы сопровождения или разработчика ОАО «БМРЦ»).

В случае необходимости изменения расположения архивного каталога в маршрутах AISCO_ARC_IN, AISCO_ARC_OUT или AISCO_TRASH значение нового пути задается в параметре Path непосредственно в реестре ОС (в

стандартной программе Windows regedit.exe). Для этих маршрутов можно установить собственную библиотеку обработки (библиотеку-плагин Basic.dll) или изменить тип маршрута.

В маршрутах KB_MQ и KB_MQ2 описывается способ обмена данными с серверами приложений АИС КР посредством IBM MQ (см. рисунок 2). Пользователь в случае получения сообщений об истечении интервала ожидания получения данных (при отсутствии сбоев или ошибок связи) может увеличить интервал ожидания ответов. Рекомендуется устанавливать интервал в пределах от 30000 до 180000 миллисекунд (300000 – это предельно допустимое значение).

Опции для аутентификации и шифрования канала в маршрутах KB_MQ и KB_MQ2 снимаются совместно с установкой соответствующих опций для канала на соответствующем сервере приложений в случае выполнения тестирования. Другие параметры маршрутов KB_MQ и KB_MQ2 корректировать не разрешается.

3.2 Настройка маршрутов средств ЭЦП и комплекса управления ключами СКЗИ

Комплекс управления ключами СКЗИ и средства ЭЦП используют следующие маршруты:

– KeyMgr – маршрут для обращения к локальной базе сертификатов открытых ключей СКЗИ, используемый при проверке ЭЦП (в DocSignc.dll);

– KeyMgrCN – маршрут для обращения к центральному хранилищу ключевой информации СКЗИ, расположенному в ОАО «БМРЦ» на центральном узле системы передачи финансовой информации АС МБР. Используется для отправки заявок на создание и отзыв ключей ЭЦП в программе регистрации ключей СКЗИ. Взаимодействие клиента АИС КР с центральным хранилищем ключей СКЗИ осуществляется через сервер приложений АИС КР;

– KeyMgr_REMOTE – маршрут для обращения к базе сертификатов открытых ключей СКЗИ сервера приложений. Используется для актуализации локальной базы сертификатов открытых ключей СКЗИ в программе регистрации ключей СКЗИ;

– KeyDistributionGroup – номер списка рассылки ключевой информации (значение 2), который включается в заявки на создание ключей ЭЦП в программе регистрации ключей СКЗИ, используемый для рассылки ключевой информации из центрального хранилища для АИС КР;

– KeyUnitID_Group – трехзначный идентификатор группы ключей ЭЦП, используемый при идентификации ключей ЭЦП (пятизначный идентификатор) в процессе создания заявок на создание ключей ЭЦП пользователей и для получения ключей своей группы при актуализации локальной базы сертификатов открытых ключей СКЗИ (см. 3.6).

Маршруты комплекса управления ключами СКЗИ и средств ЭЦП и их параметры приведены в таблице А.2 Приложения А.

Если при отправке заявок для создания ключей ЭЦП или актуализации локальной базы сертификатов открытых ключей СКЗИ (см. 3.6) выдаются сообщения об истечении интервала ожидания получения данных (при отсутствии сбоев или ошибок связи), то пользователь может увеличить интервал ожидания ответов в маршрутах KeyMgr_REMOTE и KeyMgrCN и повторить операцию. Рекомендуется устанавливать интервал в пределах от 30000 до 180000 миллисекунд (300000 – это предельно допустимое значение).

Для перехода на работу с другим сервером приложений АИС КР маршруты KeyMgrCN и KeyMgr_REMOTE автоматически (без участия пользователя) корректируются программой настройки параметров подключения к серверу приложений (см. 3.7). Опции для аутентификации и/или шифрования канала в этих маршрутах отменяются только в случае выполнения тестирования (по требованию службы сопровождения или разработчика ОАО «БМРЦ»), причем, в канале на стороне сервера приложений должны быть установлены соответствующие опции.

3.3 Настройка маршрутов комплекса получения обновлений ППО

Программные средства комплекса получения обновлений ППО используют следующие маршруты:

– UPDATE_LIST – маршрут, определяющий список версий установленного ПО АИС КР (в подразделах это раздела реестра ОС, т.е. маршрута), необходимый для формирования запросов на получение обновлений ППО, с указанием библиотеки выполнения запросов;

– UPDATE_SERVER – маршрут для получения файлов обновлений ППО с сервера приложений АИС КР;

– UpdateParams – маршрут, в котором устанавливаются параметры для получения обновлений ППО, используемые для службы автоматического обновления ППО (Applications Update Service).

Маршруты комплекса получения обновлений ППО и их параметры приведены в таблице А.3 Приложения А.

Также для формирования запроса к серверу приложений используется маршрут комплекса защиты соединений MQSeries:

– NODE_ID – маршрут, определяющий идентификатор узла-клиента АИС КР этого рабочего места (см. таблицу А.4 Приложения А).

Если при получении обновлений ППО выдаются сообщения об истечении интервала ожидания получения данных (при отсутствии сбоев или ошибок связи), то пользователь может увеличить интервал ожидания ответов в маршруте UPDATE_SERVER и повторить запрос (с помощью программы загрузки обновлений). Рекомендуется устанавливать интервал в пределах от 30000 до 180000 миллисекунд (300000 – это предельно допустимое значение).

Для установки параметров в маршруте UpdateParams используется программа настройки параметров автоматического обновления UpdateParams.exe. Программа позволяет настроить режим запуска службы (при загрузке ОС

Windows, либо по времени), а также режимы работы: получать только уведомления о наличии новых обновлений на сервере приложений или автоматически получать файлы обновлений в заданный каталог. Подробное описание комплекса получения обновлений ППО приведено в [13].

3.4 Настройка маршрутов комплекса защиты соединений MQSeries

Программные средства комплекса защиты соединений MQSeries используют следующие маршруты:

– ADMIN_NOTIFY – маршрут, в котором определены режимы отображения и протоколирования сообщений об ошибках средств комплекса защиты соединений при работе канала MQ;

– DefaultChlType – маршрут установки типа канала. Значение DefChlType по ссылке в Path должно быть установлено равным «2», что означает тип канала «Client», и в программе регистрации каналов будет выбираться первым тип канала «Client»;

– Node_ID – маршрут, определяющий идентификатор рабочего места – узла для аутентификации сторон в АИС КР;

– RegAuth – маршрут, определяющий расположение локальной библиотеки функций программы регистрации каналов RegAuth.dll;

– NodeType – маршрут, определяющий тип узла и набор операций в программе регистрации каналов. Для узла-клиента АИС КР задается значение «0» – конечный узел (если маршрут отсутствует, принимается значение «0»);

– RegCEnc – маршрут, определяющий путь к файлу channel.enc с аутентификационными данными канала, используемый при регистрации канала в программе регистрации каналов;

– RegFBase – маршрут, определяющий путь к разделу реестра ОС, содержащему подраздел C# (где # – порядковый номер канала) с аутентификационными данными канала в параметре «(По умолчанию)», используемый в программе регистрации каналов и модулем аутентификации каналов;

– RegFInd – маршрут, определяющий путь к разделу реестра ОС – IND, содержащему параметр «(По умолчанию)» со списком зарегистрированных каналов, используемый в программе регистрации каналов и модулем аутентификации каналов;

– Serv_ID – маршрут, определяющий идентификатор выбранного сервера приложений АИС КР, т.е. установленного активным. Идентификатор меняется автоматически при выборе сервера приложений.

Маршруты комплекса защиты соединений MQSeries и их параметры приведены в таблице А.4 Приложения А. Подробное описание комплекса защиты соединений MQSeries приведено в [6], описание программы регистрации каналов приведено в [7].

Пользователь, при необходимости, может снять в маршруте ADMIN_NOTIFY режим «Показывать сообщения» и, в этом случае, установить режим «Сохранять сообщения в журнал событий» (в окне программы TransportParam.exe). Снимать оба режима не разрешается.

До выполнения операции регистрации каналов в программе регистрации каналов пользователь может проверить или установить при необходимости новый путь размещения регистрационного файла канала channel.enc в маршруте RegCEnc.

3.5 Аутентификация каналов. Регистрация и синхронизация

Для соединения с сервером приложения АИС КР используется аутентифицируемый канал связи, при каждом запуске которого осуществляется взаимная проверка подлинности сторон. В процессе аутентификации также контролируется последовательность соединений между двумя узлами – клиентом и сервером приложений АИС КР.

