МОСКОВСКАЯ БИРЖА

Универсальный файловый шлюз системы ЭДО Московской Биржи

Руководство пользователя

версия 1.0.0.36

Москва 2021

Содержание

История изменений

Дата	Версия	Изменения

04.04.2014	1.0.0.26	Внесены следующие изменения:
		• Изменения и дополнения в EdiMail.ini:
		  • В секции [crypto] добавлен ключ search.
		  • Добавлена секция [notification] — Параметры уведомлений.
		• Изменения и дополнения в EDIMailSrvs.ini:
		  • В секции [global] добавлены ключи onCertFindError, onMsgSend, onMsgReceive.
		• Добавлена поддержка сквозной нумерации принимаемых файлов (см. раздел 4.1.3.3, раздел 7.2 и раздел 6.11).
		• Добавлен раздел 5.4.
		• Добавлены раздел 6.8, раздел 6.9, раздел 6.10.
		• Добавлен раздел 8.

19.10.2016	1.0.0.31	Внесены следующие изменения: • Добавлена поддержка работы с нерезидентами (см. раздел 4.5). • Добавлена возможность архивации с помощью SQL Server 2008 – хранение тела сообщений в файлах, а не в полях таблицы. • Добавлена возможность задания паролей для почтовых ящиков и пин кодов для носителей криптоключей с помощью JavaScript функций (см. раздел 6.12).
05.10.2017	1.0.0.36	Внесены следующие изменения: • Добавлен глобальный запрет на удаленное обновление ПО (см. раздел 7.1 секция [permission], ключ noUpdate). • Добавлена возможность рассылки почтовых уведомлений для администратора ЭДО модулем FileGate (см. раздел 6.8). • Добавлена возможность задавать способ аутентификации при обмене с почтовым сервером. В соответствующие секции настроечных файлов добавлен ключ login_options.

1. Введение

1.1. Цель документа

Цель документа — дать общее представление об архитектуре, принципах функционирования и возможностях использования файлового шлюза ЭДО МБ в системах обработки информации. В документе рассматриваются следующие вопросы:

- Краткое описание системы ЭДО МБ. Архитектура, состав и назначение основных компонентов системы.
- Описание архитектуры файлового шлюза ЭДО МБ. Назначение и состав ПО, форматы файлового обмена, правила приема/отправки сообщений, типовая структура каталогов файлового шлюза.
- Описание процедуры установки и запуска.
- Порядок работы с файловым шлюзом. Настройка правил приема/отправки сообщений, настройка параметров идентификации, возможность одновременного использования нескольких файловых шлюзов, автоматическое обновление ПО и т.п.
- Справочная информация.

1.2. Круг пользователей

Настоящий документ предназначен для разработчиков и пользователей ПО универсальный файловый шлюз ЭДО МБ.

1.3. Термины, определения и сокращения

В рамках настоящего документа используются следующие термины:

Термин	Определение
МБ	ПАО Московская Биржа.
УЦ	Удостоверяющий центр — ПАО Московская Биржа, осуществляющее выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законодательством.
ЭДО	Корпоративная система электронного документооборота Московской Биржи, предназначенная для обмена электронными документами в рамках корпоративной Торговой системы МБ.
ЭЦП	Электронная цифровая подпись — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

2. Краткий обзор системы ЭДО МБ

Система ЭДО МБ — это корпоративная система электронного документооборота, представляющая собой совокупность программного обеспечения, баз данных и вычислительных средств, а также организационно-технических мероприятий, обеспечивающих формирование электронных документов, подписание электронных документов ЭЦП и обмен электронными документами, подписанными ЭЦП.

Система ЭДО используется для передачи информации между приложениями торгово-расчетной инфраструктуры Московской Биржи.

С архитектурной точки зрения система ЭДО представляет собой стандартную электронную почту, в которую встроены средства криптографической защиты информации и управления открытыми ключами, а также скриптовый язык.

Для защиты передаваемой информации от раскрытия и подлога в системе ЭДО используется сертифицированное программное обеспечение шифрования и электронно-цифровой подписи СКЗИ "Валидата CSP " и ПК "Справочник сертификатов" АПК Клиент МБ (ПКЗИ СЭД МБ для нерезидентов).

Структурно система состоит из Центра ЭДО, расположенного в ПАО Московская Биржа, и почтовых сервисов ЭДО — EDIMailService, установленных в локальных сетях участников ЭДО (см. рис. 1).

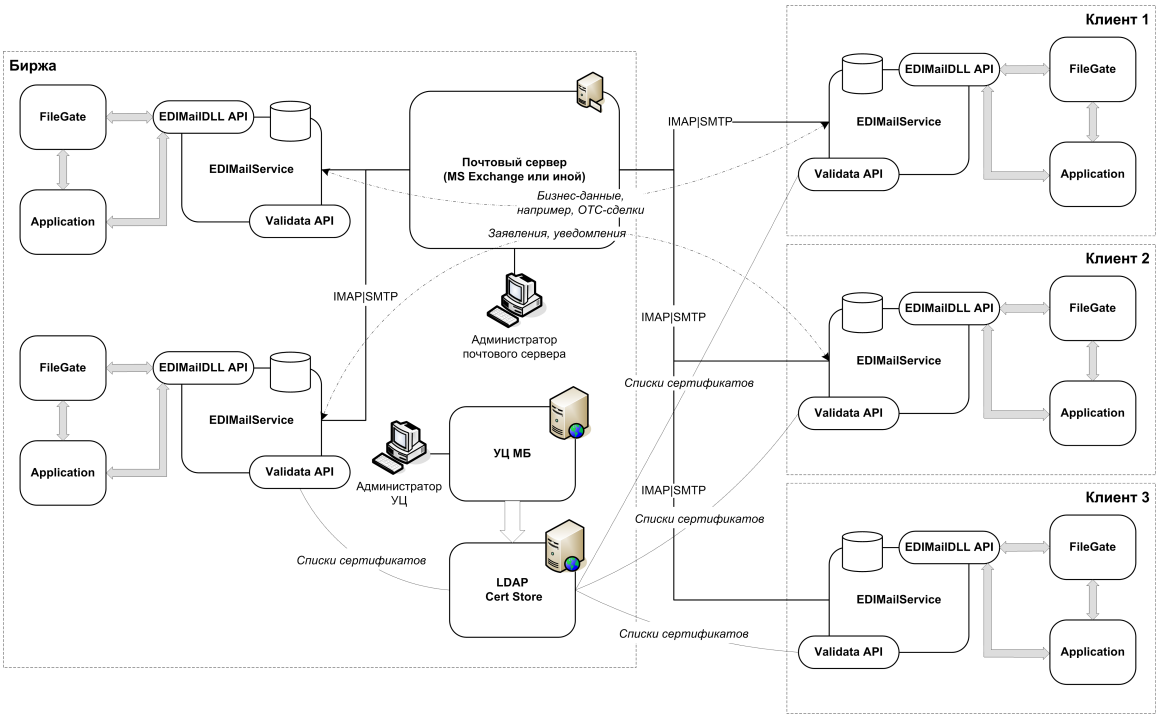

Рис. 1. Архитектура системы ЭДО МБ

Центр ЭДО включает в себя:

- Почтовый сервер ЭДО (MS Exchange);
- Удостоверяющий центр Московской Биржи;
- Хранилище сертификатов (LDAP Certificate Store).

В функции Центра ЭДО входит:

- Организация обмена электронными сообщениями между участниками ЭДО;
- Изготовление, хранение и распространение сертификатов открытых ключей подписей;
- Приостановка и возобновление действия сертификатов ключей подписей, а также их аннулирование;
- Ведение реестра Удостоверяющего центра;

EDIMailService играет роль почтового клиента, он непосредственно взаимодействует с почтовыми SMTP и IMAP серверами и выполняет криптографические операции. В его функции входит:

- Взаимодействие с почтовым сервером ЭДО, прием и отправку документов по электронной почте. Отправка сообщений производится по протоколу SMTP, прием сообщений может производиться по протоколам IMAP или POP3;
- Подпись документов ЭЦП отправителя с использованием СКЗИ "Валидата CSP" и шифрацию их на сертификатах получателя;
- Расшифровка полученных документов, проверка ЭЦП отправителя и проверка соответствия адреса отправителя реквизитам его ЭЦП;
- Взаимодействие с инфраструктурой системы ЭДО и ведение БД локальных справочников.

Для доступа к функциям EDIMailService (прием/отправка сообщений) клиентское приложение может использовать специальное API библиотеки EDIMailDLL.dll, либо воспользоваться интерфейсом обмена сообщениями через файловую систему с помощью файлового шлюза FileGate.exe.

3. Назначение и состав файлового шлюза

Универсальный файловый шлюз Московской Биржи предназначен для организации подключения приложений пользователей к системе ЭДО МБ посредством обмена файлами документов через файловую систему. Файловый шлюз используется для замены файлового шлюза ЭДО РТС в следующих сервисах Московской Биржи:

- Предоставление клиринговых отчетов срочного рынка Московской Биржи и Биржи СПб;
- Информационное взаимодействие с Клиентским центром Московской Биржи и АКБ НКЦ;
- Информационное взаимодействие с системой отчета о внебиржевых сделках (OTC-клиент).

Файловый шлюз состоит из следующих узлов и компонентов:

- Приложение EDIMailService.exe — обеспечивает взаимодействие клиентских приложений с криптографией и почтовыми серверами. Приложение EDIMailService может работать и как системная служба, и как консольное приложение.
- Библиотека EDIMailDLL.dll — предоставляет API для работы с EDIMailService (подробное описание библиотеки представлено в документе **EDIMail_API.pdf**).
- Файловый шлюз FileGate.exe — обеспечивает обработку документов в соответствии с правилами приема и отправки сообщений.
- Настроечные ini-файлы и скрипты.
- База данных пользователей ЭДО (export.sqlite3) для организации системы адресации и контроля полномочий отправителей.
- Локальный справочник сертификатов администратора ЭДО для проверки сообщений, рассылаемых от имени администратора ЭДО МБ.
- Необязательного сервера архивации сообщений. Служба EDIMailService может сохранять в базе данных на сервере архивации полученные документы, их ЭЦП и другие реквизиты в виде, удобном для последующего поиска.

Кроме перечисленных компонентов для работы файлового шлюза на рабочем месте необходимо установить стандартные криптографические компоненты ЭДО МБ:

- СКЗИ "Валидата".
- ПК "Справочник сертификатов" (АПК Клиент ММВБ) и настроенный профиль для локального справочника сертификатов.
- ПК "Справочник сертификатов" (ПКЗИ СЭД МБ) для работы с нерезидентами.

Также необходим действующий криптографический ключ и соответствующий ему сертификат, выпущенный удостоверяющим центром Московской Биржи. В ПК "Справочник сертификатов" должен быть настроен доступ к сетевому справочнику сертификатов (см. раздел 5.2, раздел 5.3).

4. Архитектура

С одной стороны шлюз поддерживает интерфейс взаимодействия со службой EDIMailService посредством вызова функций EDIMailDLL API, с другой стороны используется обмен файлами на уровне файловой системы (см. рис. 1).

Обмен между EDIMailService и файловым шлюзом осуществляется по проприетарному протоколу на базе XML-RPC. Настройки обмена содержатся в EdiMail.ini секция [xmlrpc] и не требуют дополнительной настройки со стороны клиента, при условии, что служба EDIMailService установлена на компьютере в единственном числе.

К службе EDIMAilService можно подключить как один, так и несколько файловых шлюзов. Каждый файловый шлюз должен иметь адрес ЭДО (код ЭДО + сервис ЭДО), внесенный в базу участников ЭДО. Допускается, но не рекомендуется запуск файловых шлюзов с одинаковым адресом ЭДО.

Файловый шлюз представляет собой консольное приложение и не умеет взаимодействовать с сервис-менеджером Windows, поэтому запустить его как службу и управлять им через оснастку "Панель управления" — "Система и безопасность" — "Администрирование" —"Службы" нельзя. Но служба EDIMailService может запускать и останавливать один или несколько файловых шлюзов одновременно с собственным запуском и остановкой. Если EDIMailService запускает файловые шлюзы вместе с собой, то окна файловых шлюзов размещается на невидимом десктопе, и диагностику их работы можно будет увидеть только в их логах.

4.1. Форматы файлового обмена

Формат файлового обмена определяет тип и структуру передаваемых файлов, а также правила их именования.

4.1.1. Формат "BBS"

С помощью этого формата можно передавать как текстовые, так и двоичные файлы. В одном сообщении может быть передано не более одного файла.

4.1.1.1. Структура файлов

Передаваемые файлы могут быть любыми. Содержание файлов не анализируется. Для передачи файлов требуется дополнительный файл-конверт. Он содержит служебную информацию, используемую шлюзом для идентификации получателя и темы сообщений. В сообщениях файл-конверт не передается.

При приеме и записи файла на диск также создается файл-конверт. Он содержит информацию об отправителе, теме сообщения, исходном имени файла, дате/времени и др.

