Федеральное государственное унитарное предприятие
«ЗащитаИнфоТранс Министерства транспорта Российской Федерации»
(ФГУП «ЗащитаИнфоТранс»)

Информационная система «Авиационная сервисная платформа»

Инструкция по подключению

Листов 18

2023

Аннотация

Настоящая инструкция предназначена для подключения к информационной системе «Авиационная сервисная платформа» (далее – Система) с целью проверки работоспособности подключения для передачи авиационных сообщений. Инструкция содержит в себе сведения о предварительном этапе и установке формализованных отношений между Участниками подключения и ФГУП «ЗащитаИнфоТранс» (далее – Оператор Системы), об условиях корректного подключения Участников подключения, об организации каналов связи между Участниками подключения и методах тестирования.

Участниками подключения являются все организации, являющиеся участниками информационного взаимодействия на платформе Системы. Участниками подключения могут быть авиакомпании, аэропорты, агенты по продаже авиабилетов, компании по наземному обслуживанию.

Содержание

Перечень обозначений и сокращений

В настоящем документе применяются следующие обозначения и сокращения:

ИС	–	информационная система
ИС АСП	–	информационная система Информационная система «Авиационная сервисная платформа»
СКЗИ	–	Средствами криптографической защиты информации
Email	–	адрес электронной почты

Перечень терминов и определений

В настоящем документе применяются следующие термины с соответствующими им определениями:

Анкета участника подключения (анкета)	–	анкета, заполняемая Участником подключения на предварительном этапе подключения к Системе
Информационная система	–	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (ГОСТ 34.601-90)
Информационная система «Авиационная сервисная платформа» (Система)	–	система, обеспечивающая непрерывность пассажироперевозок в гражданской авиации в части реализации безопасного информационного обмена авиателеграммами на территории Российской Федерации
Оператор Системы	–	организация, оператор ИС АСП (ФГУП «ЗащитаИнфоТранс»)
Система	–	Информационная система «Авиационная сервисная платформа»
Участник подключения	–	организация, участник информационного взаимодействия на платформе ИС АСП. Участниками подключения могут быть авиакомпании, аэропорты, агенты по продаже авиабилетов, компании по наземному обслуживанию
AMQP	–	открытый протокол прикладного уровня для передачи сообщений между компонентами системы. Основная идея состоит в том, что отдельные подсистемы (или независимые приложения) могут обмениваться произвольным образом сообщениями через AMQP-брокер, который осуществляет маршрутизацию, возможно гарантирует доставку, распределение потоков данных, подписку на нужные типы сообщений;
IATA	–	международная ассоциация воздушного транспорта, выступает координатором и представителем интересов авиатранспортной

		отрасли в таких областях как обеспечение безопасности полётов, производство полётов, тарифная политика, техобслуживание, авиационная безопасность, разработка международных стандартов
IPsec	–	набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном применяется для организации VPN-соединений
MPLS	–	многопротокольная коммутация по меткам – способ организации передачи данных в сети с организацией сквозных виртуальных каналов
SMTP	–	простой протокол передачи почты, широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
TYPE B	–	формат передачи сообщений между наземными службами и воздушным судном
VIPNet Coordinator	–	программно-аппаратный комплекс защищенной сети ViPNet. Выполняет фильтрацию открытых пакетов на каждом сетевом интерфейсе в соответствии с заданными настройками по адресам, протоколам и портам

1. Общие положения

Процесс подключения запускается после получения заявки от потенциального Участника подключения. Заявка может быть направлена следующими способами:

– отправка запроса на консультацию по электронной почте sales@transio.ru;

– заполнение формы «Оставить заявку на подключение к системе» на transio.ru;

– звонок по номеру телефона +7 (495) 380-21-53;

– отправка запроса на консультацию по электронной почте support@transio.ru.

После получения запроса Оператор Системы связывается с потенциальным Участником подключения по выбранному каналу связи, консультирует по возникающим вопросам, например:

– варианты подключения;

– стоимость подключения;

– стоимость обслуживания;

– тарификация сообщений;

– процесс подключения.