Режимы аутентификации и канального шифрования (с опцией сжатия) указываются в настройках маршрутов KB_MQ (KB_MQ2 и т.д.), KeyMgrCN и KeyMgr_REMOTE (см. Приложение А). Режимы задаются в соответствии с устанавливаемыми режимами на стороне соответствующего сервера приложений АИС КР в настройках канала для клиента АИС КР. Функцию аутентификации выполняет программа выхода security exit (CSQAUTH.dll), функцию канального шифрования (с опцией сжатия) – программа выхода send/receive exit (CSQCPHR.dll).

В процессе установки клиентской части информационного взаимодействия АИС КР выполняется регистрация канала для каждого сервера приложений, т.е. в настройки реестра ОС записываются ключевые данные для модуля аутентификации каналов из регистрационных файлов каналов channel.enc (см. [1]). Затем для каналов выполняется операция синхронизации, т.е. установка начального значения счетчика последовательности соединений.

После этого при каждом запуске канала выполняется процедура аутентификации – взаимное подтверждение сторон, и канал стартует. Однако в силу ряда причин может произойти нарушение аутентификации канала и потребуется выполнить действия для восстановления его работы. Нарушение аутентификации канала связи возможно в случаях:

– при установлении предыдущего соединения с сервером приложений АИС КР произошел сетевой или программный сбой. Например, если при неожиданном завершении работы ОС, когда канал мог в это время соединяться, не происходит сохранение счетчика последовательности соединений, то при следующем старте канала происходит нарушение аутентификации;

– при установлении предыдущего соединения с сервером приложений АИС КР другого компьютера, с неверными регистрационными данными канала. Например, рабочее место клиента уже было установлено ранее на другом компьютере и не было удалено ПО или, например, подключение выполнялось с

предыдущей копии (snapshot) текущего клиента АИС КР (а создавать копии не следует). Также возможен случай подключения злоумышленника, пытающегося выдать себя за клиентское место АИС КР;

– на другой стороне находится злоумышленник, пытающийся выдать себя за сервер приложений АИС КР.

Нарушение аутентификации, как правило, обнаруживает сервер приложений АИС КР. При этом на стороне клиента АИС КР программные приложения клиентской части подсистемы информационного взаимодействия выдают сообщение об ошибке 0xE8020109 «Нарушение аутентификации. В соединении с сервером отказано», а модуль аутентификации каналов CSQAUTH.dll выдает ошибку 0xE8090033 «Ошибка аутентификации на противоположной стороне канала (мьютекс освобожден в term)» в журнал событий Windows «Приложение». На сервере приложений АИС КР фиксируются ошибки модуля аутентификации каналов CSQAUTH.dll: ошибка 0xE8090028 «Получен неверный пакет. Имитовставки не сравнились» и, затем, повторяющиеся ошибки 0xE8090027 «Канал заблокирован программой выхода» при каждом старте канала, – т.е. после нарушения аутентификации сервер приложений блокирует все дальнейшие попытки соединения.

Канал также может останавливаться по причинам возникновения других ошибок модуля аутентификации или канального шифрования (см. описание ошибок в разделе 4) на одной из сторон, при этом блокировка канала не производится.

В случае неработоспособности канала, получения сообщений об ошибке 0xE8020109 «Нарушение аутентификации. В соединении с сервером отказано», других ошибок модуля аутентификации и канального шифрования (фиксируются в журнале событий Windows «Приложение») следует обращаться к администратору безопасности ОАО «БМРЦ». Администратором безопасности ОАО «БМРЦ» проводится анализ ситуации и выполняются совместные действия по восстановлению работы канала. В случае невозможности определить причину и восстановить работу канала следует обращаться в службу сопровождения ОАО «БМРЦ» (либо к разработчику ОАО «БМРЦ»).

Особое внимание следует обратить на то, что если в случае неработоспособности канала не было явных проблем на стороне клиента и сообщений об ошибках, то причиной может быть проблема нарушения безопасности. Возможно, существует выполняющий несанкционированные попытки подключения к Кредитному регистру с идентификационными данными клиента другой компьютер, который подключается до работы клиента АИС КР, что привело к блокировке канала на сервере приложений. В этих случаях следует незамедлительно уведомить собственную службу безопасности и сетевого администратора (в организации Участника).

Если канал был заблокирован на стороне сервера приложений АИС КР, то после устранения обнаруженных проблем совместно с администратором

безопасности ОАО «БМРЦ» выполняется синхронизация канала, а со стороны сервера приложений и разблокировка канала.

Синхронизация канала производится с помощью программы регистрации каналов RegAuth.exe, ярлык для запуска которой расположен на рабочем столе и имеет наименование «Мастер регистрации каналов», описание программы приведено в [7]. Окно программы RegAuth.exe приведено на рисунке 3. При синхронизации используется пароль, который сообщает администратор безопасности ОАО «БМРЦ». При успешном выполнении синхронизации каналов на экран выводится сообщение «Для канала Client узла AISCOSR* сброшен флаг синхронизации».

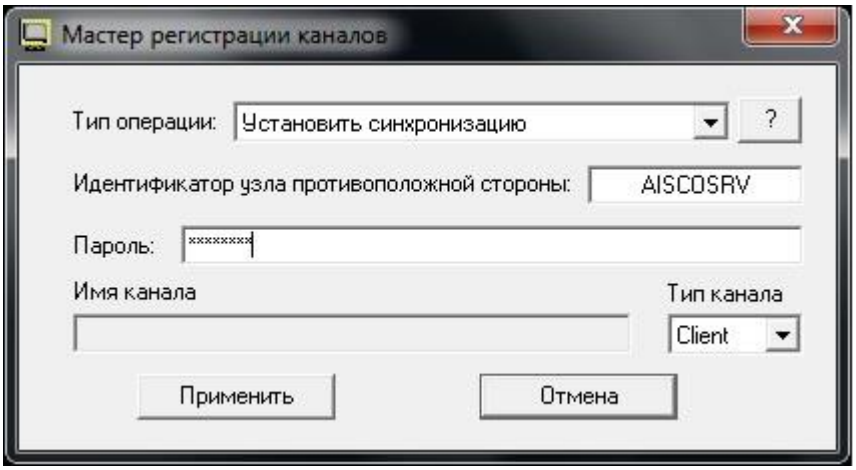

Рисунок 3

Другие операции, кроме синхронизации канала, выполняемой совместно с администратором безопасности ОАО «БМРЦ», в программе регистрации каналов RegAuth.exe в штатном режиме выполнять не требуется. В случае переустановки клиентской части информационного взаимодействия АИС КР или смены компьютера следует выполнять действия, описанные в [1].

3.6 Управление ключами ЭЦП

3.6.1 Общее описание

Для вычисления ЭЦП запросов к Кредитному регистру используются личные ключи ЭЦП пользователей АИС КР, записанные на внешние носители ключа – eToken Pro или iKey 1000/1032 (либо в память компьютера – в реестр ОС). Генерация личных ключей ЭЦП и запись на внешний носитель производится непосредственно на рабочем месте пользователя АИС КР.

При создании электронной заявки в программе RegCenter.exe, ярлык для запуска которой расположен на рабочем столе и имеет наименование «Программа регистрации ключей СКЗИ», для ключа ЭЦП нового пользователя администратором безопасности ОАО «БМРЦ» назначается уникальный регистрационный номер ключа СКЗИ – пятизначный номер, где первые три

символа – регистрационный номер группы ключей для этого рабочего места клиента АИС КР, следующие два символа – идентификатор пользователя – владельца ключа. Для регистрационных номеров ключей СКЗИ определяются права на выполнение запросов к Кредитному регистру.

Электронная заявка поступает в ОАО «БМРЦ» для регистрации в центральном хранилище сертификатов открытых ключей СКЗИ. На основании электронной заявки администратор безопасности ОАО «БМРЦ» предоставляет пользователю (по почте, нарочным и т.п.) карточки открытого ключа проверки ЭЦП (2 экз.) для оформления. После получения оформленной карточки от пользователя (по почте, нарочным и т.п.) администратор безопасности ОАО «БМРЦ» регистрирует заявку. В процессе регистрации издается сертификат открытого ключа, который рассылается на серверы приложений АИС КР. Пользователь АИС КР запрашивает локальную базу сертификатов открытых ключей СКЗИ с сервера приложений, т.е. актуализирует базу, получая новый сертификат с уникальным 32-символьным серийным номером, и записывает на носитель ЭЦП этот серийный номер сертификата (связывает личный ключ с открытым). После этого ключ ЭЦП, записанный на носителе, готов к использованию.

По мере истечения срока действия сертификата открытого ключа ЭЦП либо в случае смены пользователя – владельца ключа, а также в связи с компрометацией ключа создается электронная заявка для смены ключа, при этом выпускается новый сертификат открытого ключа с уникальным серийным номером, регистрационный номер ключа СКЗИ при этом не изменяется. Серийный номер сертификата идентифицирует ЭЦП в запросе к Кредитному регистру.