Файл-конверт состоит из строк вида: **параметр: значение**. Между двоеточием и значением параметра возможны пробелы. Конверт может включать в себя следующие строки:

- **To:** - Адрес получателя. Обязательный параметр.
- **From:** - Адрес отправителя (игнорируется при формировании исходящего сообщения).
- **Subject:** - Тема сообщения. Поле заканчивается концом строки и может содержать пробелы.
- **Date/Time:** - Дата и время сообщения (игнорируется при формировании исходящего сообщения и формируется шлюзом при сохранении принятого сообщения). Формат даты YYYYMMDD/HHMMSS.
- **MsgID:** - Идентификатор криптопакета (игнорируется при формировании исходящего сообщения).
- **Type:** - Тип сообщения. Числовое шестнадцатеричное значение coretype, с префиксом 0x или без.
- **Filename:** - Имя принимаемого файла из сообщения (игнорируется при формировании исходящего сообщения и формируется шлюзом при сохранении принятого сообщения, если это имя у файла есть).

Пример файла конверта:

```
To: EMAIL@DCC.CSO
From: EMAIL@NPRTS.FILEGATE
Subject: MT599
Date/Time: 20131231/235901
MsgID: 6379128184795513456
Type: 0x1206
Filename: bbs49956
```

4.1.1.2. Правила именования файлов

Файлы сообщения в каталоге отсылки должны иметь произвольное одинаковое имя и расширение ".env" - для конверта и ".001" - для передаваемого файла.

Имя файла, отправляемого в сообщении, формируется путем отрезания у него расширения ".001".

Соответственно при приеме в приемный каталог записывается принятый файл с добавлением расширения ".001" и формируется файл-конверт с тем же именем и расширением ".env". При этом в файл конверта добавляется строка "**Filename:**" с именем файла из сообщения.

Если в каталоге приема файл уже существует, то в имя нового файла (между именем и расширением) вставляется порядковый номер в круглых скобках.

Файловый шлюз FileGate.exe умеет также работать и со старыми форматами обмена, которые использовались в EDIGATE. Для включения поддержки старых форматов используется ключ *compatibility_option* в секции правил приема/отправки сообщений. Если поддержка совместимости со старыми именами файлов включена, то шлюз работает по следующим правилам:

- Передаваться будут только файлы с именами формата bbsDDDDD.001 с конвертом bbsDDDDD.env, где D - произвольная цифра.
- Будет передаваться только содержимое файла, но не его имя.
- При приеме файлы также будут именоваться по вышеизложенной схеме, но, если в принятом сообщении имя файла есть, информация об этом появится в конверте (строка "**Filename:**").

4.1.2. Формат "MSG"

По этому формату передаются только текстовые сообщения.

4.1.2.1. Структура файлов

Первые несколько строк файла (заголовок) играют роль конверта и содержат служебную информацию для шлюза:

- **To:** - Адрес получателя. Обязательный параметр.
- **From:** - Адрес отправителя (игнорируется при отправке и формируется при приеме).
- **Subject:** - Тема сообщения. Поле заканчивается концом строки и может содержать пробелы.
- **Type:** - Тип сообщения. Числовое шестнадцатеричное значение coretype, с префиксом 0x или без.
- **Date:** - Дата и время сообщения (игнорируется при отправке и формируется при приеме). Формат даты YYYYMMDDHHMMSS.
- **Filename:** - Имя файла из сообщения (читается при отправке и формируется при приеме). Опциональное поле.

Далее следует содержимое файла. Передаче подлежит только содержимое, служебная информация с сообщением не отправляется.

Заголовок и содержимое отделяются пустой строкой, при этом при отправке допустимы любые имена параметров в заголовке, неизвестные параметры просто игнорируются. Началом содержимого считается первая строка после разделительной пустой строки.

Если включена опция поддержки совместимости со старым форматом конвертов, то набор параметров заголовка строго ограничен вышеперечисленными. Никакие другие имена параметров не допустимы. Любая строка, начинающаяся не с допустимого имени, будет считаться началом содержимого файла.

Пример файла сообщения:

```
To:EMAIL@FIRMM.DCC
From:EMAIL@TCRTS.FILEGATE
Type:0x1100
Subject:TEST
MsgID:xo7hOJACAAAT1u7WTwaIR73ZDq6mU59b
Date:20000329090406
:MT:598
:20:1234567890123456
:12:620
:77E:
|DICTID|01
|DATEFROM|<d>19981005<h>000000
```

4.1.2.2. Правила именования файлов

Файлы сообщения в каталоге отсылки могут иметь любое имя с обязательным расширением ".msg".

Имя файла, отправляемого в сообщении, формируется по следующим правилам:

- При отправке сообщения в заголовке файла ищется строка "**Filename:**". Если она есть, то имя файла в аттачменте задается этой строкой.
- Если такой строки нет, то имя файла в аттачменте — имя файла в каталоге отсылки без расширения ".msg".

В каталоге принятых сообщений файлы именуются путем добавления к имени файла из сообщения расширения ".msg ". При этом в заголовок добавляется строка "**Filename:**" с именем файла из сообщения.

Если в каталоге приема файл уже существует, то в имя нового файла (между именем и расширением) вставляется порядковый номер в круглых скобках.

Если включена поддержка совместимости со старыми именами файлов, то в каталоге отсылки имена файлов должны состоять из пяти цифр с обязательным расширением ".msg". В передаваемом сообщении имя файла не передается. Если в принимаемом сообщении имя файла присутствует, то оно записывается в заголовок, в параметр "**Filename:**", однако имя файла в приемном каталоге все равно будет состоять из пяти цифр и расширения ".msg".

4.1.3. Формат "FILE"

Этот формат предназначен для передачи произвольных файлов с сохранением их имени.

4.1.3.1. Структура файлов

Файлы могут быть любыми. Содержание файлов не анализируется.

4.1.3.2. Правила именования файлов

Имена отправляемых файлов должны удовлетворять следующим правилам:

- не содержат пробелов;
- символы стоящие после последней точки считаются расширением имени файла;
- расширение имени файла не должно быть более 3 символов.

Все отправляемые файлы помещаются в сообщение с тем же именем, с которым они были в каталоге отправки.

Все полученные файлы сохраняются в каталоге приема с тем именем, с которым они были отправлены.

Если в каталоге приема файл уже существует, то в имя нового файла (между именем и расширением) вставляется порядковый номер в круглых скобках.

4.1.3.3. Опция FIRM

Если для правила **FILE** на прием задан параметр **FIRM**, то входящие файлы именуются в соответствии с маской **YYMMDD-FIRM-NNNNN.EXT**, где

- **YYMMDD** - Дата прихода сообщения.
- **FIRM** - Пятибуквенный код компании, полученный из адреса отправителя (EMAIL@FIRM.USER).
- **NNNNN** - Порядковый номер файла. Предусмотрено два способа нумерации файлов:
  - Нумерация ведется в рамках одного правила для сообщений одного адресата. Нумерация сбрасывается при каждом переходе на новую дату.
  - Сквозная нумерация файлов по всем правилам. Нумерация не сбрасывается при переходе на новую дату и при перезапуске шлюза. Начальный номер для сквозной нумерации можно настраивать.

  Выбор способа нумерации осуществляется путем задания соответствующего значения параметра **FIRM** в FileGate.ini.
- **EXT** - Расширение полученного файла.

```
Примеры имен файлов:

030305-TROYM-00001.xls
001231-NPRTS-00002.msg,
000501-TCRTS-01234.doc
```

Опция **FIRM** может использоваться для ручной обработки полученных файлов, при необходимости сохранения сообщений от всех адресатов в одном каталоге с возможностью визуально определить отправителя и дату получения по имени файла.

4.2. Типовая структура каталогов шлюза

По умолчанию, дистрибутив устанавливает компоненты шлюза в папку Moscow Exchange\EDIMail на диск с операционной системой. Типовая структура каталогов в этой папке следующая:

- Moscow Exchange\EDIMail\Doc - документация.
- Moscow Exchange\EDIMail\EDIMailService - содержит исполняемые файлы модуля EDIMailService.
- Moscow Exchange\EDIMail\FileGate - содержит исполняемые файлы модуля FileGate.
- Moscow Exchange\EDIMail\FileGateMail - содержит каталоги для приема отправки сообщений.

- Moscow Exchange\EDIMail\ProgData - содержит файлы БД, служебные файлы и файлы логов.

4.3. Правила приема/отправки сообщений

Правила приема/отправки сообщений задают порядок обмена файлами между приложением и шлюзом, некоторые атрибуты сообщений при отправке и критерии отбора сообщений при приеме.

Правила задаются в настроечном ini-файле шлюза. Существуют основное (есть всегда) и дополнительные правила. Для каждого правила могут быть заданы:

- Формат файлового обмена.
- Входной и выходной каталоги. Если входной каталог не задан, то по данному правилу шлюз будет работать только на отсылку. Если не задан выходной, то шлюз работает только на прием.
- Атрибуты сообщения address, subject и coretype. Данные атрибуты определяют условия отбора входящих сообщений для правила, а также задают параметры исходящих сообщений.
- Другие опции, определяющие некоторую дополнительную функциональность файлового шлюза.

Если не задать ни одного правила, то используется основное правило по умолчанию: TYPE=BBS, IN=IN, OUT – отсутствует (правило только на прием).

4.4. Алгоритм работы

Шлюз работает в цикле (количество повторов может задаваться в ini-файле). Через заданные промежутки времени программа совершает следующие действия:

Отправка сообщений

1. Последовательный просмотр выходных каталогов основного правила и каждого дополнительного правила в порядке их задания в файле настроек на предмет нахождения в них файлов для отправки.
2. Отправка файлов на EDIMailService в соответствии с заданными условиями. Отправляемый файл автоматически подписывается электронной подписью отправителя с использованием СКЗИ "Валидата CSP", шифруется на сертификатах получателя, и в виде вложения почтового сообщения отправляется через почтовый сервер ЭДО МБ получателю.
3. Отправленные файлы удаляются из выходного каталога (или переносятся в каталог отправленных сообщений, если он задан в ini-файле) после получения подтверждения от EDIMailService о приеме сообщения. Если сообщение не может быть доставлено на EDIMailService, выдается сообщение об ошибке и файлы удаляются (или переносятся в каталог ошибок, если он задан).
4. В каталоге отосланных сообщений (SENT) и каталоге ошибок (ERROR) файлы именуются в соответствии с тем правилом, по которому они отправлялись.

Прием сообщений

1. Проверка очереди входящих почтовых сообщений от EDIMailService, и прием сообщений.
2. Последовательная проверка условий, заданных в дополнительных правилах (в порядке их перечисления в файле настроек). Если сообщение удовлетворяет какому-либо правилу (если условий несколько, то они должны выполняться одновременно – логическое "И"), то оно сохраняется во входной каталог в соответствии с заданным форматом. Если полученное сообщение удовлетворяет нескольким правилам, то оно будет сохранено в соответствии с первым из подходящих правил, после чего цикл переходит к обработке следующего сообщения.
3. Файл сохраняется в формате, заданном в правиле приема, а не в том формате, в котором он был отправлен.
4. Если не задано ни одного дополнительного правила или ни одно из условий, заданных в дополнительных правилах не удовлетворяется, то принятые файлы записываются в каталог, указанный в параметре IN основного правила в соответствии с форматом, указанном в параметре TYPE этого правила.

Удаление файлов из входного каталога должно производиться приложением, для которого эти файлы предназначены.

4.5. Поддержка ЭДО с нерезидентами

В системе ЭДО Московской Биржи поддерживается два типа сертификатов:

- **Квалифицированные сертификаты** - выпускаются УЦ Московской Биржи, аккредитованным Минкомсвязи РФ; используется сертифицированное СКЗИ "Валидата CSP", реализующее российский ГОСТ.
- **Неквалифицированные сертификаты** - выпускаются неаккредитованным УЦ Московской Биржи; используется криптопровайдер Microsoft CSP, входящий в состав Windows и реализующий алгоритм RSA.

Для сертифицированных СКЗИ существуют ограничения по ввозу/вывозу за пределы РФ, поэтому квалифицированные сертификаты используются только для ЭДО с резидентами РФ. Для ЭДО с нерезидентами РФ используются неквалифицированные сертификаты.

Соответственно, может быть настроено три варианта системы ЭДО:

- ЭДО с подписями/шифрованием ГОСТ (для работы с резидентами).
- ЭДО с подписями/шифрованием RSA (для работы с нерезидентами).
- ЭДО для работы с двумя криптосистемами одновременно, и возможностью посылать файлы резидентам с подписями/шифрованием ГОСТ и нерезидентам с подписями/шифрованием RSA.

Настройка осуществляется установкой соответствующего ПО (EDIMailService, FileGate) и криптографии:

- Для резидентов - устанавливается система в составе: EDIMailService, FileGate, СКЗИ "Валидата CSP", ПК "Справочник сертификатов" (АПК Клиент МБ).
- Для нерезидентов - устанавливается система в составе: EDIMailService, FileGate, СКЗИ "Валидата CSP", ПК "Справочник сертификатов" (ПКЗИ СЭД МБ).
- Для одновременной работы с резидентами и нерезидентами - устанавливается система в составе: EDIMailService, двух FileGate, СКЗИ "Валидата CSP", АПК Клиент МБ и ПКЗИ СЭД МБ.

5. Установка и запуск

Установка программного обеспечения выполняется с помощью дистрибутивов, находящихся на мини CD-ROM, полученном в УЦ Московской Биржи, либо скачанных со страницы сайта МБ: http://moex.com/s1292. Для каждого программного продукта имеются две версии дистрибутивов: 32-bit – для 32-х разрядных ОС и 64-bit – для 64-х разрядных ОС.

В случае самостоятельного скачивания дистрибутивов, для получения регистрационных данных, необходимых для установки ПО, следует обратиться к Администратору системы ЭДО.