По результатам консультации Оператора Системы с потенциальным Участником подключения, запускается процесс подключения к Системе.

Процесс подключения к Системе состоит из этапов:

– предварительный этап;

– организация подключения к Системе;

– тестирование взаимодействия;

– подключение к промышленной среде Системы.

По окончанию этапов подключения к Системе осуществляется оказание технической поддержки Оператором Системы.

Любые вопросы по проблемам, связанным с подключением или выполнением любого из этапов подключения, необходимо направлять сотруднику Оператора Системы, ответственному за данное подключение. Контакты данного сотрудника будут предоставлены представителю Участника подключения на предварительном этапе.

2. Предварительный этап

В рамках подготовки к организации подключения к Системе с целью формализации всех положений информационного взаимодействия между Участником подключения и Оператором Системы следует согласовать и подписать один из следующих документов:

– договор о научно-техническом сотрудничестве для апробации и тестирования Системы Участником подключения;

– соглашение о неразглашении конфиденциальной информации;

– договор об оказании услуг.

После заключения одного из указанных выше документов между Участником подключения и Оператором Системы выделяется специалист Оператора Системы, ответственный за данное подключение. Ответственный специалист Оператора Системы связывается с представителем Участника подключения и направляет логин и пароль для доступа к анкете участника подключения.

Анкета участника подключения представляет собой перечень полей для заполнения, представленных на интернет-странице. Анкета доступна по ссылке welcome.transio.ru, также к ней можно получить доступ через кнопку «Войти в личный кабинет», расположенной на transio.ru.

При переходе на интернет-страницу анкеты необходима авторизация с помощью присланных специалистом Оператора Системы данных (логин и пароль).

Все поля анкеты обязательны к заполнению представителем Участника подключения, в случае отсутствия возможности заполнить поле – необходимо поставить в данном поле прочерк или указать поясняющий комментарий. Информация, введенная в анкете, автоматически передается сотруднику Оператора Системы после ее заполнения на интернет-странице. После получения заполненной анкеты сотрудник Оператора Системы изучает данные и, при необходимости, направляет дополнительные либо уточняющие вопросы по электронной почте представителю Участника подключения.

3. Организация подключения

3.1. Организация тестового соединения

Для организации тестового соединения с Системой осуществляется настройка канала с применением шифрованного соединения стандарта IP Sec.

Для установления IP Sec соединения (туннеля) инженерному персоналу Участника подключения необходимо провести конфигурационные настройки на своем сервере, используя те же значения параметров, которые были указанных в заполненной анкете и сообщить о завершении конфигурационных настроек сотруднику Оператора Системы. Указанные в данном разделе действия могут выполняться совместно со специалистом Оператора Системы, ответственным за подключение Участника подключения.

3.1.1. Настройка IKE

IKE (Internet Key Exchange) нужен для установления Security Association. На этом этапе необходимо сконфигурировать политики безопасности и указать полученный от сотрудника Оператора Системы Pre-Shared ключ для аутентификации с другой стороной подключения. Pre-Shared ключ передается представителю Участника подключения в рабочем порядке.

3.1.2. Настройка IPSec

Сотрудник Оператора системы передает параметры настройки представителю Участника подключения в рабочем порядке.

Для настройки IPSec необходимо выполнить следующие действия:

1. Создать Access-list и в нем указать список сетей (маршрутизацию) для организации VPN-туннеля.
2. Создать набор преобразования IPSec Transform и указать метод и алгоритм шифрования.
3. Создать криптографическую карту (Crypto Map) для объединения двух этапов настройки.
4. Применить криптографическую карту к общедоступному (public) интерфейсу хоста, через который выходит трафик.

3.2. Организация защищённого подключения

Создание защищенного подключения представляет собой организацию комплекса средств криптографической защиты информации, предназначенного для организации защищенной виртуальной частной сети и создания криптозащищенного канала передачи данных в Систему. Криптозащищенный канал передачи данных строится на базе выбранного Участником подключения варианта. Для примера ниже описана организация для следующих вариантов:

– ПАК ViPNet;

– MPLS.