При отсутствии необходимости использования ключа ЭЦП или при отключении от АИС КР Участником Кредитного регистра оформляется заявка на удаление ключей СКЗИ (см. [11]). Электронный запрос на отзыв ключа ЭЦП выполняет либо пользователь АИС КР в программе RegCenter.exe, либо администратор безопасности ОАО «БМРЦ». Освободившийся регистрационный номер ключа может быть присвоен другому пользователю.

На рисунке 4 представлен вид главного окна программы RegCenter.exe.

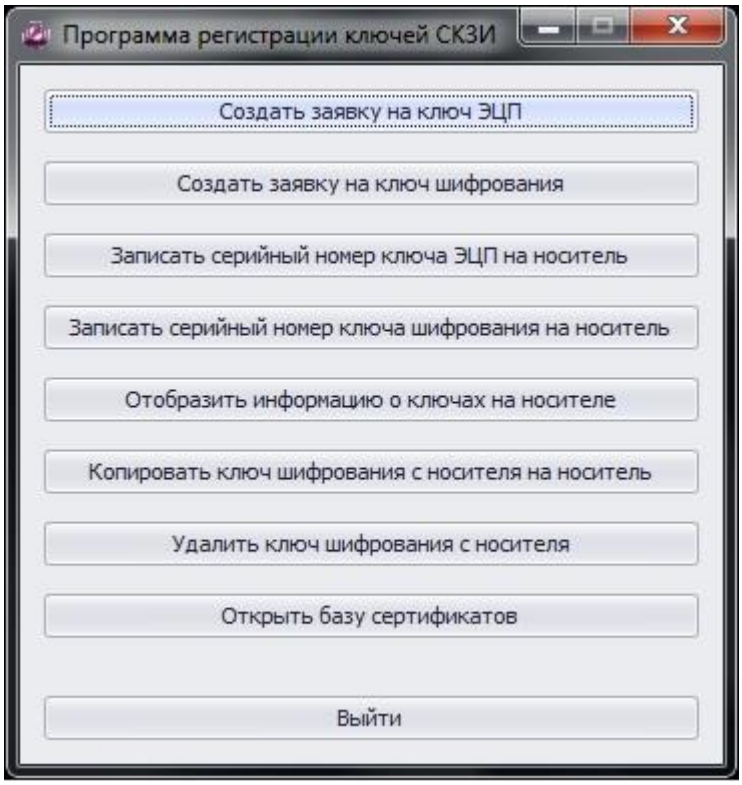

Рисунок 4

На рабочем месте пользователя АИС КР используются следующие кнопки главного окна программы RegCenter.exe:

– «Создать заявку на ключ ЭЦП». Осуществляется генерация ключа ЭЦП при создании нового ключа либо при смене ключа, т. е. генерация пары ключей – личного и открытого ключа. Личный ключ ЭЦП с нулевым номером сертификата записывается на носитель пользователя, а открытый, с информацией о владельце ключа, в форме электронной заявки (формата XML) поступает на сервер приложений АИС КР и, далее, в центральное хранилище сертификатов открытых ключей ОАО «БМРЦ»;

– «Записать серийный номер ключа ЭЦП на носитель». На носитель с новым личным ключом ЭЦП записывается регистрационный номер сертификата соответствующего открытого ключа. Используется после передачи оформленной карточки открытого ключа проверки ЭЦП в ОАО «БМРЦ» и выполнения актуализации локальной базы сертификатов открытых ключей СКЗИ (по кнопке «Открыть базу сертификатов», операция «Актуализировать базу»);

– «Отобразить информацию о ключах на носителе». Используется при необходимости удостовериться в соответствии личного ключа ЭЦП на носителе открытому ключу из локальной базы сертификатов и для получения идентификационной информации и сведений о владельце ключа;

– «Открыть базу сертификатов». Осуществляется просмотр локальной базы сертификатов открытых ключей СКЗИ, включающей записи сертификатов открытых ключей ЭЦП серверов приложений АИС КР и всех открытых ключей ЭЦП группы пользователей СКЗИ, установленной в настройках для данного

рабочего места. При необходимости выполняются операции «Актуализировать базу» для получения локальной базы сертификатов открытых ключей СКЗИ с сервера приложений АИС КР и «Отозвать сертификат» для удаления открытого ключа ЭЦП пользователя из базы сертификатов открытых ключей на серверах приложений АИС КР.

В случае необходимости создания нового ключа ЭЦП для пользователя, продления срока его действия, смены владельца ключа (смены в связи с компрометацией ключа) необходимо создать соответствующую заявку на ключ ЭЦП, выполнив операции в программе регистрации ключей СКЗИ RegCenter.exe, изложенные в [10]. Сначала выполняются действия по кнопке «Создать заявку на ключ ЭЦП», затем после уведомления администратора безопасности ОАО «БМРЦ» о регистрации заявки по кнопке «Открыть базу сертификатов» выполняется операция «Актуализировать базу», после чего выполняется операция по кнопке «Записать серийный номер ключа ЭЦП на носитель».

3.6.2 Актуализация локальной базы сертификатов открытых ключей СКЗИ

Получение локальной базы сертификатов открытых ключей СКЗИ с сервера приложений АИС КР, т.е. актуализация базы, выполняется в обязательном порядке при подключении нового рабочего места клиента АИС КР. В состав локальной базы сертификатов открытых ключей СКЗИ первоначально входят записи сертификатов открытых ключей ЭЦП серверов приложений АИС КР, необходимые для выполнения проверки ЭЦП ответов Кредитного регистра.

Актуализация локальной базы ключей также выполняется для проверки соединения (взаимодействия) с серверами приложений АИС КР в случае восстановления работы каналов MQ после сбоев либо после переустановки ПО.

Для получения локальной базы сертификатов открытых ключей СКЗИ необходимо воспользоваться программой регистрации ключей СКЗИ RegCenter.exe (см. рисунок 4) и выполнить по кнопке «Открыть базу сертификатов» операцию «Актуализировать базу» (см. рисунок 5). Производится удаление всех записей текущей базы и занесение полученной выборки сертификатов из сервера приложений АИС КР, который на данный момент установлен для работы (установлен активным). В состав выборки включаются сертификаты открытых ключей ЭЦП серверов приложений АИС КР (группа SKB) и всех открытых ключей ЭЦП группы пользователей СКЗИ.

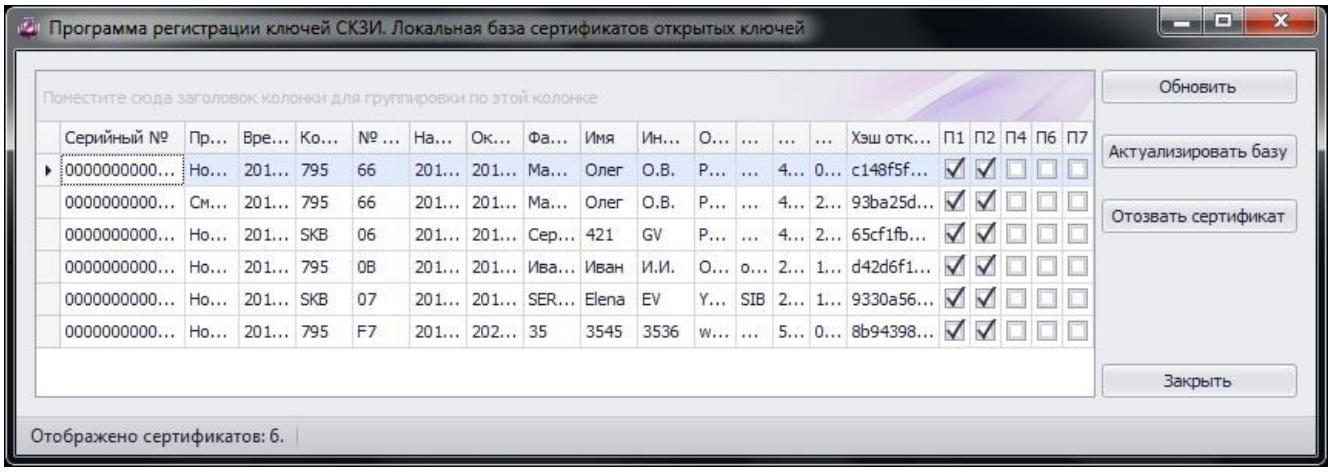

Рисунок 5

3.6.3 Переустановка службы HKService.exe

Если в процессе функционирования ПО АИС КР возникают проблемы при работе с ключами ЭЦП и выдается ошибка 0xE850000D «Ошибка работы со службой защиты ключей», то требуется переустановить службу защищенного хранения данных для доступа к ключам СКЗИ на носителях HKService.exe. Требуется, с правами администратора ОС (с повышением привилегий администратора), выполнить следующие действия:

1) остановить службу HKService. Открыть консоль services.msc (или в контекстном меню, вызванном по правой кнопке мыши на ярлыке «Компьютер», выбрать «Управление» затем «Службы и приложения» -> «Службы») и остановить службу HKService, если она была в рабочем состоянии. Закрыть окно консоли;

2) удалить службу HKService.exe, выполнив команду из командной строки (например, в Total Commander):

HKService.exe –unregserver

3) зарегистрировать службу HKService.exe, выполнив команду:

HKService -service

4) убедиться, что служба HKService.exe зарегистрирована. Заново открыть окно консоли services.msc. Стартовать службу HKService.exe вручную не требуется;

5) перезапустить выполняемую прикладную программу.