5.1. Установка СКЗИ "Валидата CSP"

Установку СКЗИ "Валидата CSP" необходимо выполнять под учетной записью с правами Администратора.

Для начала установки запустить файл acsptls_x86.msi (acsptls_AMD64.msi), соответствующий разрядности установленной у вас ОС. Далее:

- Ввести выданный в УЦ Московской Биржи ключ установки (номер продукта).
- Выбрать тип установки "Выборочная". Обязательными для установки являются следующие компоненты:
  - "Биологический ДСЧ"
  - "Считыватель Съёмный Диск"
  - "Считыватель Реестр"
- НЕ УСТАНАВЛИВАТЬ компоненты "Валидата TLS".

После установки обязательно перезагрузить компьютер.

5.2. Установка ПК "Справочник сертификатов" с поддержкой квалифицированных сертификатов на основе российского криптографического ГОСТ (АПК Клиент МБ)

Перед установкой ПК "Справочник сертификатов" следует скопировать каталоги SPR и VDKeys с ключами и сертификатами на внешний носитель (флеш-диск) в корень.

Установку ПК "Справочник сертификатов" необходимо выполнять под учетной записью с правами Администратора.

Для начала установки запустить файл xcs_x86.msi.

Выбрать тип установки "Обычная".

После установки убедиться, что в **Программе конфигурации СКЗИ** на вкладке **Считыватели ключа** указан "Считыватель ключа с дискеты или USB flash".

При запуске ПК "Справочник сертификатов" выбрать в качестве сменного диска для инициализации ДСЧ диск с внешним носителем (флеш-диск), на котором находятся ключи.

Настроить путь к сетевому справочнику квалифицированных сертификатов. Для этого установить курсор на узел **Сетевые справочники сертификатов** и по правой клавише мышки выбрать пункт "Добавить сетевой справочник". В поле **LDAP сервер** прописать строку: ldap://vcert.pki.moex.com:50001/c=RU.

Указать в качестве каталога с резервными копиями справочника сертификатов скопированный на внешний носитель каталог SPR.

5.3. Установка ПК "Справочник сертификатов" с поддержкой неквалифицированных сертификатов на основе Microsoft CSP (ПКЗИ СЭД МБ)

Перед установкой ПК "Справочник сертификатов" следует скопировать каталоги SPR и VDKeys с ключами и сертификатами на внешний носитель (флеш-диск) в корень.

Установку ПК "Справочник сертификатов" необходимо выполнять под учетной записью с правами Администратора.

Для начала установки запустить файл rcs_x86.msi.

Выбрать тип установки "Обычная".

После установки убедиться, что в **Программе конфигурации СКЗИ** на вкладке **Считыватели ключа** указан "Считыватель ключа с дискеты или USB flash".

При запуске ПК "Справочник сертификатов" выбрать в качестве сменного диска для инициализации ДСЧ диск с внешним осителем (флеш-диск), на котором находятся ключи.

Настроить путь к сетевому справочнику неквалифицированных сертификатов. Для этого установить курсор на узел **Сетевые справочники сертификатов** и по правой клавише мышки выбрать пункт "Добавить сетевой справочник". В поле **LDAP сервер** прописать строку: ldap://vcert.pki.moex.com:50003/c=RU.

Указать в качестве каталога с резервными копиями справочника сертификатов скопированный на внешний носитель каталог SPR.

5.4. Проверка доступности сетевой инфраструктуры

По умолчанию служба EDIMailService устанавливается инсталлятором как система, работающая под логином LocalSystem. То, что СКЗИ и сеть нормально работают для интерактивного пользователя, не означает, что все необходимые настройки сделаны для логина LocalSystem. Поэтому перед установкой и запуском службы и файлового шлюза следует проверить (настроить) возможность загрузки ключей и доступность требуемых сетевых ресурсов. Для проверки можно воспользоваться утилитой PsExec из пакета PsTools.

5.4.1. Проверка загрузки ключей

Устройства загрузки ключей настраиваются программой конфигурации СКЗИ "Валидата CSP" индивидуально для каждого логина. Для настройки СКЗИ "Валидата CSP" под логином LocalSystem надо сделать следующее:

- Со страницы http://technet.microsoft.com/ru-ru/sysinternals/bb897553.aspx скачать утилиту PsExec и распаковать ее в рабочую папку.
- Запустить командную строку от имени администратора и перейти в рабочую папку, где лежит PsExec (команда cd c:\...).
- Ввести команду: @PsExec.exe -i -s -d "%ProgramFiles%\Validata\VDCSP\vdcsp_cfg.exe"
- В появившемся окне конфигурации СКЗИ настроить считыватели ключа и проверить правильное считывание ключей с помощью их копирования.

5.4.2. Проверка доступности серверов (портов)

Для проверки доступности серверов системы ЭДО можно воспользоваться все той же утилитой PsExec и стандартной утилитой Telnet. Следует учитывать, что изначально утилита Telnet в состав Windows 7 не входит, и ее придется доставить из меню Панель управления > Программы > Программы и компоненты > Включение или отключение компонентов Windows.

Для проверки доступности следует выполнить следующие действия:

- Запустить командную строку от имени администратора и перейти в рабочую папку, где лежит PsExec.
- Ввести команду: @PsExec.exe -i -s -d "cmd.exe".
- В появившейся командной строке ввести: telnet <имя сервера и номер порта> (например, telnet mars.moex.com 25).

При ответе, отличном от показанного на рис. 2 (не 220), пользователю следует обратиться к администратору своей локальной сети для организации доступа к требуемым сетевым ресурсам.

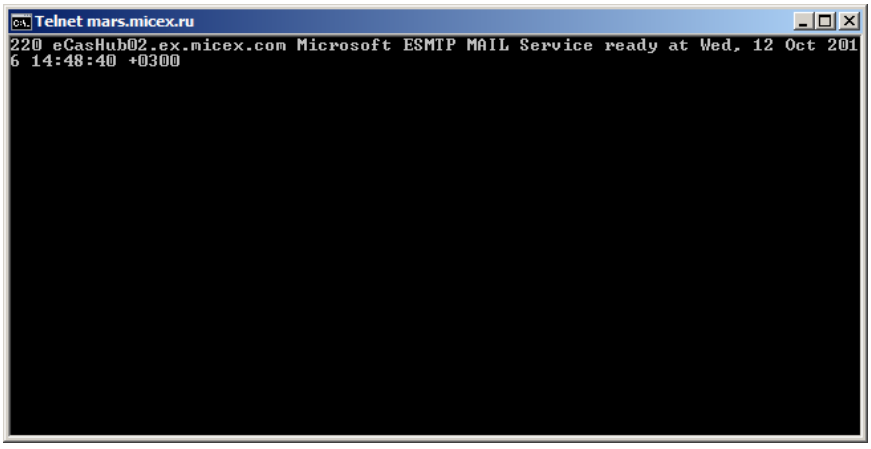

Рис. 2. Проверка доступности серверов

5.4.3. Проверка возможности SSL/TLS шифрования

В некоторых случаях у пользователя может не работать отправка сообщений ЭДО из-за того, что на его офисном маршрутизаторе запрещена возможность переключения протокола SMTP в режим работы по зашифрованному каналу (у файлового шлюза SSL/TLS шифрование включено).

Для проверки правильности работы сетевого оборудования можно воспользоваться все теми же утилитами PsExec и Telnet. Для проверки следует выполнить следующие действия:

- Запустить командную строку от имени администратора и перейти в рабочую папку, где лежит PsExec.
- Ввести команду: @PsExec.exe -i -s -d "cmd.exe".
- В появившейся командной строке ввести: telnet <имя сервера и номер порта> (например, telnet mars.moex.com 25).

- Ввести: HELO
- Ввести: STARTTLS

Ответ, отличный от показанного на рис. 3 (например, 500 5.5.1 Unrecognized command), означает, что шифрование на маршрутизаторе запрещено.

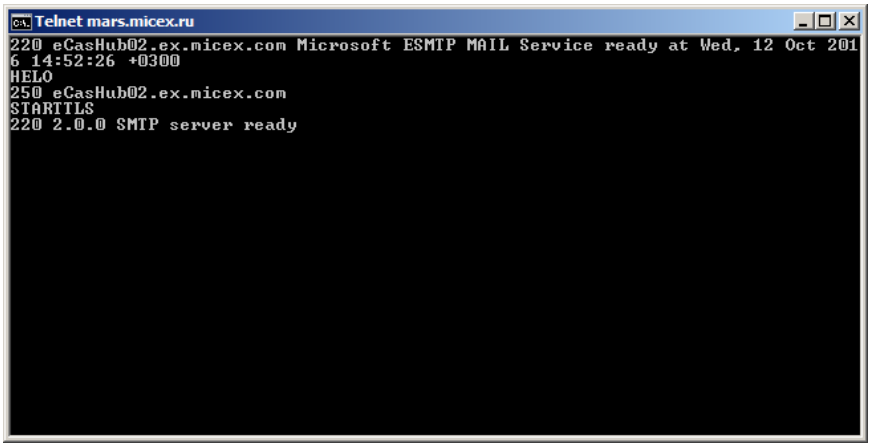

Рис. 3. Проверка возможности SSL/TLS шифрования

Есть два варианта решения проблемы:

- Перенастроить отправку сообщений так, чтобы не использовалось SSL/TLS шифрование. Для этого необходимо в файле FileGate.ini в секции с настройками почтового протокола для отправки сообщений (SMTP) выставить useTLS=no. Не рекомендуется использовать этот вариант, так как пароли/логины на доступ к почтовому ящику будут передаваться по сети в незашифрованном виде.
- Обратиться к системному администратору для настройки соответствующего сетевого оборудования.

5.5. Установка файлового шлюза

Установку файлового шлюза необходимо выполнять под учетной записью с правами Администратора. В зависимости от варианта устанавливаемой системы ЭДО (с шифрованием ГОСТ или RSA) необходимо использовать соответствующий инсталлятор:

- setup_MOEX_EDIMail_vx.x.x.exe - установка ЭДО с подписями/шифрованием ГОСТ.
- setup_MOEX_EDIMail_RSA_vx.x.x.exe - установка ЭДО с подписями/шифрованием RSA.
- setup_MOEX_EDIMail_MultiCS_vx.x.x.exe - установка ЭДО для работы с двумя криптосистемами одновременно.

При инсталляции устанавливаются все компоненты EDIMail, либо выполняется выборочная установка.

5.5.1. Полная установка

Для начала установки надо запустить файл соответствующего инсталлятора.

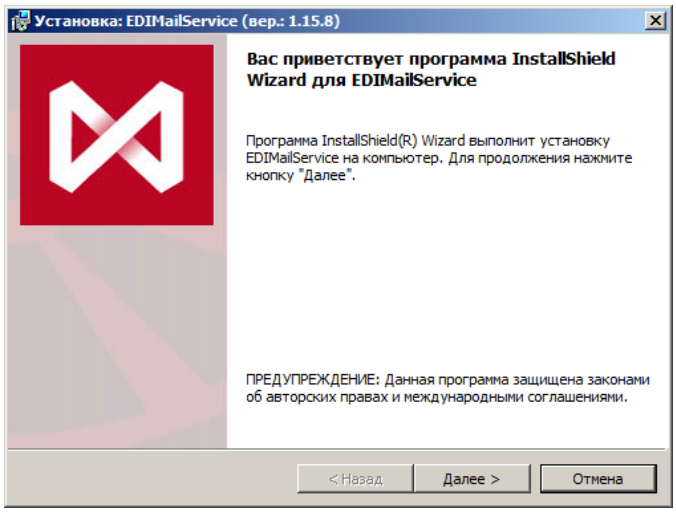

Рис. 4. Установка Шаг 1. Начало установки

Нажать кнопку **Далее** для продолжения установки.

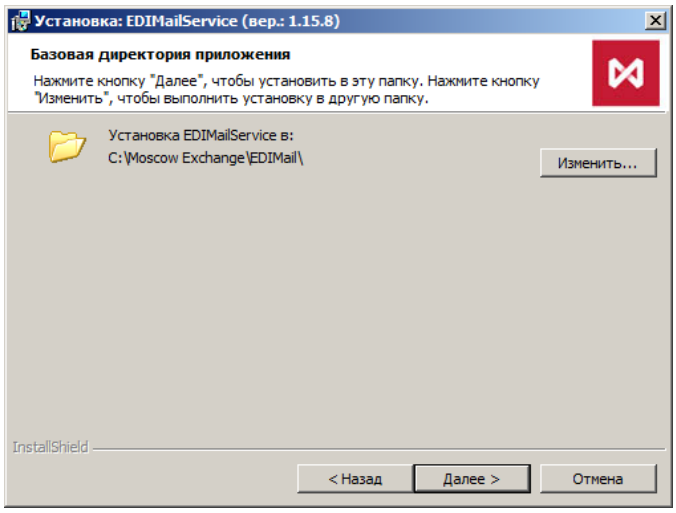

Рис. 5. Установка Шаг 2. Выбор каталогов для установки

По умолчанию, дистрибутив устанавливает приложения в папку Moscow Exchange\EDIMail на диск с операционной системой (см. раздел 4.2). При необходимости выбрать каталог для установки и нажать кнопку **Далее** для продолжения.