Организация защищённого подключения включает в себя в большинстве случаев следующие этапы:

1. Разработку технического решения.
2. Согласование технического решения с Участником подключения.
3. Закупку оборудования Оператором системы.
4. Установку и настройку оборудования Оператором системы для Участника подключения.

Пункты 3 и 4 выполняются после заключения договора.

Оператор Системы обладает лицензией ФСБ России на оказание данных услуг, в т.ч. оказание любой технической поддержки, связанной с эксплуатацией сетей и использованием СКЗИ.

3.2.1. Организация защищенного подключения через VipNet

Организация защищенного подключения через VipNet может осуществляться одном из двух способов в зависимости от выбранного участником подключения способа организации защищенного соединения и наличия у участника подключения ПАК VipNet.

Для организации подключения по VipNet выполняются следующие действия:

1. Специалисты Оператора Системы запрашивают у представителя Участника подключения локальные параметры сетевых настроек для обеспечения согласованной работы оборудования в защищенном канале. Инженерный персонал Участника подключения выполняет настройки криптомаршрутизатора перед его установкой в серверном (коммутационном) зале.
2. Специалисты Оператора Системы производят выезд на территорию участника для проведения настроек и монтажа оборудования, предварительно настроенного в соответствии с параметрами, полученными от Участника подключения. Участник подключения должен обеспечить необходимые условия на своей территории для качественного монтажа оборудования (координатора) VipNet специалистами Оператора Системы.
3. Участник подключения собственными силами должен произвести настройки маршрутизации трафика через интерфейс координатора VipNet для подсети 10.1.0.0/24 на своем оборудовании.

В случае наличия оборудования у Участника подключения организовывается межсетевое взаимодействие с Оператором Системы, пункт 2 списка выше не выполняется, установка в серверном (коммутационном) зале не производится.

Концептуальная структурная схема, представленная ниже (рисунок 1), содержит типовое решение, обеспечивающее защиту передаваемых данных в сети Интернет за счет установки криптомаршрутизаторов HV100 на границе выхода в незащищенное коммуникационное пространство.