3.7 Настройка взаимодействия с одним из серверов приложений АИС КР

Программа настройки параметров подключения к серверу приложений АИС КР SetAISCOServer.exe, ярлык для запуска которой расположен на рабочем столе и имеет наименование «Настройка параметров подключения к серверу приложений», используется для выбора активного сервера приложений АИС КР,

т.е. того сервера, с которым будут взаимодействовать все прикладные программы клиента АИС КР. Программа SetAISCOServer.exe выполняет следующие функции:

– создание параметров подключения к серверу приложений АИС КР (добавление сервера);

– изменение параметров подключения к серверу приложений АИС КР;

– удаление параметров подключения к серверу приложений АИС КР (удаление сервера);

– установка активного сервера приложений АИС КР.

ВНИМАНИЕ! Для создания или изменения параметров подключения к серверу приложений АИС КР требуется выполнять программу с правами администратора ОС.

Для первоначального запуска программы должен существовать раздел реестра ОС HKLM\SOFTWARE\BTC\Router\KB_MQ с эталонными параметрами подключения к серверу приложений.

Параметры подключения к серверу приложений хранятся в разделах реестра ОС HKLM\SOFTWARE\BTC\Router\KB_MQ#, где # – порядковый номер сервера приложений (для основного отсутствует). При создании подключения к новому серверу приложений АИС КР параметры подключения создаются на основании параметров подключения к эталонному серверу.

В левой части главного окна программы (см. рисунок 6) отображается список серверов (т.е. серверов приложений АИС КР). Звездочкой помечается активный сервер. Список серверов всегда содержит хотя бы один сервер – эталонный (его настройки находятся в маршруте KB_MQ). При выборе конкретного сервера приложений в правой части окна отображаются параметры подключения: имя менеджера MQ, IP-адрес (порт) сервера приложений и имя канала.

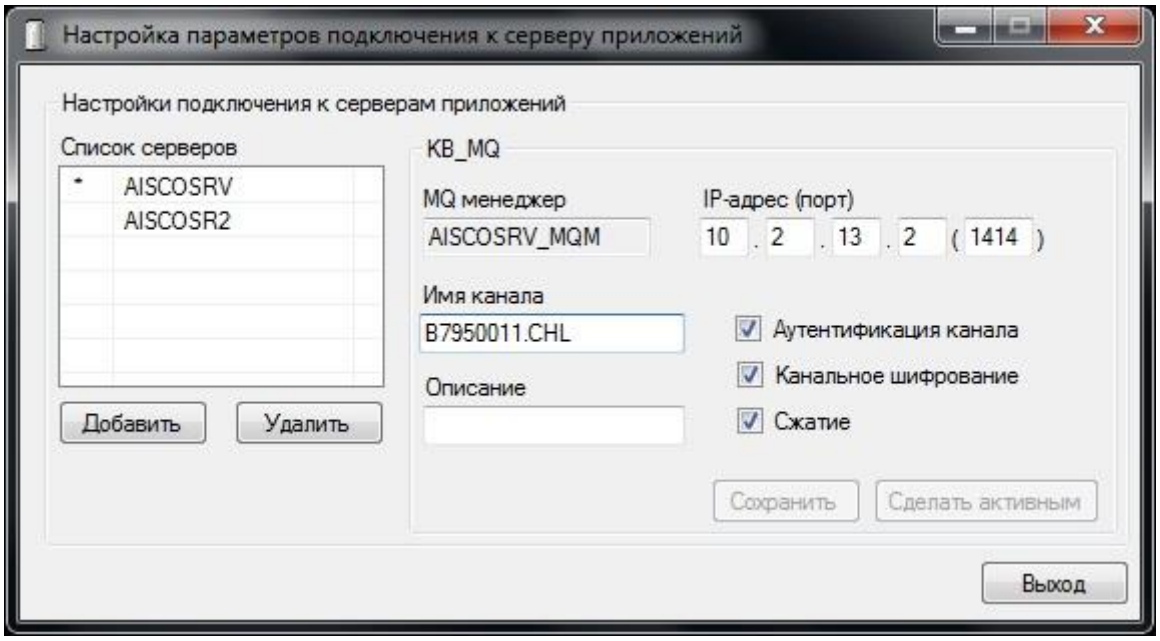

Рисунок 6

3.7.1 Создание параметров подключения к серверу приложений

Чтобы настроить параметры подключения к новому серверу приложений АИС КР, необходимо нажать кнопку «Добавить» или выбрать пункт «Добавить» контекстного меню в окне списка серверов. В появившемся диалоге (см. рисунок 7) ввести порядковый номер и IP-адрес сервера приложений. Поля являются обязательными для заполнения.

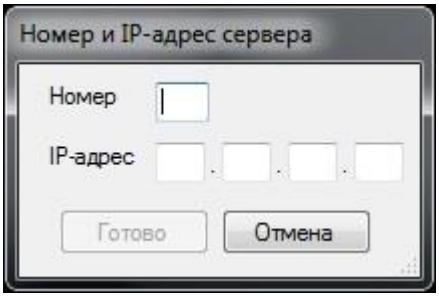

Рисунок 7

После нажатия кнопки «ОК» в списке серверов появится строка с названием сервера. В правой части основного окна программы отобразятся

параметры подключения к серверу. При необходимости параметры подключения к серверу можно отредактировать и сохранить.

3.7.2 Установка активного подключения

Для установки активного подключения к серверу приложений следует выбрать нужный сервер в списке серверов и нажать кнопку «Сделать активным» в правой части окна (см. рисунок 6). В случае успешной установки программа выдаст сообщение «Установлен сервер <*имя_сервера*>» и возле имени сервера в левой части окна появится звездочка.

Перед выполнением данной операции рекомендуется закрыть все работающие прикладные программы, взаимодействующие с АИС КР. После повторного запуска прикладные программы будут взаимодействовать с АИС КР через установленный сервер приложений, т.е. активный.

3.7.3 Изменение настроек подключения к серверу приложений

Для того чтобы внести изменения в параметры подключения к серверу приложений АИС КР, следует выбрать нужный сервер в списке серверов, в правой части окна внести в поля необходимые изменения и затем нажать кнопку «Сохранить» или выбрать пункт «Сохранить» контекстного меню в окне списка серверов (см. рисунок 6).

Если параметры подключения были изменены и не сохранены, то при выборе другого сервера или выходе из программы появится запрос на сохранение параметров подключения.

3.7.4 Удаление параметров подключения к серверу приложений

Для удаления параметров подключения к серверу приложений необходимо нажать кнопку «Удалить» или выбрать пункт «Удалить» контекстного меню в окне списка серверов. Появится запрос на подтверждение удаления. Нельзя удалить настройки подключения к эталонному серверу (AISCOSRV, его настройки находятся в маршруте KB_MQ) и активному серверу, о чем программа выдаст соответствующие сообщения.

4 СООБЩЕНИЯ И КОДЫ

Различные функции программных модулей (библиотек) клиентской части подсистемы информационного взаимодействия АИС КР возвращают четырехбайтовые значения – коды сообщений либо размер данных (положительное число) или признак успешного выполнения (значение 0).

Для получения информации о событии, идентифицированном кодом сообщения, используется шестнадцатеричное представление кода сообщения 0xTCCC####, где:

– первая цифра (T) – тип сообщения: 2 – успех; 6 – информация; A – предупреждение; E – ошибка;

– следующие три цифры (CCC) – категория сообщения, которая определяет источник – программный модуль (библиотеку) (например, 803 – категория библиотеки Basic.dll);

– четыре последние цифры (####) – номер сообщения в данной категории.

В десятичном представлении отрицательное значение кода сообщения означает, таким образом, получение ошибки либо предупреждения (T = E или A).