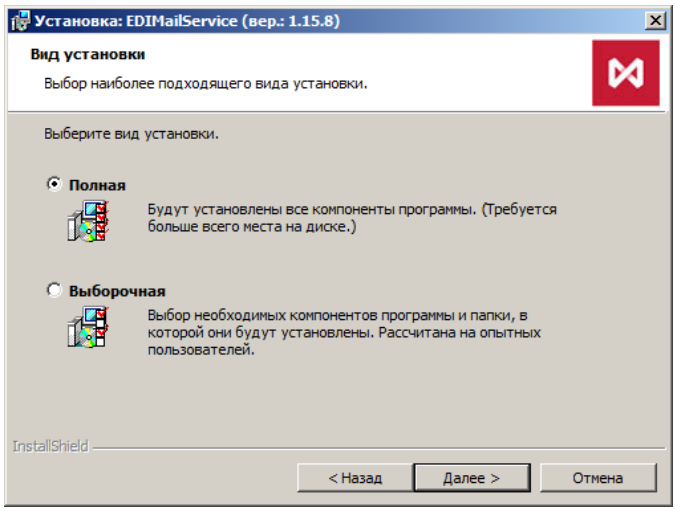

Рис. 6. Установка Шаг 3. Выбор вида установки

Выбрать вид установки **Полная** и нажать кнопку **Далее** для продолжения.

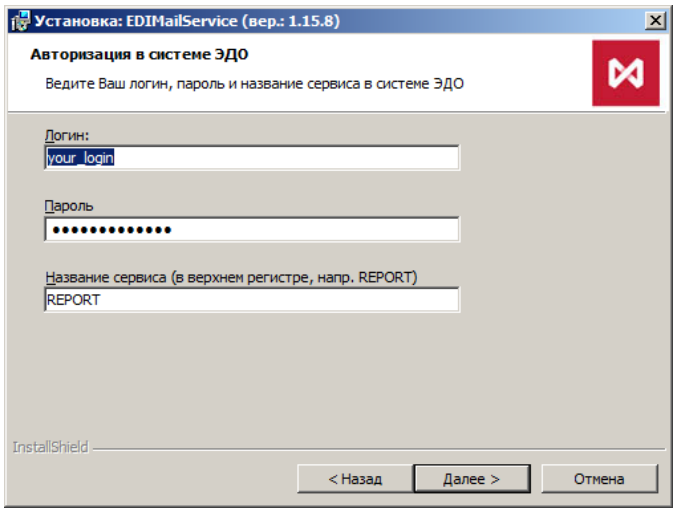

Рис. 7. Установка Шаг 4. Авторизация

Ввести логин, пароль, а также имя сервиса ЭДО и нажать кнопку **Далее** для продолжения установки.

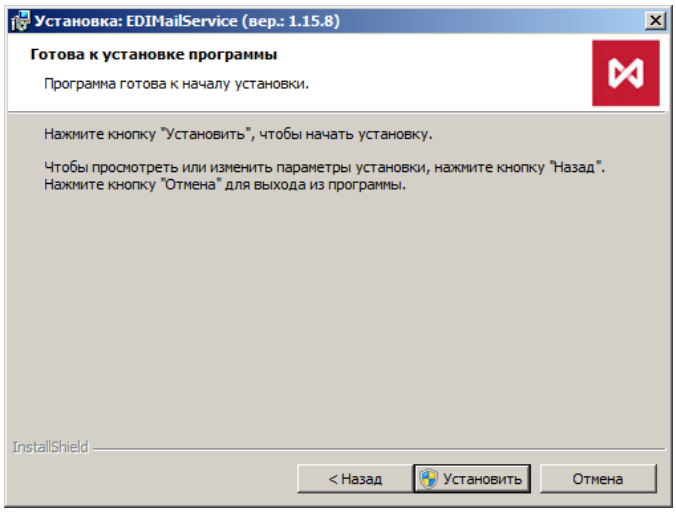

Рис. 8. Установка Шаг 5. Запуск процесса установки

Для запуска процесса установки нажать кнопку **Установить**.

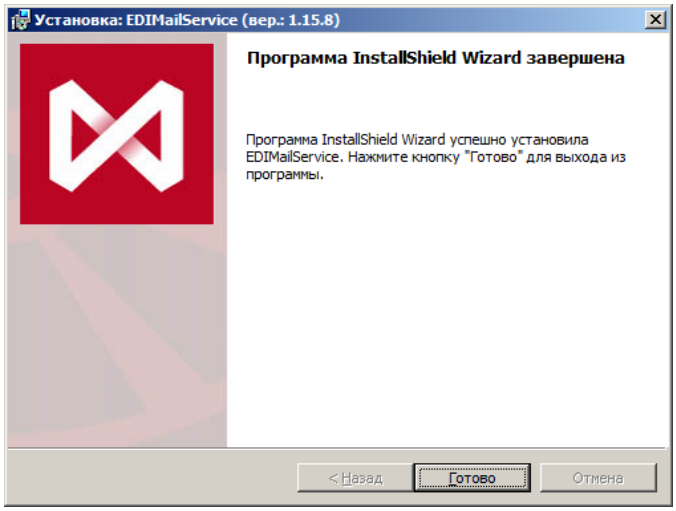

Рис. 9. Установка Шаг 6. Завершение установки

Нажать кнопку **Готово** для завершения установки.

5.5.2. Выборочная установка

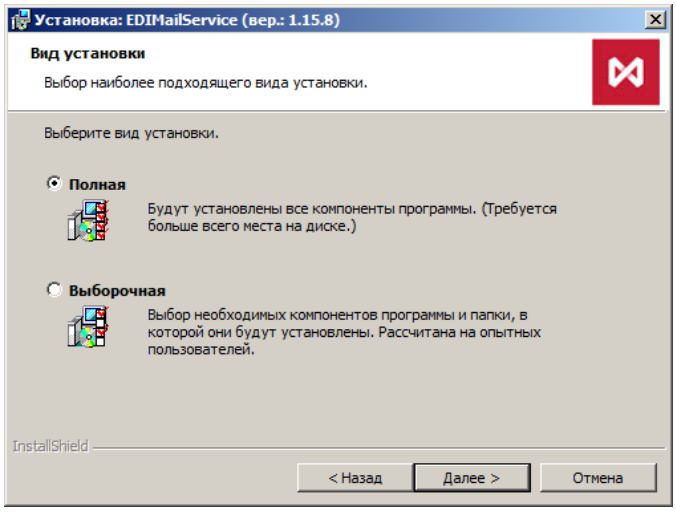

Рис. 10. Установка Шаг 3. Выбор вида установки

На третьем шаге выбрать вид установки **Выборочная** и нажать кнопку **Далее** для продолжения.

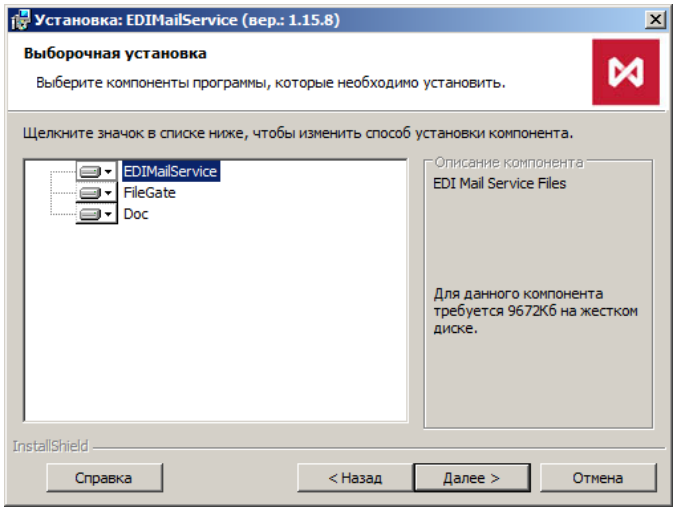

Рис. 11. Установка Шаг 4. Выбор компонентов

Выбрать компоненты, которые необходимо установить, и нажать кнопку **Далее** для продолжения установки.

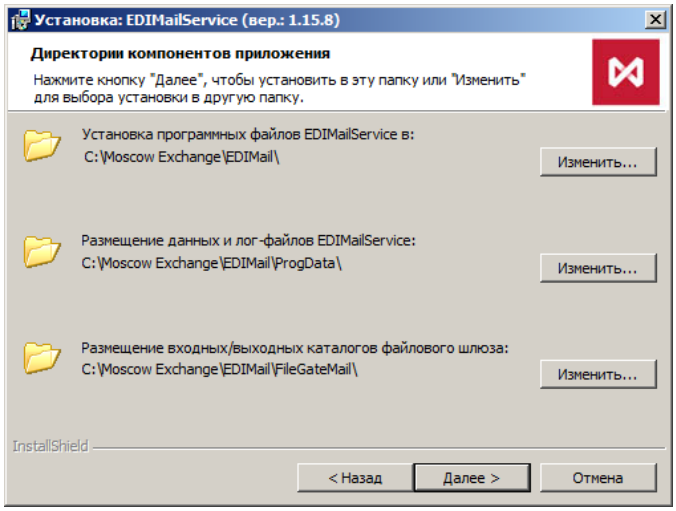

Рис. 12. Установка Шаг 5. Выбор каталогов для установки

По умолчанию, дистрибутив устанавливает приложения в папку Moscow Exchange\EDIMail на диск с операционной системой (см. раздел 4.2). При необходимости выбрать каталог для установки и нажать кнопку **Далее** для продолжения.

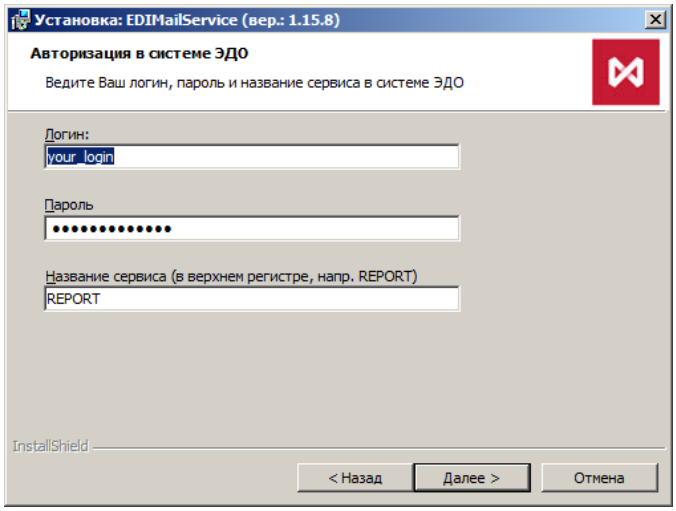

Рис. 13. Установка Шаг 6. Авторизация

Ввести логин, пароль, а также имя сервиса ЭДО и нажать кнопку **Далее** для продолжения установки.

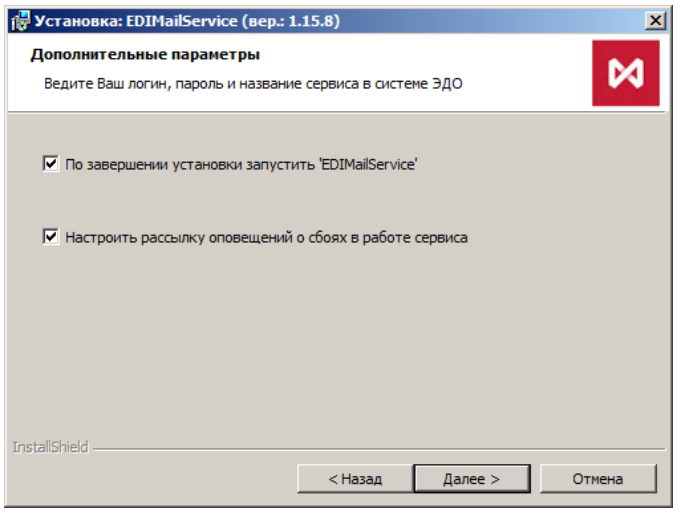

Рис. 14. Установка Шаг 7. Дополнительные параметры

В качестве дополнительных параметров можно указать:

- Признак автоматического запуска EDIMailService / FileGate после завершения установки.
- Признак включения механизма рассылки уведомлений (см. раздел 6.8). Если механизм включен, появится дополнительное окно для настройки параметров рассылки уведомлений.

Нажать кнопку **Далее** для продолжения установки.

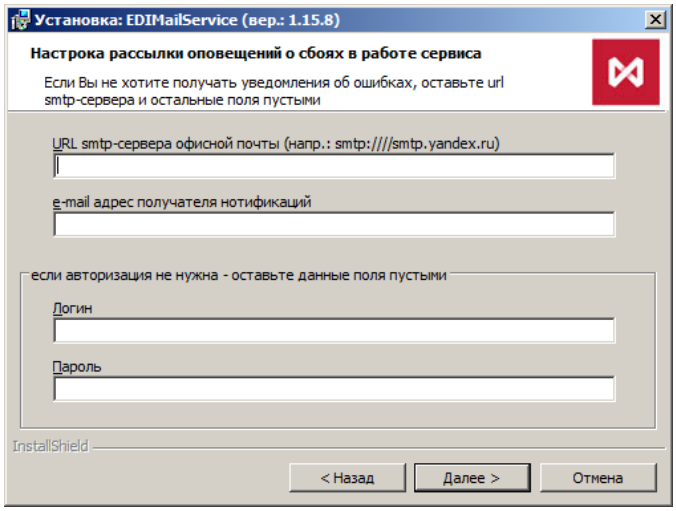

Рис. 15. Установка Шаг 8. Параметры рассылки уведомлений

Ввести параметры рассылки уведомлений. Параметр URL является обязательным, если он не задан, то уведомления рассылаться не будут. После завершения установки, введенные параметры записываются в настроечный файл EdiMail.ini в секцию [notification].