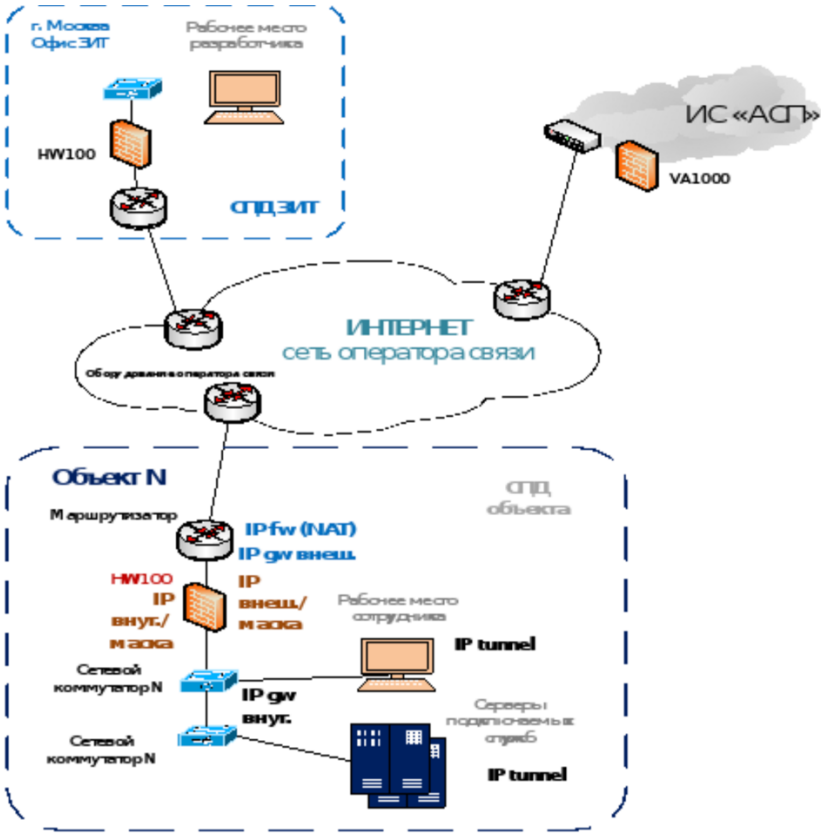

Рисунок 1 – Структурная схема

Пояснения к рисунку 1:

– сеть оператора связи – существующая в настоящее время сеть, к которой подключен аэропорт для выхода в сеть Интернет;

– СПД Аэропорта – сеть аэропорта (объекта), подключаемого к временному защищенному каналу передачи данных;

– ИС «АСП» – размещение Системы;

– IP xxx.xxx – адресное пространство СПД объекта для настройки защищенной сети передачи данных. IP tunnel – не более десяти устройств на время тестирования;

– HW100 – криптомаршрутизатор предоставляемый на время проведения испытаний службами ФГУП «ЗащитаИнфоТранс»;

– прочее используемое оборудование из состава существующих на объектах подключения СПД.

Вариант размещения оборудования VipNet на территории Участника подключения представлено на рисунке ниже (рисунок 2). Размещение оборудования выполняется в коммутационной стойке, с возможностью установки в свободном пространстве и подключения электропитания 220В. Подключение выполняется патч-кордами с разъемами RJ45.