Коды сообщений программных модулей клиентской части подсистемы информационного взаимодействия, тексты сообщений и источники сообщений (по категориям), а также описание действий по устранению ошибок и проблем приведены в [14], сообщения категории 809 для модулей аутентификации каналов и канального шифрования MQSeries – в [6], сообщения категории 80A для программы регистрации каналов – в [7].

В случае получения неизвестных кодов ошибок или программных исключений (Application Error) следует обращаться в службу сопровождения ОАО «БМРЦ» (либо к разработчику ОАО «БМРЦ»).

В случае невозможности устранить ошибки самостоятельно, выполняя действия в соответствии с документацией, следует обращаться в службу сопровождения ОАО «БМРЦ».

Для преобразования кода сообщения, полученного в десятичном представлении, в шестнадцатеричное представление рекомендуется использовать стандартный калькулятор Windows (для программиста). Например, при преобразовании десятичного числа -397344765 будет получено шестнадцатеричное число FFFFFFFFE8510003, из которого требуется выбрать последние восемь цифр. Полученный код сообщения E8510003 относится к категории 851 «Сообщения об ошибках по стандарту PKCS11 v.2.01», выдаваемой из библиотеки работы с носителем (FDT_et.dll или FDT_ik.dll), и соответствует сообщению «Неверно указан номер слота».

В случае интегрирования клиентской части подсистемы информационного взаимодействия в ПО клиента АИС КР для получения текста сообщения и описания источника/категории по коду сообщения используются функции поставляемой библиотеки менеджера сообщений MsgMgr.dll. Описание использования предоставляемого интерфейса приведено в [2].

Программные модули клиентской части подсистемы информационного взаимодействия АИС КР помимо возврата кодов сообщений в вызывающие прикладные программы регистрируют собственные сообщения о событиях и ошибках в журнале событий Windows «Приложение».

4.1 Наиболее часто получаемые коды сообщений об ошибках при выполнении запросов

Наиболее часто получаемыми кодами сообщений об ошибках (в том числе предупреждения) при выполнении запросов к Кредитному регистру являются следующие коды:

– 0xE806#### (0xA806####) – ошибки обработки сообщений АИС КР – это ошибки форматного контроля, вычисления либо проверки ЭЦП. Источником ошибок является библиотека DocSignc.dll или DocSigns.dll, функционирующая на сервере приложений АИС КР, коды возврата которой передаются на сторону клиента. При возникновении ошибок данной категории запрос или ответ на запрос бракуется – направляется по маршруту сохранения в архивный каталог брака;

– 0xE802#### (0xA802####) – ошибки средств работы с IBM MQ. Источником ошибок является библиотека MQBasec.dll или MQBases.dll, функционирующая на сервере приложений АИС КР, коды возврата которой передаются на сторону клиента. Из ошибок данной категории наиболее часто получаемыми являются ошибки:

– 0xE8020101 «Ошибка подключения к менеджеру очередей MQSeries». Данная ошибка означает отсутствие связи с менеджером MQ на сервере приложений, причиной которой может быть отсутствие физической связи, отсутствие собственно канала (не был создан), неверные имена менеджера MQ, соединения, очередей в настройках маршрутов в реестре ОС;

– 0xE8020109 «Нарушение аутентификации. В соединении с сервером отказано». В этом случае требуется определить причину возникновения ошибки, т.е. получить информацию об ошибке модуля аутентификации каналов (модуля шифрования) категории 809, выдаваемую на экран и/или в журнал событий Windows «Приложение»;

– 0xE803#### (0xA803####) – ошибки транспортной подсистемы защищенного взаимодействия. Источником ошибок является библиотека Basic.dll, функционирующая как на стороне клиента, так и на сервере приложений АИС КР, коды возврата которой передаются на сторону клиента. Как правило, это неожиданные программные сбои («перехваченные» исключения), а также сбои, полученные вследствие некорректных настроек, некорректных входных данных, отсутствия необходимых ресурсов. Особое внимание следует уделить предупреждению:

– 0xA8033304 «Истек интервал ожидания получения результата обработки данных». Возникновение данного предупреждения означает

неопределенную ситуацию, когда за отведенный промежуток времени ответа на запрос получено не было, и состояние его обработки неизвестно.
После получения этого кода и при отсутствии сбоев или ошибок связи рекомендуется увеличить интервал ожидания ответов WaitInterval в маршруте КВ_MQ# (см. таблицу А.1 Приложения А) и повторить операцию.
Код 0xA8033304 возвращается при условии, когда не заданы внутренние повторы в параметре WaitRepete в маршруте КВ. Установите признак для внутренних повторов WaitRepete и повторите выполнение запроса. Если запрос не будет выполнен и в этом случае, то будет возвращен код ошибки 0xA8060308 «истек интервал ожидания получения результата обработки данных (заданы внутренние повторы)». Либо для повторного получения ответа реализуйте вызов ExecDataProc с опцией GET_PREV_ANSWER (см. [2]). В этом случае не требуется выполнять повторение запроса, требуется перестроить или разделить его.
В случае невозможности устранить проблему следует обратиться в службу сопровождения ОАО «БМРЦ» (либо к разработчику ОАО «БМРЦ»);

– 0xE850#### (0xA850####), 0xE851#### (0xA851####) – ошибки при работе с носителями ключа ЭЦП. Источником ошибок является одна из библиотек: FDT_et.dll, FDT_ik.dll (FDT_mem.dll). Как правило, ошибки связаны с отсутствием драйвера устройства, неверно установленного типа устройства либо недоступности носителя ключа. Конкретное описание действий при возникновении ошибки 0xE850000D приведено в 3.6.3.

4.2 Сообщения об ошибках аутентификации каналов и канального шифрования

В процессе выполнения запросов к Кредитному регистру, а также при выполнении операций управления ключами СКЗИ и запросов обновлений ППО взаимодействие с сервером приложений АИС КР осуществляется по каналу MQ. Для канала задаются режимы аутентификации и шифрования, т.е. устанавливаются программы выхода MQSeries – модуль аутентификации каналов CSQAUTH.dll и модуль канального шифрования CSQCPHR.dll.

В случаях возникновения ошибок аутентификации или канального шифрования коды сообщений об ошибках не возвращаются в вызывающие прикладные программы. В этих случаях в вызывающие программы возвращается только ошибка 0xE8020109 «Нарушение аутентификации. В соединении с сервером отказано» библиотеки базовых функций работы с MQSeries MQBasec.dll. Собственно, ошибки модулей аутентификации каналов и канального шифрования регистрируются в журнале событий Windows «Приложение» от имени источника CSQAUTH.dll или CSQCPHR.dll. Как правило, это ошибки категории 809 «Программа выхода MQSeries». Дополнительно сообщения от этих источников выдаются на экран, если в маршруте ADMIN_NOTIFY (см. таблицу А.4 Приложения А) задан режим «показывать сообщения».

Наиболее часто получаемыми кодами сообщений о нарушениях аутентификации каналов являются:

– 0xE8033307 «Ошибка открытия или создания очереди ответов MQSeries до отправки запроса на обработку данных.» (из библиотеки Basic.dll, категория/источник «Базовая библиотека обмена данными»). Ошибка при вызове функции EdpMQS (ExecDataProc) – обработка данных внешним процессом с обменом данными по MQSeries – при открытии постоянной очереди ответов или создании динамической очереди ответов с уникальным именем. В структуре ответа возвращается дополнительный код ошибки функции MQ_Open библиотеки MQBasec.dll (MQBases.dll). Код дополнительной ошибки возвращается по вызову функции GetLasError() в приложении. Ошибка 0xE8033307 и дополнительная ошибка регистрируются в журнале событий ОС Приложение.

Повторить выполняемую на ПК операцию. Если ошибка повторяется, обратиться к ответственному за установку ПК в организации участника АИС КР для проверки настроек очередей. В приложении получить информацию о дополнительном коде ошибки и выполнить действия в соответствии с этим дополнительным кодом.