Внимание! Если после частичного заполнения полей диалога пользователь решил отказаться от настройки рассылки уведомлений, вернувшись назад и сняв признак "Настроить рассылку оповещений о сбоях в работе сервиса", то введенные значения все равно будут записаны в EdiMail.ini, что может привести к ошибкам в дальнейшем. Поэтому рекомендуется при отказе оставлять поля диалога пустыми.

Нажать кнопку **Далее** для продолжения установки.

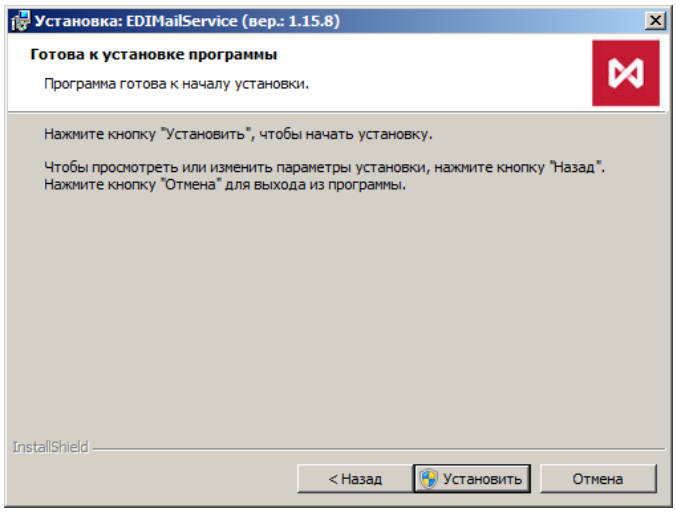

Рис. 16. Установка Шаг 9. Запуск процесса установки

Для запуска процесса установки нажать кнопку **Установить**.

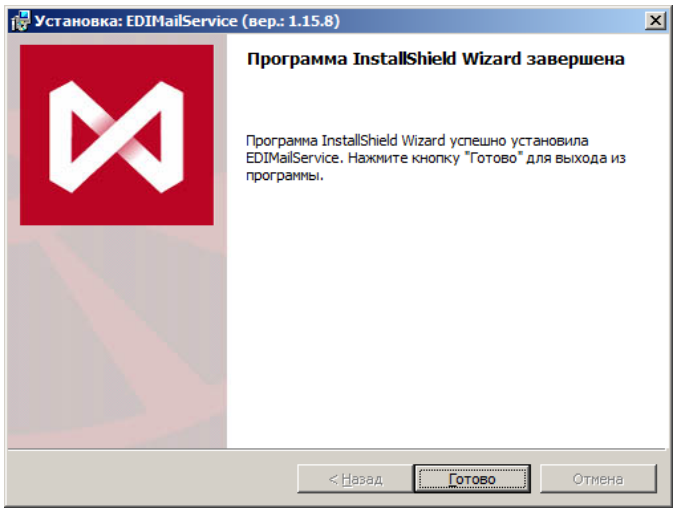

Рис. 17. Установка Шаг 10. Завершение установки

Нажать кнопку **Готово** для завершения установки.

5.6. Запуск

Для запуска файлового шлюза следует запустить службу EDIMailService. Служба зарегистрирована в системе под именем "EDI Mail Service" и запускается из Панель Управления > Система и безопасность > Администрирование > Службы > EDI Mail Service. Также ее можно запускать как приложение: Moscow Exchange\ EDIMail\ EDIMailService\ EDIMailService.exe.

Отдельный запуск FileGate.exe не требуется, так как по умолчанию дистрибутив устанавливает скрипт, который запускает шлюз вместе со службой.

6. Порядок работы с файловым шлюзом

6.1. Первоначальная настройка

После установки файлового шлюза необходимо произвести его ручную настройку.

6.1.1. Настройка EDIMailService

EDIMailService регистрируется как служба под именем "EDI Mail Service" в процессе инсталляции файлового шлюза. Одновременно на одном компьютере без специальной настройки может быть установлен и запущен только один экземпляр службы.

Если не требуется использование EDIMailService как службы, ее можно удалить из списка служб, запустив приложение EDIMailService.exe с ключом -remove. Для возврата EDIMailService в список служб нужно запустить EDIMailService.exe с ключом -install.

6.1.1.1. Настройка автоматического запуска шлюза

Приложение EDIMailService может запускать и останавливать файловый шлюз одновременно с собственным запуском и остановкой. Для запуска/остановки шлюза вместе EDIMailService нужно в файле настроек EdiMail.ini в секции [filegateDir] указать каталог, где размещен файловый шлюз.

```
[filegateDir]
Filegate1=C:\Moscow Exchange\EDIMail\FileGate\
```

Кроме этого, в секции [global] этого же ini-файла нужно задать скрипты, выполняемые при запуске и остановке EDIMailService.

```
[global]
onInit=function() { load("startup.js"); } – запуск шлюза из каталога, заданного в секции [filegateDir].
                                            Если запустить не удалось, EDIMailService останавливается
                                            и в лог пишется причина отказа.
onShutdown=function() {for (var i in pid) {kill(pid[i]);}} – остановка запущенного шлюза.
```

Пример скрипта startup.js запуска FileGate:

```
for (var i in iniFile.filegateDir) {
   var dir = cd(iniFile.filegateDir[i]);
   pid[i] = spawn("FileGate.exe", "/ini:FileGate.ini");
   cd (dir);
   if (pid[i] == 0 || pid[i] == -1) {
      var msg = "no FileGate.exe in "+iniFile.filegateDir[i];
      for (var ii in pid) {
         if (ii != i)
            kill(pid[ii]);
      }
      throw msg;
   }
   sleep(3000000);
   if (procstat(pid[i]) != "active") {
     msg = "Can't start FileGate in "+iniFile.filegateDir[i];
     for (var ii in pid) {
        if (ii != i)
           kill(pid[ii]);
     }
     throw msg;
   }
}
```

По умолчанию EDIMailService уже устанавливается из дистрибутива так, что она может запускать и останавливать файловый шлюз одновременно с собственным запуском и остановкой. Для того чтобы отказаться от автоматического запуска шлюза, следует закомментировать вышеописанные параметры в файле настроек.

6.1.1.2. Настройка архивации

При необходимости EDIMailService может производить архивацию принятых и отправленных файлов, их ЭЦП, адресов отправки и другой служебной информации в базе данных для удобства последующего поиска документов. В настоящий момент поддерживается архивирование в базах данных Microsoft SQL Server 2005, Microsoft SQL Server 2008 и последующих версий.

Для включения функции архивирования с помощью Microsoft SQL Server 2005 необходимо в файле настроек EdiMail.ini в секции [archive] задать параметры архивации.

```
[archive]
type=MSSQL2005 – тип SQL сервера.
connection=Driver={SQL Server};Server=sql.server.office.com; Database=edi_archive;Uid=edi_admin;
                                  Pwd=12345 – строка соединения с базой данных.
```

```
cs_collation=SQL_Latin1_General_Cp1251_CS_AS – способ сортировки/сравнения букв, с учетом регистра букв.
ci_collation=SQL_Latin1_General_Cp1251_CI_AS – способ сортировки/сравнения букв, без учета регистра букв.
direction=both – какие сообщения архивировать (in/out/both).
```

Система архивации сама создаст необходимые таблицы. При необходимости можно самостоятельно добавить в базу данных таблицы и индексы, добавить столбцы в существующие таблицы. Удалять столбцы из существующих таблиц или сами таблицы нельзя.

При использовании нескольких экземпляров EDIMailService, можно все экземпляры настроить на работу с одной и той же базой данных для получения единого архива документов.

При реализации архивирования с помощью Microsoft SQL Server 2008 и выше появилась возможность хранить большие данные не в полях таблиц, а в виде отдельных файлов в специальных папках файловой системы под управлением SQL-сервера. Это позволяет получить выигрыш в скорости обработки больших данных, и, что более важно, реализовать эффективную антивирусную проверку принимаемых документов.

Для включения функции архивирования с помощью Microsoft SQL Server 2008 необходимо в файле настроек EdiMail.ini в секции [archive] задать тип сервера и строку соединения с БД, а также выполнить настройки на самом SQL-сервере (stream mode, по умолчанию не настроено).

6.1.2. Настройка FileGate

6.1.2.1. Настройка соединения с почтовым сервером

Отправка сообщений производится по протоколу SMTP, прием сообщений может производиться по протоколам IMAP или POP3. Если почтовый ящик используется не только для работы ЭДО, а еще и для обычного почтового обмена, или с почтовым ящиком работают одновременно несколько файловых шлюзов с разных компьютеров, то для приема следует использовать протокол IMAP. Если почтовый ящик выделен монопольно для использования ЭДО с данного компьютера, то рекомендуется использовать более быстрый POP3.

Настройки соединения с почтовым сервером хранятся в файле FileGate.ini.

```
[FileGate]
recvparam=IMAP – имя секции с настройками соединения  для приема сообщений (IMAP или POP3).
sendparam=SMTP – имя секции с настройками соединения  для отправки сообщений (SMTP).

[IMAP]
login = <логин для IMAP>
password = <пароль для IMAP>
url=imap://mars.moex.com:993 – адрес почтового сервера ЭДО.
TLScheck = host
verbose = yes
TLSfirst = yes
useTLS = use

[SMTP]
login = <логин для SMTP>
password = <пароль для SMTP>
url=smtp://mars.moex.com:25 – адрес почтового сервера ЭДО.
TLScheck = host
verbose = yes
TLSfirst = no
useTLS = try
```

Чтобы переключиться с использования IMAP на использование POP3 следует:

- Остановить EDIMailService.
- Удалить файл mail.sqlite3 из рабочей папки EDIMailService. Это обусловлено тем, что при работе по IMAP протоколу EDIMailService запоминает, что почту, приходящую на почтовый ящик, надо раскладывать по папкам внутри почтового ящика. При переходе с IMAP на POP3 запомненные действия продолжат выполняться, тем самым сделав входящую почту недоступной, т.к. POP3 не может достать ее из папок внутри почтового ящика. В силу этих обстоятельств, при переходе с IMAP на POP3 необходимо удалить файл mail.sqlite3 из рабочего каталога EDIMailService.
- В настроечном файле FileGate.ini заменить подстроку "imap:" на "pop3:", "imaps:" на "pop3s:". Если в конце заменяемых строк стоит двоеточие и число (номер порта), то число 143 заменить на 110, а 993 на 995. Если в той же секции есть ключ port=, то заменить номер порта по тому же правилу.

6.1.2.2. Настройка правил приема/отправки сообщений

Правила задаются в настроечном файле FileGate.ini. Существуют основное (есть всегда) и дополнительные правила. Для каждого правила могут быть заданы:

- Формат файлового обмена.
- Входной и выходной каталоги. Если входной каталог не задан, то по данному правилу шлюз будет работать только на отсылку. Если не задан выходной, то шлюз работает только на прием.

- Атрибуты сообщения address, subject и coretype. Данные атрибуты определяют условия отбора входящих сообщений для правила, а также задают параметры исходящих сообщений.
- Другие опции, определяющие некоторую дополнительную функциональность файлового шлюза.

Если не задать ни одного правила, то используется основное правило по умолчанию: TYPE=BBS, IN=IN, OUT – отсутствует (правило только на прием).

Пример:

```
[RULES]
RULE2=RULE2
RULE1=RULE1
MAIN=MAIN

[MAIN]
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\MAIN_OUT\
IN=C:\Moscow Exchange\EDIMail\FileGateMail\MAIN_IN\
TYPE=BBS

[RULE1]
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_MOEX\
ADDRESS=EMAIL@NPRTS.REPORT
TYPE=FILE

[RULE2]
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_FO_REPORT\
ADDRESS=EMAIL@FORTS.REPORT
TYPE=FILE
```

6.1.2.3. Настройка параметров идентификации шлюза и криптографии

Каждый участник идентифицируется в системе ЭДО МБ своим адресом ЭДО. Адрес ЭДО представляет собой связку "Код ЭДО" (биржевой тикер, аналог кода РТС) плюс "Код сервиса ЭДО" — обязательный добавочный код, который соответствует Email-адресу участника в ЭДО МБ. Каждый файловый шлюз должен иметь адрес ЭДО, внесенный в базу участников ЭДО. Допускается, но не рекомендуется запуск нескольких шлюзов с одинаковым адресом ЭДО.

Параметры идентификации шлюза задаются в двух файлах: FileGate.ini и EDIMailSrvs.ini.

FileGate.ini

```
[IMAP]
service = <код сервиса ЭДО>
login =
password =
url=imap://mars.moex.com:993
TLScheck = host
verbose = yes
TLSfirst = yes
useTLS = use
```

EDIMailSrvs.ini (в нем же задаются параметры криптографии)

```
[self]
ticker = <код ЭДО>
service= <код сервиса ЭДО>

[crypto]
local= "file://C:\Users\AppData\Roaming\Validata\xcs\local.gdbm" – путь до файла локального
справочника сертификатов ЭДО. В случае установки нескольких шлюзов, каждый шлюз должен использовать
свой отдельный файл справочника.
pse= "pse://C:\Users\AppData\Roaming\Validata\xcs\local.pse" – путь до файла персонального
справочника ЭДО.
validata= xpki1.dll – имя и путь к файлу библиотеки, используемой для работы криптографии.
```

6.2. Использование нескольких файловых шлюзов

К сервису EDIMAilService можно подключить как один, так и несколько файловых шлюзов. Для установки второго экземпляра шлюза не рекомендуется использовать штатный инсталлятор, так как он попытается повторно установить службу EDIMAilService. Вместо этого следует скопировать папку с файловым шлюзом (Moscow Exchange\EDIMail\FileGate) в другое место, назовем его для примера C:\FileGate2, и дополнительно настроить реквизиты файлового шлюза (см. раздел 6.1.2).