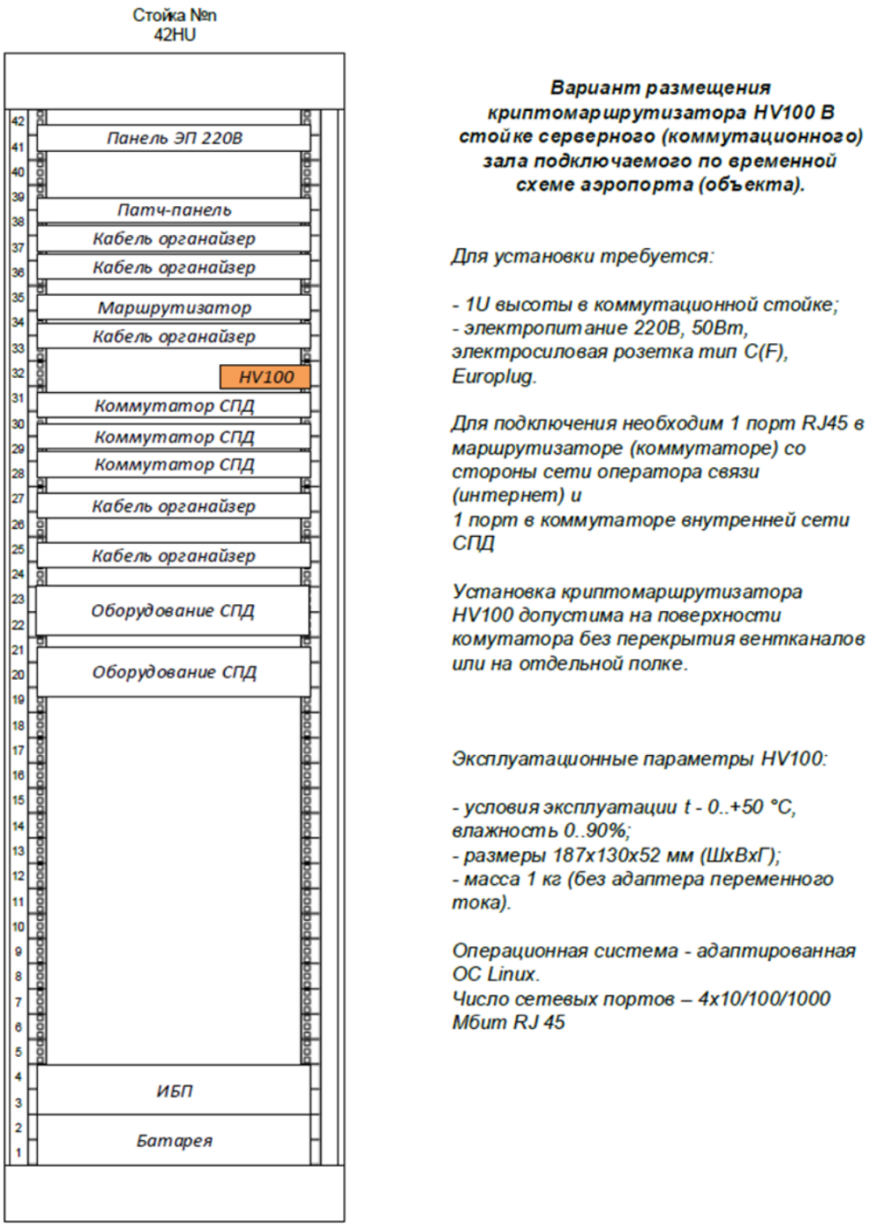

Рисунок 2 – Размещение оборудования в стойке

3.2.2. Организация защищенного подключения через MPLS

MPLS сеть настраивается индивидуально для каждого Участника подключения. Типовая структурная схема организации защищенного подключения через MPLS представлена ниже (рисунок 3).

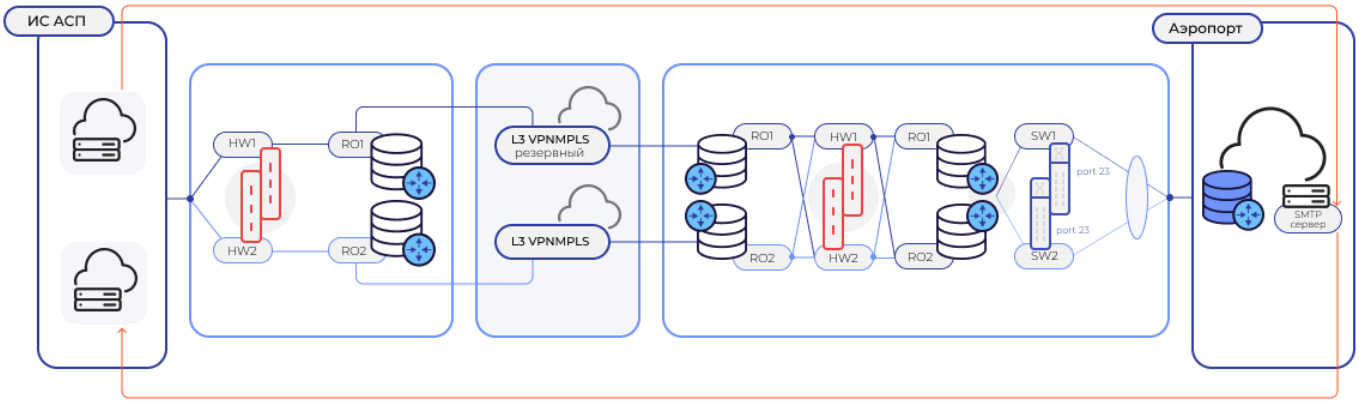

Рисунок 3 – Типовая схема подключения организации защищенного подключения через MPLS

Доступна возможность разработки персонализированной схемы для участника подключения предварительно, до организации подключения. Для получения персонализированной схемы необходимо направить запрос на электронную почту sales@transio.ru.

3.3. Настройка клиентских шлюзов

При заполнении анкеты участника подключения (п. 2) в анкете указываются предпочтительные для Участника подключения протоколы обмена – SMTP и/или AMQP.

После организации тестового соединения (п. 3.1) выполняется настройка передачи сообщений по выбранному Участником подключения протоколу (протоколам).

После организации защищенного подключения (п. 3.2) происходит переключение настроек маршрутизации с тестового подключения на выбранную Участником подключения ЗСПД.