Если на стороне клиента причины возникновения ошибки не определены, обратиться в службу сопровождения ОАО «БМРЦ» (либо к разработчику ОАО «БМРЦ») для выяснения причин возникновения ошибок открытия или создания очереди в журналах менеджера MQ (проверить права доступа, память). В случае невозможности устранения ошибки следует обратиться к разработчику выполняемого приложения и к разработчику библиотеки Basic.dll;

– 0xE8090033 «<дата время> Ошибка аутентификации канала <менеджер.канал MQSeries> узла <идентификатор сервера приложений>». Ошибка аутентификации на противоположной стороне канала (мьютекс освобожден в term)» (из библиотеки CSQAUTH.dll, категория/источник «Программа выхода MQSeries»). Это означает, что канал остановлен программой выхода аутентификации на стороне сервера приложений АИС КР, причем источником проблемы, как правило, является сторона клиента АИС КР. Причинами могут быть несоответствующее серверу приложений значение последовательности в аутентификационных данных канала на стороне клиента, когда, например, был произведен откат к предыдущему состоянию ОС и реестра ОС, или в момент предыдущего старта канала произошла внезапная выгрузка ОС Windows и новое значение последовательности соединений не было сохранено. Данная ошибка также возникает после ошибки 0xE8090019, произошедшей на стороне клиента АИС КР из-за отсутствия (потери) прав для сохранения нового значения последовательности соединений в реестре ОС. Ошибка 0xE8090033 может возникнуть также, если на сторону сервера приложений пришел неверный пакет аутентификации, измененный из-за сбоя при его передаче по сети.

В этих случаях на стороне сервера приложений АИС КР выдаются ошибки 0xE8090028 «Получен неверный пакет. Имитовставки не сравнились» или при

последующих стартах канала – 0xE8090027 «Канал заблокирован программой выхода»;

– 0xE8090019 «<дата время> Ошибка аутентификации канала <менеджер.канал MQSeries> узла <идентификатор сервера приложений>». Ошибка внесения изменений в регистрационную запись канала <дополнительный код сообщения>» (из библиотеки CSQAUTH.dll, категория/источник «Программа выхода MQSeries»). Как правило, ошибка возникает из-за потери на стороне клиента АИС КР необходимых прав для сохранения нового значения последовательности соединений в реестре ОС. Требуется восстановить права к регистрационной базе каналов в реестре ОС в соответствии с [1]. Но, как правило, данных действий недостаточно, т.к. после возникновения данной ошибки и восстановления прав при последующем старте канала возникает ошибка 0xE8090033, и требуется выполнить соответствующие действия для ее устранения.

5 АВАРИЙНЫЕ СИТУАЦИИ

Аварийные ситуации, которые могут возникнуть во время работы подсистемы информационного взаимодействия АИС КР, относятся к следующим категориям:

– выход из строя технических средств (процессора, винчестера и т.п.);
– ошибки функционирования ОС;
– ошибки функционирования IBM MQ;
– устойчивые ошибки функционирования программных модулей и сервисных программ, входящих в состав клиентской части подсистемы информационного взаимодействия АИС КР.

Рекомендуется переустановить ПО клиента АИС КР, заменив, если требуется, компьютер. Для выполнения переустановки следует предварительно сохранить регистрационные данные, переданные администратором безопасности ОАО «БМРЦ» (см. [1]). В случае невозможности устранить проблемы самостоятельно следует обращаться в службу сопровождения ОАО «БМРЦ» (либо к разработчику ОАО «БМРЦ»).

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1 «Кредитный регистр. Клиентская часть подсистемы информационного взаимодействия. Инструкция по инсталляции» ЕУЯФ.92000-01 91 01

2 «Автоматизированная информационная система представления и получения информации о кредитах. Технические требования по взаимодействию с системой АИС КБ» НБРЦ.90002-01

3 «Кредитный регистр. Правила формирования и форматы запросов и сообщений. Описание информационного обеспечения» ЕУЯФ.90000.П5

4 «АС МБР. Система информационной безопасности. Протоколы взаимной аутентификации и формирования общего ключа. Описание применения» НБРЦ.41000-01 31 01

5 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

6 «АС МБР. Система информационной безопасности. Подсистема защищенного взаимодействия. Комплекс защиты соединений MQSeries. Руководство администратора» НБРЦ.48100-01 92 01

7 «АС МБР. Система информационной безопасности. Комплекс защиты соединений MQSeries. Программа регистрации каналов. Руководство пользователя» НБРЦ.48100-01 90 02

8 СТБ 1176.2-99 Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи

9 СТБ 1176.1-99 Информационная технология. Защита информации. Функция хеширования

10 «АС МБР. Система информационной безопасности. Программа регистрации ключей системы криптографической защиты информации. Руководство пользователя». НБРЦ.41200-01 90 01

11 «Кредитный регистр. Инструкция по подключению участников» ЕУЯФ.92000.И2

12 «АС МБР. Система информационной безопасности. Программа настройки таблицы маршрутизации. Руководство пользователя» НБРЦ.48200-03 90 01

13 «АС МБР. Система информационной безопасности. Подсистема обновления прикладного программного обеспечения. Программный комплекс получения обновлений прикладного программного обеспечения. Руководство пользователя» НБРЦ.47000-01 90 01

14 «АС МБР. Система информационной безопасности. Сообщения» НБРЦ.40000.В8

ПРИЛОЖЕНИЕ А

НАСТРОЙКИ ПОДСИСТЕМЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Таблица А.1 – Маршруты клиентской части информационного взаимодействия для выполнения запросов

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
AISCO_ARC_IN				
DllName	REG_SZ	Библиотека обработки	savefile.dll	Библиотека сохранения сообщений АИС КР с уникальными именами в архивные каталоги
Path	REG_SZ	Путь	<каталог установки ПО>\ ARCHIVE\IN	Каталог создается инсталлятором
TransferType	REG_DWORD		0x00000010 (16)	Тип маршрута – другой тип (неопределенный)
AISCO_ARC_OUT				
DllName	REG_SZ	Библиотека обработки	savefile.dll	Библиотека сохранения сообщений АИС КР с уникальными именами в архивные каталоги
Path	REG_SZ	Путь	<каталог установки ПО>\ ARCHIVE\OUT	Каталог создается инсталлятором
TransferType	REG_DWORD		0x00000010 (16)	Тип маршрута – другой тип (неопределенный)
AISCO_TRASH				
DllName	REG_SZ	Библиотека обработки	savefile.dll	Библиотека сохранения сообщений АИС КР с уникальными именами в архивные каталоги
Path	REG_SZ	Путь	<каталог установки ПО>\ ARCHIVE\TRASH	Каталог создается инсталлятором

Продолжение таблицы А.1

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
TransferType	REG_DWORD		0x00000010 (16)	Тип маршрута – другой тип (неопределенный)
КВ				
ArchiveIN	REG_SZ	Сохранение в архив входящих сообщений	:AISCO_ARC_IN	Локальный маршрут, определяющий, куда направлять полученные ответы для архивного хранения. Может быть отключен пользователем
ArchiveOUT	REG_SZ	Сохранение в архив исходящих сообщений	:AISCO_ARC_OUT	Локальный маршрут, определяющий, куда направлять отправленные запросы для архивного хранения. Может быть отключен пользователем
DllName	REG_SZ	Библиотека обработки	DocSignc.dll	Библиотека вычисления/проверки подписи электронных документов АИС КР
LongRetryCount	REG_DWORD	Отсутствует	2	Количество внутренних повторов выполнения операций передачи и получения сообщений MQ при временной недоступности менеджера MQ, включая сбои в сети, через длинные интервалы. Если параметр отсутствует, его значение по умолчанию равно 2
LongRetryInterval	REG_DWORD	Отсутствует	60000	Длинный интервал при внутренних повторах выполнения операций передачи и получения сообщений MQ при временной недоступности менеджера MQ, включая сбои в сети. Если параметр отсутствует, его значение по умолчанию равно 60000 миллисекунд

Продолжение таблицы А.1

Наименования маршрута и параметров	**Тип параметра**	**Наименование поля (TransportParam.exe)**	**Значение**	**Примечание**
Options	REG_DWORD	Режимы подписи и контроля	0xF(15)	Определяет режимы предобработки запроса и ответа. Если отсутствует, то используется значение 15. Значение формируется установкой опций для форматного контроля и ЭЦП исходящих и входящих сообщений в окне настройки маршрута (TransportParam.exe)
Path	REG_SZ	Путь	KB_MQ#	Локальный маршрут подключения к конкретному серверу приложений: :KB_MQ – для основного, :KB_MQ2 – для резервного (и т.д.)
ShortRetryCount	REG_DWORD	Отсутствует	3	Количество внутренних повторов выполнения операций передачи и получения сообщений MQ при временной недоступности менеджера MQ, включая сбои в сети, через короткие интервалы. Если параметр отсутствует, его значение по умолчанию равно 3
ShortRetryInterval	REG_DWORD	Отсутствует	3000	Короткий интервал при внутренних повторах выполнения операций передачи и получения сообщений MQ при временной недоступности менеджера MQ, включая сбои в сети. Если параметр отсутствует, его значение по умолчанию равно 3000 миллисекунд