Для запуска второго экземпляра файлового шлюза вместе со службой EDIMailService нужно в файле настроек EdiMail.ini в секции [filegateDir] добавить строку с указанием местонахождения скопированного файлового шлюза.

В нашем примере:

```
[filegateDir]
Filegate1=C:\Moscow Exchange\EDIMail\FileGate\
Filegate2=C:\FileGate2\
```

6.3. Гарантированная доставка

Файловый шлюз реализует механизм гарантированной доставки на базе квитанций, предусмотренных DSN расширением SMTP протокола, описанного в стандарте rfc 3461 [https://tools.ietf.org/html/rfc3461], и сообщений Message Disposition Notification, генерируемых EDIMailService в соответствии с стандартом rfc 3798 [https://tools.ietf.org/html/rfc3798]. Служба EDIMailService обеспечивает своевременное удаление почтовых квитанций из ящика пользователя.

6.4. Автоматическое обновление ПО

По умолчанию обновления базы пользователей ЭДО и программного обеспечения ЭДО периодически рассылаются по электронной почте в виде служебного письма, подписанного ЭЦП Администратора ЭДО МБ. После проверки подписи Администратора и целостности письма и всех его вложений, выполняется автоматическая установка обновлений.

Если по каким-либо причинам пользователь хочет самостоятельно скачивать и устанавливать эти обновления, то автоматическую установку обновлений можно запретить. Для этого в файле настроек службы EDIMailService (EdiMail.ini) следует создать секцию [permission] со следующими ключами:

```
[permission]
updateUsersDB=false – запрет на автоматическое обновление базы данных пользователей ЭДО.
updateEDIMailService=false – запрет на автоматическое обновление ПО EDIMailService
                             (включая FileGate.exe и EDIMailDLL.dll).
noUpdate=true – запрет любых изменений.
```

Если понадобится разрешить автоматическое обновление, следует заменить false на true или удалить соответствующую строку (всю секцию).

6.5. Работа с общими папками (shared folders)

Для того чтобы файловый шлюз забирал для отсылки или выкладывал принятые файлы в общие папки на некотором файл-сервере, необходимо дополнительно настроить доступ сервиса EDIMailService к этим общим папкам. Это можно сделать двумя способами:

- С использованием UNC имен файлов (UNC — uniform naming convention).
- С использованием имен сетевых дисков.

При использовании UNC имен файлов перед запуском FileGate.exe нужно задать логин и пароль для доступа к общим папкам. Для этого в начало скрипта startup.js (см. раздел 6.1.1) нужно добавить вызовы функции system по числу используемых общих папок вида:

```
system("net use \\\\SERVER\\FOLDER /u:USER PASSWORD");, где
SERVER –  имя файл-сервера;
FOLDER –  имя общей папки на файл-сервере SERVER;
USER – имя пользователя файл-сервера;
PASSWORD – пароль пользователя на файл-сервере.
```

Имена общих папок в правилах приема/отправки сообщений в этом случае должны указываться по правилам UNC \\SERVER \FOLDER\...

При использовании имен сетевых дисков в начало скрипта startup.js (см. раздел 6.1.1) нужно добавить вызовы функции system по числу используемых сетевых дисков вида:

```
system("net use DISK: \\\\SERVER\\FOLDER /u:USER PASSWORD");, где
DISK –  буква используемого сетевого диска;
SERVER –  имя файл-сервера;
FOLDER –  имя общей папки на файл-сервере SERVER;
USER – имя пользователя файл-сервера;
PASSWORD – пароль пользователя на файл-сервере.
```

Имена общих папок в правилах приема/отправки сообщений в этом случае должны указываться с помощью сетевых дисков DISK:\...

При работе с общими папками и сетевыми дисками следует иметь ввиду, что назначение сетевых дисков, даже указанное в команде net use с ключом /permanent, действует только в пределах интерактивной logon-сессии, и поэтому не распространяется на службу EDIMailService, даже если она работает под тем же логином, что и вы в интерактивной сессии. Служба может использовать только назначения, сделанные с помощью функции system("net use ...").

6.6. Запуск под разными пользователями

Рекомендуется запускать EDIMailService и файловые шлюзы под одним пользователем, для которого установлены сертификаты/ключи. В случае хранения ключей в реестре Windows запуск под разными пользователями не допускается. В случае хранения ключей на съемном диске использование разных учетных записей допустимо.

6.7. Совместимость с файловым шлюзом ЭДО РТС

Файловый шлюз совместим со старым шлюзом ЭДО РТС на уровне правил приема/отправки сообщений и формата конверта. Обмен сообщениями между двумя почтовыми иерархиями невозможен.

6.8. Рассылка уведомлений

EDIMailService может по результатам запуска или проверки состояния своих клиентов, таких как файловый шлюз, производить генерацию и рассылку по электронной почте соответствующих уведомлений для системного администратора, поддерживающего работу EDIMailService. Настройки для рассылки e-mail уведомлений задаются при инсталляции шлюза и хранятся в EdiMail.ini в секции [notification]. Секция является опциональной, если она отсутствует или закомментирована, никакие уведомления не посылаются.

По умолчанию устанавливаемые дистрибутивом скрипты посылают уведомления в следующих случаях:

- использование неверного адреса в настройках FileGate;
- невозможности запустить FileGate в указанных в секции [filegateDir] папках;
- если в ходе работы процесс FileGate был завершен и автоматически перезапущен.

Шлюз FileGate также может по мере написания сообщений об ошибках в лог производить генерацию и рассылку по электронной почте соответствующих уведомлений для системного администратора ЭДО. Настройки для рассылки e-mail уведомлений задаются в FileGate.ini в секции [notification]. Секция является опциональной, если она отсутствует или закомментирована, никакие уведомления не посылаются.

6.9. Архивация отправляемых и принимаемых файлов в отдельную папку с помощью JavaScript

Приложение EDIMailService может при отправке и приеме сообщений производить архивацию отправляемых и принимаемых файлов и их ЭЦП в заданный каталог архива. Для этого в EDIMailService используются JavaScript-события onMsgSend и onMsgReceive, срабатывающие, соответственно, при отправке и приеме сообщений, и функция для обработки сообщений — файл gs-functions.js.

Пример gs-functions.js:

```
var ini;

if (!String.prototype.format) {
  String.prototype.format = function() {
    var args = arguments;
    return this.replace(/{(\d+)}/g, function(match, number) {
      return typeof args[number] != 'undefined'
        ? args[number]
        : match
      ;
    });
  };
}

function parseINIString(data) {
    var regex = {
        section: /^\s*\[\s*([^\]]*)\s*\]\s*$/,
        param: /^\s*([\w\.\-\_]+)\s*=\s*(.*?)\s*$/,
        comment: /^\s*;.*$/
    };
    var value = {};
    var lines = data.replace(/\/\/\/\//g,"//").split(/\r\n|\r|\n/);
    var section = null;
    lines.forEach(function(line){
        if(regex.comment.test(line)){
            return;
        }else if(regex.param.test(line)){
            var match = line.match(regex.param);
            if(section){
                value[section][match[1]] = match[2];
            }else{
                value[match[1].toLowerCase()] = match[2];
            }
        }else if(regex.section.test(line)){
            var match = line.match(regex.section);
            value[match[1].toLowerCase()] = {};
            section = match[1].toLowerCase();
        };
```

```
    });
    return value;
}

function archiveMsg(msg, archRootDir)
{
    var now = new Date();
    msg.needDecrypt = true;
    var archDir = archRootDir+'\\'+now.getFullYear()+'-'+pad2(now.getMonth()+1)+'-'+pad2
                  (now.getDate());
    mkdirstruct(archDir);
    var attNumMax = msg.numStreams;
    for (var attNum = 1; attNum <= attNumMax; ++attNum)
    {
 illegalChar = /[\\/\:\*\?"<>|]/g;
        var fileName = pad2(now.getHours())+'.'+pad2(now.getMinutes())+'
                       '+msg.attachmentFilename(attNum).replace(illegalChar,'_');
        for (var cnt = 0;; ++cnt)
        {
            if (cnt)
                var newFileName = fileName+'('+cnt.toString()+')';
            else
                newFileName = fileName;
            try {
                stat(archDir+'\\'+newFileName);
            }
            catch (err)
            {
  try {stat(archDir+'\\'+newFileName+'.signature');}
  catch (err)
  {
      var stream = new EDIMailStream(archDir+'\\'+newFileName, 'wb', '');
      var sig_stream = new EDIMailStream(archDir+'\\'+newFileName+'.signature', 'wb', '');
      break;
  }
            }
        }
        msg.attachToStream(attNum, stream);
 if (msg.signatureToStream)
     msg.signatureToStream(attNum, sig_stream);
        stream.dispose();
 sig_stream.dispose();
 system('process_archive.bat '+archDir+'\\'+newFileName+' '+archDir+'\\'+newFileName+'.signature');
    }
}

function processOutMsg(msg, archRootDir)
{
    archiveMsg(msg, archRootDir+"\\out\\"+get_to_addr(msg));
}

function processInMsg(msg, archRootDir)
{
    if(msg.numStreams > 0)
    {
        archiveMsg(msg, archRootDir+"\\in\\"+get_from_addr(msg));
    }
    else // if(false) //temporary disabled
    {
        print('Found '+msg.numStreams+' streams in the message');
        var errorMsg = 'Can\'t decrypt message \''+msg.subject+ '\'
                       ' +get_from_addr(msg) + ' -> ' +get_to_addr(msg);
        print( errorMsg );
        var serviceFolder = iniFile.executable.substring (0, iniFile.executable.lastIndexOf('\\')+1);
 print('Service Folder: '+serviceFolder);
        var file;
        try {
            file = new EDIMailStream(serviceFolder+'EdiMail.ini', 'rt', '');
        }
        catch (err) { print('Could not open EdiMail.ini'); return false; }
        ini = parseINIString(file.readText(file.length));
        file.dispose();
```

```
        var backup = new EDIMailStream('', '');
        msg.toStream(backup);
        var url=null;
        if (ini.notification) // && false) temporarily disabled
        {
     print('Notification pending');
            try {url = new EDIMailURL(ini.notification.url, "ini.notification");} catch(err)
                      { print('Failed to construct EDIMailURL'); return false; }
            var notif = new EDIMailMessage("ini.notification");
            notif.addRecepient(ini.notification.address);
            notif.subject = notif.subject.format(iniFile.hostname);
            notif.text = errorMsg;
            notif.postTo(url);
            print('Sent error report');
            notif.dispose();
            url.dispose();
        }
        try {var dir_status = stat(archRootDir);} catch (err) { print ('Archive directory does
                              not exist'); backup.dispose(); return false;}
        if (dir_status.mode & 0x4000)
        {
            var now = new Date();
            var fileName = 'failed_decrypt_'+now.getFullYear()+'-'+pad2(now.getMonth()+1)+'.
                          '+pad2(now.getDate())+'_'+pad2(now.getHours())+'.'+pad2(now.getMinutes());
            for (var cnt = 0;; ++cnt)
            {
                if (cnt)
                    var newFileName = fileName+' ('+cnt.toString()+')';
                else
                    newFileName = fileName;
                try {
                    stat(archRootDir+'\\'+newFileName);
                }
                catch (err)
                {
                    var stream = new EDIMailStream(archRootDir+'\\'+newFileName, 'wb', '');
                    backup.seek(0,0);
                    backup.writeToStream(stream);
                    stream.dispose();
             print('Dumped undecryptable message to '+ archRootDir+'\\'+newFileName);
                    break;
                }
            }
        }
        backup.dispose();
    }
}

function get_to_addr(msg) {
    try {
        var rfc2047_mail_address = msg.recepients; /* это строка - адрес получателя по rfc2047,
                                                      например "Good company <post@firm.com>" */
        var email = /[^<>]*<(.*)>/.exec(rfc2047_mail_address)[1]; /* это мы выделили e-mail, например
                                                      "post@firm.com" из адреса в формате rfc2047 */
        var service = msg.recepientsService.split(",")[0].toUpperCase(); /* сервис ЭДО, которому
                                                         посылается сообщение, например "REPORT" */
        var addr = new EDIMailAddress("", service, email); /* торговый код адресата в сообщении
          отсутствует, чтобы его узнать по имеющимся сервису ЭДО и e-mail, делаем этот объект */
        var ticker = addr.ticker.split("\n")[0].toUpperCase();
        var edo_addr = ticker+"."+service; /* собрали ЭДО адрес, например, FIRM.REPORT */
        addr.dispose(); /* объект адрес больше не нужен, его надо явно уничтожить */
        return edo_addr;
    }
    catch (err) { return "UNKNOWN";}
}

function get_from_addr(msg)
{
    try {
        var sender = msg.ediMailSender;
        var ticker = sender.ticker.split("\n")[0].toUpperCase();
        var service = sender.service.split("\n")[0].toUpperCase();
```

```
        return ticker+"."+service;
    }
    catch (err) { return "UNKNOWN";}
}


function mkdirstruct(path) {
    var folderList = path.split('\\');
    var current = '';
    for (var folder in folderList) {
        if (current)
            current += '\\'+folderList[folder];
        else
            current = folderList[folder] + '\\';
        try {
            var test = stat(current);
            if (test.mode & 0x8000) {
                /* указанный путь существует, но это файл, а не каталог, и это наверное,
                   ошибка – надо обработать */
  print('File exists here; directory expected: '+current);
            }
        }
        catch (err) {
            /* ошибка в stat – текущий путь не существует, делаем его */
     print('mkdir '+current);
            mkdir(current);
        }
    }
}

function pad2(number) {
     return (number < 10 && number >=0 ? '0' : '') + number
}
```

Что делает скрипт:

- получает объект — адрес отправителя ЭДО сообщения (sender);
- при отсутствии делает подкаталог в заданной архивной папке (archRootDir), который называется по торговому коду отправителя (sender.ticker);
- для каждого прикрепленного к сообщению ЭДО файла выясняет его имя (fileName) и создает архивный файл (stream) с этим именем; если имя уже используется, то добавляет к имени последовательные целые числа в скобках, пока не получится уникальное имя (newFileName);
- сохраняет содержимое прикрепленного файла в архивный файл (attachToStream).