3.3.1. Подключение по протоколу SMTP

При заполнении анкеты участника подключения (п. 2), при выборе протокола обмена SMTP, в анкете заполняются поля параметров подключения к SMTP relay server Участника подключения, используемые им адреса (если их несколько, то можно направить их отдельным списком сотруднику Оператора системы после заполнения анкеты), адреса электронной почты в формате address@customer.domain, где:

– address – это часть почтового адреса (учетная запись) в составе семи символов до знака @ (на примере аэропорта г. Волгограда – это VOGBSXH). Перечень адресов предоставляется Участником подключения. В случае отсутствия у Участника подключения address, ему может быть выдана учетная запись для регистрация почтового адреса внутри собственного домена только для использования во внутренних рейсах на территории Российской Федерации;

– customer.domain – это внутренняя доменная часть Участника после знака @ (на примере аэропорта г. Волгограда – это transio.mav.ru). Данную часть Участник подключения определяет самостоятельно.

Обращаем внимание, что адрес для отправки и адрес для получения (поле "TO" и поле "FROM") сообщений могут отличаться, необходимо учесть важное требование: оба адреса должны соответствовать формату address@customer.domain (на примере аэропорта г. Волгограда – это VOGBSXH@transio.mav.ru для получения сообщений и VOGBSXH@mav.ru для отправки сообщений). Решение о регистрации на внутреннем почтовом сервере единого адреса для отправки и получения Участник подключения принимает самостоятельно. Участником подключения должно быть четко сопоставлено какой address к какому email относится.

Допускается относить к одному address несколько адресов электронной почты и наоборот. Параметры подключения по протоколу SMTP предоставляются Участнику подключения на электронный адрес представителя Участника подключения.

После окончания обмена необходимой информацией Участник подключения настраивает на своей стороне SMTP relay server, где создает правило, по которому поток сообщений может быть перенаправлен в сторону SMTP relay server Системы. Обращаем внимание, что продуктивный поток сообщений не направляется до момента успешного окончания прохождения тест кейсов и подписания протокола тестирования (п. 4). Логическая модель взаимодействия по протоколу SMTP на примере информационного обмена между а/п Волгограда и а/п Калининграда представлена ниже (рисунок 4).

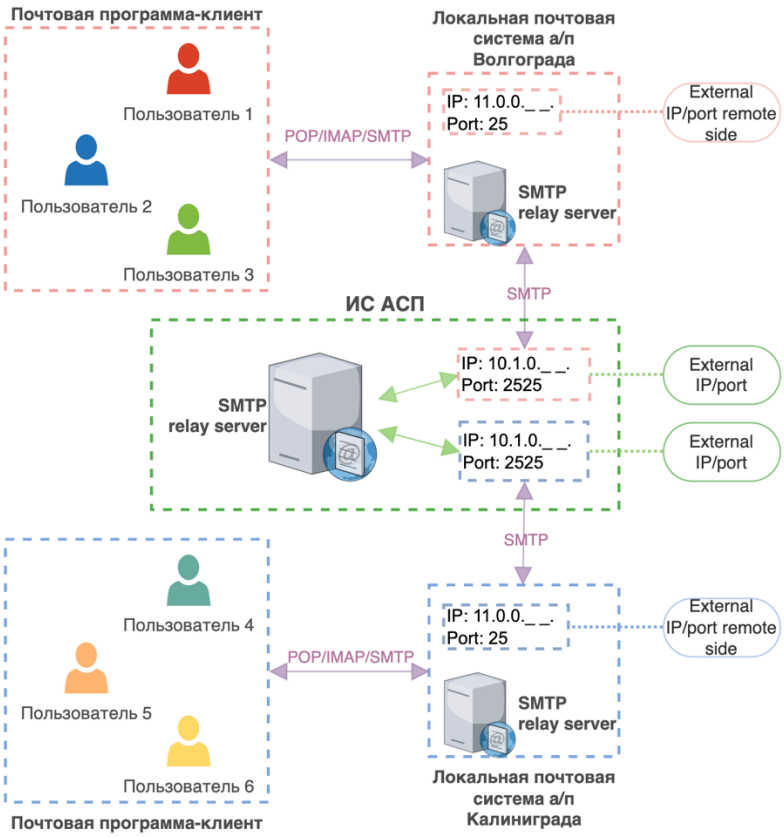

Рисунок 4 – Логическая модель взаимодействия по протоколу SMTP на примере информационного обмена между а/п Волгограда и а/п Калининграда