Продолжение таблицы А.1

Наименования маршрута и параметров	**Тип параметра**	**Наименование поля (TransportParam.exe)**	**Значение**	**Примечание**
TransferType	REG_DWORD		0x806 (2054)	Тип маршрута – вычисление/проверка подписи документов. Установлен номер категории сообщений DocSignc.dll
Trash	REG_SZ	Сохранение/обработка брака	:AISCO_TRASH	Локальный маршрут, определяющий куда направлять отбракованные сообщения для архивного хранения
WaitIntervalLim	REG_DWORD	Отсутствует	360000	Значение, ограничивающий значение интервала ожидания ответов WaitInterval в KB_MQ#. Если параметр отсутствует, его значение по умолчанию равно 360000 миллисекунд (6 минут, время KeepAlive)
WaitRepete	REG_DWORD	Отсутствует	1	Признак для внутренних повторов по истечении интервала ожидания ответов WaitInterval в KB_MQ#. Параметр устанавливается неравным 0 для обеспечения выполнения запросов, время выполнения которых более 5 минут. Если параметр отсутствует, его значение по умолчанию равно 0 (не выполнять внутренние повторы по истечении интервала ожидания ответов)

Продолжение таблицы А.1

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
WaitRepeteInterval	REG_DWORD	Отсутствует	1800000	Общее время ожидания с внутренними повторами по истечении интервала ожидания ответов WaitInterval в KB_MQ# при установленном признаке WaitRepete. Если параметр отсутствует, его значение по умолчанию равно 1800000 миллисекунд (30 минут)
KB_MQ# – KB_MQ, KB_MQ2 (и т.д.)				
ChannelName	REG_SZ	Имя канала	<имя узла>.CHL (для резервного сервера – <имя узла>.CHL#)	В поле указывается имя канала, для подключения к серверу приложений АИС КР (где # – номер сервера)
ConnectionName	REG_SZ	Connection Name	<#.#.#.#(#)>	В поле указывается IP-адрес и порт для подключения к серверу приложений
GetQueue	REG_SZ	Очередь ответов		Локальная очередь с сообщениями по безопасности для мониторинга Если в маршрутах типа «2 - Обмен данными через MQSeries» отсутствует параметр GetQueue (очередь ответов), то для ответов используется временная динамическая очередь.
MQSType	REG_DWORD	Тип локального MQ	0	Установлено значение «Клиент», т.е. тип используемого API IBM MQ
MQTransportType	REG_DWORD	Тип транспорта	0xE0000002	Означает, что для канала IBM MQ задан протокол TCP (младшая цифра – 2) и установлены аутентификация, канальное шифрование и сжатие данных (старшая цифра – E)

Окончание таблицы А.1

Наименования маршрута и параметров	**Тип параметра**	**Наименование поля (TransportParam.exe)**	**Значение**	**Примечание**
Path	REG_SZ	Путь	:KB	Маршрут на стороне сервера приложений
PutQueue	REG_SZ	Очередь запросов	INCOMQUERY.LQ.QUEUE	При установке ПК АИС КР, предназначенных для администраторов Кредитного регистра, значение параметра меняется на ADMINQUERY.LQ
QueueManager	REG_SZ	MQ менеджер	AISCOSR#_MQM	Имя менеджера MQ на сервере приложений (где # – V для основного сервера приложений, 2, 3 и т.д. – для резервных)
TransferType	REG_DWORD		2	Тип маршрута – обмен данными через IBM MQ
WaitInterval	REG_DWORD	Интервал ожидания ответов	0x7530 (30000)	Время ожидания получения данных из ответной очереди (в миллисекундах). Ограничивается значением WaitIntervalLim в маршруте KB
PK_source (из раздела ОС HKLM\ SOFTWARE\BTC\ Crypt_Doc)	REG_DWORD	Тип носителя	<выбранный тип при установке ПО>	Параметр PK_source может иметь значения: 4 – означает расположение ключа ЭЦП на носителе eToken, 8 – на носителе iKey, 10 – ключ занесен в реестр ОС

Таблица А.2 – Маршруты комплекса управления ключами СКЗИ и средств ЭЦП

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
KeyDistributionGroup				
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ KeyDistributionGroup	Раздел реестра ОС и его параметр. Значение параметра KeyDistributionGroup (REG_SZ) – номер списка рассылки ключей ЭЦП. Для АИС КР значение KeyDistributionGroup равно 2
RemCall	REG_DWORD	Разрешить удаленный вызов	0	Удаленный вызов маршрута не разрешен
TransferType	REG_DWORD		3	Тип маршрута – чтение/запись данных в реестр MS Windows
KeyMgr				
DllName	REG_SZ	Библиотека обработки	SC_KeyMgrF.dll	Библиотека обработки запросов к хранилищу ключевой информации
Path	REG_SZ		:KeyMgrCN	Маршрут на стороне сервера приложений
RemCall	REG_DWORD	Разрешить удаленный вызов	0	Удаленный вызов маршрута не разрешен
TransferType	REG_SZ		0x811(2065)	Тип маршрута – обработка запросов к хранилищу ключевой информации. Установлен номер категории сообщений KeySql.dll
KeyMgr_REMOTE				
ChannelName	REG_SZ	Имя канала	<имя узла>.CHL (для резервного сервера – <имя узла>.CHL#)	В поле указывается имя канала, для подключения к серверу приложений (где # – номер сервера)

Продолжение таблицы А.2

Наименования маршрута и параметров	**Тип параметра**	**Наименование поля (TransportParam.exe)**	**Значение**	**Примечание**
ConnectionName	REG_SZ	Connection Name	<#.#.#.#(#)>	В поле указывается IP-адрес и порт для подключения к серверу приложений
Format	REG_SZ	Формат	DTSQUERY	Формат сообщений MQ компонентов информационной безопасности
MQSType	REG_DWORD	Тип локального MQ	0	Установлено значение «Клиент», т.е. тип используемого API IBM MQ
MQTransportType	REG_DWORD	Тип транспорта	0xE0000002	Означает, что для канала MQ задан протокол TCP (младшая цифра – 2) и установлены аутентификация, канальное шифрование и сжатие данных (старшая цифра – E)
Path	REG_SZ	Путь	:KeyMgr	Маршрут на стороне сервера приложений
PutQueue	REG_SZ	Очередь запросов	AISCOSR#.SECURITY_QUERY.LQ	Имя очереди MQ на сервере приложений для запросов СКЗИ (где # – V для основного сервера приложений, 2, 3 и т.д. – для резервных)
QueueManager	REG_SZ	MQ менеджер	AISCOSR#_MQM	Имя менеджера MQ на сервере приложений (где # – V для основного сервера приложений, 2, 3 и т.д. – для резервных)
RemCall	REG_DWORD	Разрешить удаленный вызов	0	Удаленный вызов маршрута не разрешен
TransferType	REG_DWORD		2	Тип маршрута – обмен данными через IBM MQ
WaitInterval	REG_DWORD	Интервал ожидания	0x7530 (30000)	Время ожидания получения данных (в миллисекундах)

Продолжение таблицы А.2

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
KeyMgrCN				
ChannelName	REG_SZ	Имя канала	<имя узла>.CHL (для резервного сервера – <имя узла>.CHL#)	В поле указывается имя канала, для подключения к серверу приложений (где # – номер сервера)
ConnectionName	REG_SZ	Connection Name	<#.#.#.#(#)>	В поле указывается IP-адрес и порт для подключения к серверу приложений
Format	REG_SZ	Формат	DTSQUERY	Формат сообщений MQ компонентов информационной безопасности
MQSType	REG_DWORD	Тип локального MQ	0	Установлено значение «Клиент», т.е. тип используемого API IBM MQ
MQTransportType	REG_DWORD	Тип транспорта	0xE0000002	Означает, что для канала MQ задан протокол TCP (младшая цифра – 2) и установлены аутентификация, канальное шифрование и сжатие данных (старшая цифра – E)
Path	REG_SZ	Путь	:KEYMGR_REMOTE	Маршрут на стороне сервера приложений
PutQueue	REG_SZ	Очередь запросов	AISCOSR#.SECURITY_QUERY.LQ	Имя очереди MQ на сервере приложений для запросов СКЗИ (где # – V для основного сервера приложений, 2, 3 и т.д. – для резервных)
QueueManager	REG_SZ	MQ менеджер	AISCOSR#_MQM	Имя менеджера MQ на сервере приложений (где # – V для основного сервера приложений, 2, 3 и т.д. – для резервных)