Для настройки архивации необходимо:

- в файл EDIMailSrvs.ini каждого FileGate в секции [global] нужно задать параметры:
  - onInit=function(){load('gs-functions.js');} - для загрузки и компиляции скрипта, чтобы не делать это каждый раз;
  - onMsgSend = function(msg) { processOutMsg(msg, 'C:\\Archive'); } - архивация при отправке; 'C:\\Archive' - папка, в которую нужно записывать архив;
  - onMsgReceive = function(msg) { processInMsg(msg, 'C:\\Archive'); } - архивация при получении.
- поместить gs-functions.js в каталог, где хранятся стандартные скрипты — startup.js, watchdog.js (по умолчанию, C:\Moscow Exchange\EDIMail\ProgData); если скрипт хранится в каком-то другом каталоге, путь к нему должен быть задан при загрузке скрипта (например, onInit=function(){load('C:\\scripts\\gs-functions.js');}.

6.10. Обработка сообщений с не расшифрованными файлами

По умолчанию, если EDIMailService / FileGate не могут расшифровать прикрепленный к сообщению ЭДО файл или проверить его ЭЦП, то сообщение отклоняется (отправитель информируется о том, что сообщение не получено) с соответствующей записью в логе. При необходимости EDIMailService можно настроить таким образом, чтобы обработка таких ситуаций была более информативной. Например, производить архивацию некорректных файлов с уведомлением об этом администратора системы. Данный функционал реализован в виде скрипта cant_decrypt_msg.js:

```
var archRootDir = "D:\\ME_EDIMail\\Bin\\arch";
var ini;
if (!String.prototype.format) {
String.prototype.format = function() {
var args = arguments;
return this.replace(/{(\d+)}/g, function(match, number) {
```

```
return typeof args[number] != 'undefined'
? args[number]
: match
;
});
};
}
function parseINIString(data) {
var regex = {
section: /^\s*\[\s*([^\]]*)\s*\]\s*$/,
param: /^\s*([\w\.\-\_]+)\s*=\s*(.*?)\s*$/,
comment: /^\s*;.*$/
};
var value = {};
var lines = data.replace(/\/\/\/\//g,"//").split(/\r\n|\r|\n/);
var section = null;
lines.forEach(function(line){
if(regex.comment.test(line)){
return;
}else if(regex.param.test(line)){
var match = line.match(regex.param);
if(section){
value[section][match[1]] = match[2];
}else{
value[match[1].toLowerCase()] = match[2];
}
}else if(regex.section.test(line)){
var match = line.match(regex.section);
value[match[1].toLowerCase()] = {};
section = match[1].toLowerCase();
};
});
return value;
}
function cant_decrypt_msg(msg)
{
var serviceFolder = iniFile.executable.substring (0, iniFile.executable.lastIndexOf('\\')+1);
var file;
try {
file = new EDIMailStream(serviceFolder+'EDIMail.ini', 'rt', '');
}
catch (err) { return false; }
ini = parseINIString(file.readText(file.length));
file.dispose();
var backup = new EDIMailStream('', '');
msg.toStream(backup);
var url=null;
if (iniFile.notification && msg.numStreams == 0)
{
try {url = new EDIMailURL(ini.notification.url, "ini.notification");} catch(err) { return false; }
var notif = new EDIMailMessage("ini.notification");
notif.addRecepient(ini.notification.address);
notif.subject = notif.subject.format(iniFile.hostname);
notif.text = notif.text.format("Can't decrypt message from "+msg.ediMailSender.fullname+"
sender ticker "+msg.ediMailSender.ticker+" received by FileGate", iniFile.filegateDir[i]);
notif.postTo(url);
notif.dispose();
url.dispose();
try {var dir_status = stat(archDir);} catch (err) { print ('Archive directory does not exist');
backup.dispose(); return false;}
if (dir_status.mode & 0x4000)
{
var now = new Date();
var fileName = 'cant_decrypt_'+now.getFullYear()+'.'+(now.getMonth()+1)+'.'+now.getDate()
+'_'+now.getHours()+'.'+now.getMinutes();
for (var cnt = 0;; ++cnt)
{
if (cnt)
var newFileName = fileName+' ('+cnt.toString()+')';
else
newFileName = fileName;
try {
```

```
stat(archDir+'\\'+newFileName);
}
catch (err)
{
var stream = new EDIMailStream(archDir+'\\'+newFileName, 'wb', '');
backup.seek(0,0);
backup.writeToStream(stream);
stream.dispose();
break;
}
}
}
}
backup.dispose();
}
```

Что делает скрипт:

- посылается сообщение администратору EDIMailService/FileGate, адрес которого указан в EDIMail.ini, секция [notification];
- принятый файл записывается в архив для последующего анализа с именем, содержащем дату/время прихода по шаблону: cant_decrypt_ГГГГ.ММ.ДД_ЧЧ.ММ (номер).

Для настройки данного функционала необходимо:

- в файл EDIMailSrvs.ini каждого FileGate вставить секцию [global] с параметром onMsgReceive=function(msg) {load(cant_decrypt_msg.js); cant_decrypt_msg(msg); }
- поместить скрипт cant_decrypt_msg.js в тот же каталог, что и уже имеющиеся скрипты startup.js, watchdog.js (например, C:\Moscow Exchange\EDIMail\ProgData);
- отредактировать cant_decrypt_msg.js, заменив в начале файла строку var archRootDir = "D:\\ME_EDIMail\\Bin\\arch"; на путь до каталога, куда будут складываться нерасшифрованные файлы; если каталога не существует, это не будет ошибкой, просто файлы архивироваться не будут;
- настроить в EDIMail.ini секцию [notification] с параметрами уведомлений.

6.11. Настройка сквозной нумерации принимаемых файлов

Если для правила **FILE** на прием задан параметр **FIRM**, то входящие файлы именуются в соответствии с маской **YYMMDD-FIRM-NNNNN.EXT**, где

- **YYMMDD** — Дата прихода сообщения.
- **FIRM** — Пятибуквенный код компании, полученный из адреса отправителя (EMAIL@FIRM.USER).
- **NNNNN** — Порядковый номер файла. Предусмотрено два способа нумерации файлов:
  - Нумерация ведется в рамках одного правила для сообщений одного адресата. Нумерация сбрасывается при каждом переходе на новую дату.
  - Сквозная нумерация файлов по всем правилам. Нумерация не сбрасывается при переходе на новую дату и при перезапуске шлюза. Начальный номер для сквозной нумерации можно настраивать.

  Выбор способа нумерации осуществляется путем задания соответствующего значения параметра FIRM в FileGate.ini.

Для настройки начального номера необходимо выполнить следующие действия:

- Скопировать нижеследующий фрагмент текста в файл set_start_num.js, находящийся в той же папке, что и startup.js и watchdog.js

```
--------------------------- Начало set_start_num.js -------------------------
var filegatePath = "C:\My filegate\FileGate.ini"; /* full path to FileGate.ini in use */
var startNum = 123; /* starting number for received file enumeration */
var maxDate = "18 Febrary 2014 14:52"; /* Date for start number patch applay */
if (new Date() < new Date(maxDate) ) {
var num = parseInt(readParam("infilenum "+filegatePath));
if (!num || num < startNum)
{
saveParam("infilenum "+filegatePath, startNum.toString());
}
}
--------------------------- Конец set_start_num.js --------------------------
```

- Отредактировать первые три строки файла set_start_num.js следующим образом:

- в **filegatePath** указать полный путь до файла FileGate.ini, используемого нашим файловым шлюзом, в кавычках, с сохранением регистра букв.
- в **startNum** указать число, с которого должна начинаться нумерация.
- **maxDate** — защита от постоянного выполнения установки номера файла в начальное значение. Установка будет выполнена только до указанной даты/времени. Указать текущие дата/время плюс 2-3 минуты.

- В файле EDIMailSrvs.ini добавить секцию [global] с параметром onInit=function() { load("set_start_num.js"); }.
- Запустить EDIMailService/FileGate.
- После запуска отредактировать EDIMailSrvs.ini, удалив оттуда строку onInit=function() { load("set_start_num.js"); }.

6.12. Задание паролей для почтовых ящиков и пин кодов для носителей криптоключей с помощью JavaScript функций

По умолчанию пароли для доступа к почтовым ящикам хранятся в открытом виде в ini-файле шлюза (FileGate.ini), что не является корректным. Для исправления ситуации в EDIMailService реализована возможность указывать в ini-файле вместо пароля функцию, которая будет возвращать значение пароля, хранящегося в другом месте. Сама функция реализована в виде скрипта get_password.js:

```
function get_password()
{
  system('passwd.bat password.txt'); /* Run passwd.bat batch file with password.txt as paramater -
                                        here we assume that passwd.bat file creates password.txt */
  var file = EDIMailStream('password.txt', 'rt', ''); /* open file with modified password
                                                         for reading as text file */
  var passwd = file.readText(file.length); /* read password.txt content */
  file.dispose(); /* close file password.txt */
  system('del password.txt'); /* delete password.txt */
  passwd = passwd.split(''); /* Strings is immutable so we need to convert string to char array */
  for (var i in passwd) {
     if (i & 1) {/* on odd i */
        passwd[i] = String.fromCharCode(passwd[i].charCodeAt(0) + 1);  /* add 1 to character
                                                                          code at odd index */
     } else { /* on even i */
        passwd[i] = String.fromCharCode(passwd[i].charCodeAt(0) - 1);  /* subtract 1 from character
                                                                          code at even index */
     }
  }
  passwd = passwd.join(''); /* Convert character array to string */
  return passwd;
}
```

Для настройки данного функционала необходимо:

- в файл EDIMailSrvs.ini каждого FileGate вставить в секцию [global] параметр onInit=function(){load('get_password.js');} для загрузки и компиляции скрипта, чтобы не делать это каждый раз, когда потребуется пароль;
- поместить скрипт get_password.js в тот же каталог, что и уже имеющиеся скрипты startup.js, watchdog.js (по умолчанию, C:\Moscow Exchange\EDIMail\ProgData); если скрипт хранится в каком-то другом каталоге, путь к нему должен быть задан при загрузке скрипта (например, onInit=function(){load('c:\\scripts\\get_password.js');});
- в FileGate.ini вместо пароля задать функцию: password=function(){return get_password();}

В случаях когда криптоключи хранятся на носителях, требующих для доступа ввода пин кода/пароля, система ЭДО работоспособна только, если EDIMailService запущена как консольное приложение, где есть интерактивная сессия и можно ввести код/пароль. Для EDIMailService, работающей в режиме службы, такой возможности не было.

В текущей версии системы данная проблема решена путем добавления в настройки криптографии шлюза (файл EDIMailSrvs.ini, секция [crypto] или [crypto_rsa]) дополнительного параметра pin, в котором можно указать в открытом виде пин код/пароль, либо JavaScript функцию, которая будет получать пароль из другого места. Сама функция может быть реализована, по аналоги с вышеописанным, в виде скрипта и загружаться при инициализации шлюза.

7. Файлы настройки

Для настройки работы файлового шлюза используются следующие файлы:

- EdiMail.ini — файл содержит параметры настройки сервиса EDIMailService;
- FileGate.ini — файл содержит параметры настройки файлового шлюза (FileGate.exe);
- EDIMailSrvs.ini — файл содержит реквизиты дополнительной идентификации файлового шлюза и параметры криптографии.

7.1. Файл EdiMail.ini

Файл содержит параметры настройки сервиса EDIMailService. Ниже приведено описание секций EdiMail.ini.

[dirs]

В секции задается имя рабочего каталога. Рабочий каталог должен иметь доступ на чтение/запись для пользователя, от имени которого работает EDIMailService. В других местах .ini-файла на рабочий каталог можно ссылаться с помощью макро $(workdir).

Ключ	Описание
work_dir	Полный путь до рабочего каталога.

[crypto]

В секции задаются параметры криптографии с шифрованием ГОСТ. Данные параметры используются только для верификации данных, принятых от администратора ЭДО. Каждый файловый шлюз задает параметры криптографии отдельно, в своем ini-файле (EDIMailSrvs.ini).