После настройки SMTP relay server на своей стороне Участник подключения может проверить соединение с SMTP relay server Системы, выполнив команду и указав свои значения параметров:

– отправка по SMTP: nc -v host:port 2525.

3.3.2. Подключение по протоколу AMQP

Для получения необходимых индивидуальных значений параметров подключения к Системе по протоколу AMQP, в анкете участника подключения (п. 2) заполняются все поля, обязательные к заполнению, в том числе, информация об используемых адресах. Параметры подключения по протоколу AMQP предоставляются на электронный адрес представителя Участника подключения сотрудником Оператора системы .

После окончания обмена необходимой информацией Участник подключения настраивает на своей стороне сервис по подключению и отправке сообщений в Систему. Обращаем внимание, что продуктивный поток сообщений не направляется до момента успешного окончания прохождения тест кейсов и подписания протокола тестирования (п. 4). Логическая модель взаимодействия по протоколу AMQP на примере информационного обмена между а/п Шереметьево и а/к Аэрофлот представлена ниже (рисунок 5).

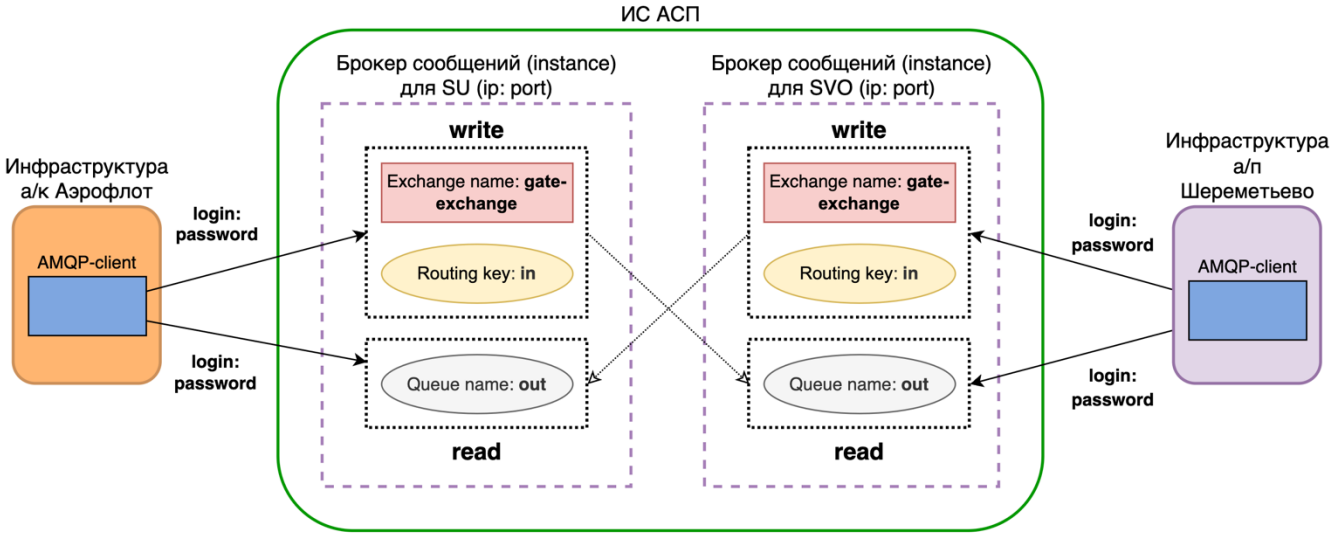

Рисунок 5 – Логическая модель взаимодействия по протоколу AMQP на примере информационного обмена между а/п Шереметьево и а/к Аэрофлот