Окончание таблицы А.2

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
RemCall	REG_DWORD	Разрешить удаленный вызов	0	Удаленный вызов маршрута не разрешен
TransferType	REG_DWORD		2	Тип маршрута – обмен данными через IBM MQ
WaitInterval	REG_DWORD	Интервал ожидания	0x7530 (30000)	Время ожидания получения данных (в миллисекундах)
KeyUnitID_Group				
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ KeyGroup	Раздел реестра ОС и его параметр. Значение параметра KeyGroup (REG_SZ) – код группы ключей ЭЦП клиента АИС КР. Значение KeyGroup задает пользователь при инсталляции ПО
RemCall	REG_DWORD	Разрешить удаленный вызов	0	Удаленный вызов маршрута не разрешен
TransferType	REG_DWORD		3	Тип маршрута – чтение/запись данных в реестр MS Windows

Таблица А.3 – Маршруты комплекса получения обновлений ППО

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
UPDATE_LIST				
\AISCO_Client\ Version	REG_SZ		KBC0XXYYZZ (где XXYYZZ – номер версии ПО)	Номер версии заносится при установке или обновлении ПО клиентской части подсистемы информационного взаимодействия
DllName	REG_SZ	Библиотека обработки	UpdtChk.dll	Библиотека обработки запросов обновлений ППО
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\Router\ UPDATE_LIST\	Раздел реестра ОС, где находятся подразделы (с именами категорий ППО) с параметрами Version (REG_SZ)
TransferType	REG_DWORD		0x80d (2061)	Тип маршрута – другой тип (неопределенный). Установлен номер категории сообщений UpdtChk.dll
UPDATE_SERVER				
Path	REG_SZ	Путь	:KB_MQ#	Запрос обновлений ППО осуществляется через маршрут активного подключения к серверу приложений
PutQueue	REG_SZ		AISCO_UPDATE.LQ	Очередь запросов на сервере приложений, обрабатываемая службой от имени AISCOUPDATE
UpdateParams				
CheckInterval	REG_DWORD		86400 (24 часа)	Интервал проверки наличия актуальных обновлений (в программе UpdateParams.exe) в секундах

Продолжение таблицы А.3

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
DownloadNotOn	REG_DWORD		1	Оповещение о загрузке (в программе UpdateParams.exe) в случае автоматической загрузки обновлений: 0 – не оповещать; 1 – оповещать
DownloadOp	REG_DWORD		2	Загрузка обновлений (в программе UpdateParams.exe): 1 – уведомлять о наличии, но не загружать; 2 – загружать автоматически
DownloadPath	REG_SZ		<каталог установкиПО>\ UpdatesCache\	Каталог для загрузки обновлений (в программе UpdateParams.exe)
DownloadTime	REG_DWORD		1368009000	Интервал проверки наличия актуальных обновлений
InstallOp	REG_DWORD		1	Установка обновлений (в программе UpdateParams.exe): 1 – не устанавливать; 2 – устанавливать автоматически
InstallTime	REG_DWORD		0xFFFFFFFF (-1)	Время установки загруженных обновлений (в программе UpdateParams.exe): 0 – немедленно, > 0 – время дня в секундах; -1 – время установки не задано

Окончание таблицы А.3

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
ParamsNames	REG_MULTI_SZ		ServiceOn CheckInterval DownloadOp DownloadNotOn DownloadPath DownloadTime InstallOp InstallTime	Должны быть указаны три списка – ParamsNames, ParamsSizes и ParamsTypes для 8 параметров структуры. Значения параметров настраиваются при помощи программы UpdateParams.exe (подробное описание см. в [13]). ParamsNames – это список имен параметров
ParamsSizes	REG_BINARY		04000000 04000000 04000000 04000000 04000000 04000000 04000000 04000000 04010000 04000000 04000000 04000000 04000000 04000000 04000000 04000000	ParamsSizes – это список максимальных размеров полей для значений параметров в структуре (в байтах)
ParamsTypes	REG_BINARY		04000000 04000000 04000000 04000000 04000000 04000000 04000000 04000000 01000000 04000000 04000000 04000000 04000000 04000000 04000000 04000000	ParamsTypes – это список типов значений параметров в структуре (в байтах)
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\Router\UpdateParams\	Раздел реестра ОС, где расположены три параметра: ParamsNames, ParamsSizes и ParamsTypes – для получения структуры данных
RemCall	REG_DWORD	Разрешить удаленный вызов	0	Удаленный вызов маршрута не разрешен
ServiceOn	REG_DWORD		1	Включить службу автоматического обновления: 0 – служба отключена; 1 – служба включена
TransferType	REG_DWORD		3	Тип маршрута – чтение/запись данных в реестр MS Windows

Таблица А.4 – Маршруты комплекса защиты соединений MQSeries

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
ADMIN_NOTIFY				
DllName	REG_SZ	Библиотека обработки	KC_AdmNotify.dll	Библиотека обработки административных уведомлений
LogEvents	REG_DWORD	Сохранять в журнал событий	0	Уведомления сохраняются в журнал событий «Приложение»
ShowMessages	REG_DWORD	Показывать сообщения	1	Уведомления выводятся на экран
TransferType	REG_DWORD		0x805 (2053)	Тип маршрута – обработка административных уведомлений. Установлен номер категории сообщений KC_AdmNotify.dll
DefaultChlType				
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ RegAuth\DefChlType	Раздел реестра ОС и его параметр. Значение параметра DefChlType (REG_DWORD) – тип канала по умолчанию в программе регистрации каналов. Значение DefChlType равно 2 (Client)
TransferType	REG_DWORD		3	Тип маршрута – чтение/запись данных в реестр MS Windows
Node_ID				
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ RegAuth\NodeID	Раздел реестра ОС и его параметр. Значение параметра NodeID (REG_SZ) – идентификатор узла-клиента АИС КР этого рабочего места. Значение NodeID задает пользователь при инсталляции ПО

Продолжение таблицы А.4

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
TransferType	REG_DWORD		3	Тип маршрута – чтение/запись данных в реестр MS Windows
RegAuth				
DllName	REG_SZ	Библиотека обработки	RegAuth.dll	Библиотека функций регистрации каналов для модуля аутентификации
TransferType	REG_DWORD		0x80a (2058)	Тип маршрута – регистрация каналов в модуле аутентификации. Установлен номер категории сообщений RegAuth.dll
RegCEnc				
Path	REG_SZ	Путь	<выбранный каталог при установке ПО>\ Channel.enc	Путь к файлу channel.enc с аутентификационными данными канала, используемый при регистрации канала
TransferType	REG_DWORD		0	Тип маршрута – чтение/запись файлов
RegFBase				
DllName	REG_SZ	Библиотека обработки	WinCrypt.dll	Библиотека шифрования данных встроенными алгоритмами Windows
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ RegAuth	Раздел реестра ОС, содержащий в подразделах в параметрах «(По умолчанию)» (REG_BINARY) аутентификационные данные каналов (C1, C2 и т.д.)
TransferType	REG_DWORD		0x807 (2055)	Тип маршрута – шифрование данных алгоритмами MS Windows. Установлен номер категории сообщений WinCrypt.dll

Окончание таблицы А.4

Наименования маршрута и параметров	Тип параметра	Наименование поля (TransportParam.exe)	Значение	Примечание
RegFInd				
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ RegAuth\Ind	Раздел реестра ОС, содержащий параметр «(По умолчанию)» (REG_BINARY) – список каналов, зарегистрированных в программе регистрации каналов
Serv_ID				
Path	REG_SZ	Путь	HKLM\SOFTWARE\BTC\AISCO\ RegAuth\ServID	Раздел реестра ОС и его параметр. Значение параметра ServID (REG_SZ) – идентификатор сервера приложений. Значение ServID пользователь устанавливает при выборе активного сервера приложений
TransferType	REG_DWORD		3	Тип маршрута – чтение/запись данных в реестр MS Windows

ЛИСТ СОГЛАСОВАНИЯ

От Национального банка Республики Беларусь

Должность	Фамилия, имя, отчество	Подпись	Дата
Зам. нач. УВЧТ	Бубрышкин		04.11.2019
Гл. спец. УКР	Силявко Е.А.		04.11.19

ЛИСТ СОГЛАСОВАНИЯ

От ОАО «БМРЦ»

Должность	Фамилия, имя, отчество	Подпись	Дата
Зам. Председателя Правления	Гогулин А.Н.		1.11.2019
Нач. департамента	Тлаев А.Б.		31.10.2019
Нач. ДЭ АИС	Харина О.А.		31.10.19
Нач. УРиСЕВИС	Коленкин Е.Д.		31.10.19
Нач. УЭ АИС	Тонич В.Ф.		31.10.2019
Зам.нач. ДЭ АИС	Шубенский Ю.Н.		31.10.19
Начальник УРиССИБ	Кравченко В.В.		31.10.2019

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Извещение об изменении	Подпись	Дата
	измененных	замененных	новых	аннулированных				