После окончания настройки, Участник подключения может проверить соединение по AMQP протоколу с Системой, выполнив команды ниже, указав свои значения параметров:

– запись по AMQP: echo "hello" | ~/go/bin/rabtap pub -- uri=amqp://login:password@host:port --exchange gate-exchange --routingkey=in;

– чтение по AMQP: ~/go/bin/rabtap sub --uri=amqp://loging:password@host:5672 out.

3.4. Внесение адресов для передачи сообщений в базу данных

Адресные коды АТА/IATA, полученные от Участников подключения, а также соответствующие им адреса электронной почты (в случае передачи сообщений по SMTP протоколу) вносятся в базу данных Системы сотрудником Оператора Системы. Сотрудник Оператора системы вносит в базу данных все необходимые адреса, но тестирование в дальнейшем проводится с использованием выбранного Участником подключения адреса для тестирования.

4. Тестирование взаимодействия

Сотрудник Оператора системы разрабатывает персональные для данного Участника подключения тест кейсы, затем передает их представителю Участника подключения. Осуществляется взаимодействие по всем вопросам, возникающим при тестировании.

После проведения совместного тестирования взаимодействия Участника подключения с Системой принимаем решение об успешности тестирования и подписываем протокол результатов тестирования между Участником подключения и Оператором системы.

4.1. Создание сообщений

Процесс отправки сообщений по протоколу SMTP является стандартным процессом отправки сообщений через почтового клиента. Для отправки сообщения от одного Участника подключения к другому, отправителю необходимо ввести в поле определения получателя почтового клиента адрес получателя в домене msg.transio.ru.

Например, аэропорту г. Волгограда необходимо отправить сообщение в аэропорт г. Калининграда – в этом случае отправитель из аэропорта г. Волгограда, имеющий свой внутренний доменный почтовый адрес VOGBSXH@transio.mav.ru, зарегистрированный в Системе, указывает в заголовке получателя адрес аэропорта г. Калининграда KGDAPXH в домене msg.transio.ru (KGDAPXH@msg.transio.ru). Далее сервер Системы по таблице маршрутизации находит соответствующий почтовый адрес аэропорта г. Калининграда в его внутреннем домене, например, KGDAPXH@kgd.aero, и направляет сообщение на этот адрес.

Перечень адресов запрашивается у каждого вновь подключаемого участника на этапе подключения и вносится в базу данных Системы (п. 3.4).

Передача сообщений осуществляется только в формате «Обычный текст», т.е. без вложений, формат задаётся в параметрах используемой для отправки почтовой программы-клиента.

Процесс отправки по протоколу AMQP отличается от процесса отправки по SMTP протоколу только тем, что нет необходимости принудительно указывать отправителя и получателя в соответствующих полях.

Система обеспечивает возможность для получателя принимать сообщение по протоколу SMTP, даже если отправитель сообщения подключен к Системе по протоколу AMQP, и наоборот, получатель, подключенный по протоколу AMQP, сможет получить сообщение, отправленное от другого Участника подключения по протоколу SMTP.

5. Подключение к промышленной среде

После подписания договора на оказание услуг между Оператором системы и Участником подключения осуществляется закупка оборудования Оператором Системы, его установка и настройка для Участника подключения (п. 3.2). После завершения настроек оборудования Оператор Системы осуществляет переключение Участника подключения с тестового подключения (п. 3.1) на промышленную среду, сотрудник Оператора системы направляет представителю Участника подключения данные для доступа в Личный кабинет Системы.

6. Оказание технической поддержки

Происходит постановка Участника подключения на техническую поддержку, включающую мониторинг проходящего трафика авиационных сообщений, сетевого подключения.

Порядок взаимодействия Участника подключения с технической поддержкой описывается в рамках заключаемого с Оператором системы договора (п. 5).