Ключ	Описание
validata	Имя или полный путь к файлу библиотеки, используемой для работы криптографии с шифрованием ГОСТ (xpki1.dll). Если параметр не задан, то сервис будет работать в режиме "без криптографии".
url	Url LDAP сервера. Внимание: В старых версиях из-за того, что "//" являлся началом комментария в ini-файле, их надо было удваивать "////", сейчас это не требуется. Обязательный параметр.
base_dn	Ветка на LDAP сервере, используемая для хранения неквалифицированных сертификатов. Обязательный параметр.
pse	Полный путь до файла персонального справочника администратора ЭДО (файл обычно имеет расширение ".pse"). Обязательный параметр для режима с криптографией.
local	Полный путь до файла локального справочника сертификатов администратора ЭДО (файл обычно имеет расширение ".gdbm"). Обязательный параметр для режима с криптографией.
cleartext	Разрешение принимать незашифрованные и неподписанные файлы. • "allow" - принимать разрешено, • "deny" -запрещено. Значения по умолчанию: • для режима без криптографии - "allow", • для сервиса в режиме с криптографией - "deny". НЕ РЕКОМЕНДУЕТСЯ ИЗМЕНЯТЬ НАСТРОЙКУ ЭТОГО ПАРАМЕТРА ПО УМОЛЧАНИЮ.
updateCRL	Задержка в часах между последовательными попытками обновить список отозванных сертификатов для всех подключенных в момент запроса клиентов сервиса. Может указываться с дробными долями. Значение по умолчанию "2.0".
search	Поиск сертификатов для адресов получателей сообщений ЭДО. • "strict" - должны быть найдены сертификаты для всех получателей сообщения, • "weak" -должен быть найден хотя бы один сертификат. Значения по умолчанию "strict".
keyregex	Шаблон для выделения в dn сертификата информации, однозначно идентифицирующей организацию (в РФ - это ИНН организации). Значения по умолчанию "INN\s*=\s*(\d+),".
nameregex	Шаблон для выделения в dn сертификата информации, однозначно идентифицирующей наименование организации. Значения по умолчанию "O\s*=\s*([^,]+),".

[crypto_rsa]

В секции задаются параметры криптографии с шифрованием RSA. Данные параметры используются только для верификации данных, принятых от администратора ЭДО. Каждый файловый шлюз задает параметры криптографии отдельно, в своем ini-файле (EDIMailSrvs.ini).

Ключ	Описание
validata	Имя или полный путь к файлу библиотеки, используемой для работы криптографии с шифрованием RSA (rpki1.dll). Если параметр не задан, то сервис будет работать в режиме "без криптографии".
url	Url LDAP сервера. Внимание: В старых версиях из-за того, что "//" являлся началом комментария в ini-файле, их надо было удваивать "////", сейчас это не требуется. Обязательный параметр.
base_dn	Ветка на LDAP сервере, используемая для хранения неквалифицированных сертификатов. Обязательный параметр.
pse	Полный путь до файла персонального справочника администратора ЭДО (файл обычно имеет расширение ".pse"). Обязательный параметр для режима с криптографией.
local	Полный путь до файла локального справочника сертификатов администратора ЭДО (файл обычно имеет расширение ".gdbm"). Обязательный параметр для режима с криптографией.
cleartext	Разрешение принимать незашифрованные и неподписанные файлы. • "allow" - принимать разрешено, • "deny" - запрещено. Значения по умолчанию: • для режима без криптографии - "allow", • для сервиса в режиме с криптографией - "deny". НЕ РЕКОМЕНДУЕТСЯ ИЗМЕНЯТЬ НАСТРОЙКУ ЭТОГО ПАРАМЕТРА ПО УМОЛЧАНИЮ.
updateCRL	Задержка в часах между последовательными попытками обновить список отозванных сертификатов для всех подключенных в момент запроса клиентов сервиса. Может указываться с дробными долями. Значение по умолчанию "2.0".
search	Поиск сертификатов для адресов получателей сообщений ЭДО. • "strict" - должны быть найдены сертификаты для всех получателей сообщения, • "weak" - должен быть найден хотя бы один сертификат. Значения по умолчанию "strict".
keyregex	Шаблон для выделения в dn сертификата информации, однозначно идентифицирующей организацию (в РФ - это ИНН организации). Значения по умолчанию "INN\s*=\s*(\d+),".
nameregex	Шаблон для выделения в dn сертификата информации, однозначно идентифицирующей наименование организации. Значения по умолчанию "O\s*=\s*([^,]+),".

[imap]

В секции задаются параметры доставки сообщений. EDIMailService доставляет сообщения ЭДО из общей почтовой папки Inbox до папки, соответствующей имени сервиса ЭДО, откуда ее уже забирают клиенты сервиса. Частота выполнения этих операций задается в данной секции.

Ключ	Описание
tick	Время в секундах между опросами папки Inbox. Можно указывать значения с долями секунд. Значение по умолчанию "60.0".

[messages]

В секции задаются параметры обработки сообщений.

EDIMailService может обрабатывать сообщения "пачками". Размер "пачки" ограничивается размером буфера почтового сервера и памяти, доступной самому EDIMailService. Чем больше размер пачки, тем быстрее работает доставка сообщений, но тем больше требуется памяти EDIMailService. По умолчанию используется размер пачки в 50 сообщений.

Все почтовые серверы ограничивают размер принимаемых сообщений. Как правило, это ограничение выясняется при попытке послать большое сообщение — после приема его части, как правило, нескольких мегабайт, сервер заканчивает прием с ошибкой.

Чтобы не сталкиваться с такой ситуацией, EDIMailService сам проверяет размер файла, который необходимо отправить. По умолчанию стоит лимит в 6МБ, который соответствует установленному по умолчанию лимиту MS Exchange в 10МБ с учетом накладных расходов на почтовые кодировки.

Ключ	Описание
max	Максимальное количество сообщений, обрабатываемых за один запрос. Значение по умолчанию "50".
size	Максимальный размер прикрепляемого к сообщению файла в байтах. Значение по умолчанию "6291456".
collect	Максимальное число сообщений, отдаваемых за один запрос к службе. Все эти сообщения занимают память службы, при большом числе параллельно работающих клиентов этот параметр следует уменьшать. Значение по умолчанию "5".
onconfirm	Что делать с уже полученным сообщением, получение которого уже подтверждено. Может принимать значения: • "delete" - удалить (всегда делается для протокола POP3), • "keep" - сохранить (возможно, только для протокола IMAP; создает возможность параллельной работы 2-х шлюзов на разных машинах, получающих одно и то же). Значения по умолчанию "delete".
mdn	Нужно ли посылать уведомления об обработке сообщений ЭДО, которые используются механизмом гарантированной доставки. Может принимать значения: • "skip" - не посылать, • "send" - посылать всегда, • "ask" - решение о посылке принимает клиент EDIMailService (т.е. файловый шлюз или ЦЭД). Значения по умолчанию "ask".
unknownnotification	Удалять ли из почтовой папки "входящие" квитанции (notification) от неизвестных источников. Может принимать значения: • "delete" - удалять, • "keep" - сохранять. Значения по умолчанию "delete".
return_path	Нужно ли выполнять проверку, что заголовок Disposition-Notification-To соответствует заголовку Return-Path (см https://tools.ietf.org/html/rfc3798). Может принимать значения: • "nocheck" - не проверять соответствие, • "check" - проверять соответствие. Значения по умолчанию "nocheck".

[xmlrpc]

В секции задаются настройки протокола XM-RPC. По данному протоколу EDIMailService взаимодействует с клиентами (шлюзами). Все параметры имеют значения по умолчанию, поэтому эта секция является необязательной.

Ключ	Описание
port	TCP порт, на котором работает EDIMailService. Значение по умолчанию "12069".
verbose	Выдавать диагностику работы RPC. Может принимать значения: • "1" - да, • "0" - нет. Значения по умолчанию "0".
introspection	Включить функцию интроспекции RPC. Функция интроспекции позволяет получить перечень выполняемых сервером функций. Может принимать значения: • "1" - да, • "0" - нет.

Ключ	Описание
	Значения по умолчанию "1".
tick	Квант времени в секундах, выделяемый для обработки RPC запросов. Значение по умолчанию "0.7".
clients	Максимальное число параллельно работающих клиентов сервиса EDIMailService (приложений FileGate). Значение по умолчанию "6".

[maintenance]

В секции задаются параметры очистки почтовых папок. Удаляются сообщения, соответствующие любому из нижеприведенных критериев.

Ключ	Описание
older	Целое число дней. Все сообщения, с датой, отстоящей от сегодняшней на указанное число дней, будут удалены. Значение по умолчанию "30".
maxsize	Целое число мегабайт. Сообщения упорядочиваются по датам, и подсчитывается их суммарный размер, начиная с сегодняшней даты. Как только размер превысит указанный предел, все участвующие в подсчете сообщения будут оставлены, остальные будут удалены. Значение по умолчанию "1000".
tick	Задержка в часах между последовательными выполнениями операций очистки. Значение по умолчанию "24".

[global]

В секции задаются параметры настройки реакции на события. EDIMailService может выполнять скрипты на языке JavaScript при наступлении определенных событий. На данный момент предусмотрена обработка следующих событий:

- Запуск EDIMailService (событие onInit);
- Остановка EDIMailService (событие onShutdown);
- Ошибка при обновлении списка отозванных сертификатов (событие onCRLUpdate);
- Периодический запуск скриптов по истечении определенного интервала времени (события onEveryNNNsec, onEveryNNNmin, onEveryNNNhour).

При наступлении события выполняется одноименная событию функция, определенная в глобальном контексте JavaScript. Содержимое глобального контекста JavaScript можно задавать в секции.

Ключ	Описание
onInit	Функция JavaScript без параметров, выполняемая при запуске EDIMailService.
onShutdown	Функция JavaScript без параметров, выполняемая при остановке EDIMailService.
onCRLUpdate	Функция JavaScript с одним параметром — текстом сообщения об ошибке обновления СОС с указанием ini-файла, содержащего ссылки на криптографические справочники и другие параметры криптографии, точки распространения СОС, выполняемая при ошибке в обновлении списка отозванных сертификатов Может использоваться, например, для посылки уведомления об ошибке на электронную почту администратора сервера.
onEveryNNNsec	Функция JavaScript, выполняемая через каждые NNN секунд.
onEveryNNNmin	Функция JavaScript, выполняемая через каждые NNN минут.
onEveryNNNhour	Функция JavaScript, выполняемая через каждые NNN часов.

В качестве примера периодически выполняемых скриптов можно привести следующий скрипт, который проверяет, что все файловые шлюзы, которые должны быть запущены, работают:

```
var FileGatesToRestart = new Array;
for (var i in iniFile.filegateDir) {
 for (var j in clients) {
  if (clients[j].exefile.toUpperCase().indexOf('FILEGATE.EXE') !== -1) {
   if (iniFile.filegateDir[i].toUpperCase().indexOf(clients[j].workdir.toUpperCase()) === -1) {
    FileGatesToRestart[i] = iniFile.filegateDir[i];
   }
  }
 }
}
for (i in FileGatesToRestart) {
```

```
   var dir = cd(FileGatesToRestart[i]);
   pid[i] = spawn("FileGate.exe", "/ini:FileGate.ini");
   cd (dir);
   if (pid[i] == 0 || pid[i] == -1) {
      delete pid[i];
   }
}
FileGatesToRestart = null;
```

Если этот скрипт записан в файл watchdog.js, то параметр ini-файла onEvery5min=function () { load("watchdog.js"); } проверяет и запускает остановившиеся по каким-то причинам файловые шлюзы, запуск которых был запланирован в секции [filegateDir], описанной в следующем разделе.

[filegateDir]

В секции задаются параметры для настройки запуска файловых шлюзов одновременно с сервисом EDIMailService.

Ключ	Описание
FileGate1	Путь к каталогу, где находятся исполняемые файлы шлюза.
FileGate2	Путь к каталогу, где находятся исполняемые файлы шлюза.

[db]

В секции задаются базы данных, с которыми работает EDIMailService.

Ключ	Описание
work	Рабочая БД сервиса (mail.sqlite3) для хранения идентификаторов прочитанной почты и других служебных данных.
users	База данных пользователей ЭДО (export.sqlite3). БД используется для организации системы адресации и контроля полномочий отправителей. Файл с базой пользователей включен в дистрибутив, также доступен на сайте УЦ МБ для самостоятельного скачивания и периодически рассылается в служебных письмах администратора ЭДО всем клиентам для автоматического обновления БД.

[permission]

В секции задаются запреты на автоматическое обновление компонентов файлового шлюза. По умолчанию обновления периодически рассылаются по электронной почте в виде служебного письма, подписанного ЭЦП Администратора ЭДО МБ. После проверки подписи Администратора и целостности письма и всех его вложений, выполняется автоматическая установка обновлений. С помощью ключей данной секции автоматическое обновление можно отменить. Секция является опциональной.

Ключ	Описание
updateUsersDB	Автоматическое обновление базы данных пользователей ЭДО. Может принимать значения: • "false" - запретить, • "true" - разрешить. Значения по умолчанию "true".
updateEDIMailService	Автоматическое обновление ПО EDIMailService (включая FileGate.exe и EDIMailDLL.dll). Может принимать значения: • "false" - запретить, • "true" - разрешить. Значения по умолчанию "true".
noUpdate	Запрет любых изменений. Может принимать значения: • "false" - разрешить, • "true" - запретить. Значения по умолчанию "false".

[archive]

В секции задаются параметры архивации. При необходимости EDIMailService может производить архивацию принятых и отправленных файлов, их ЭЦП, адресов отправки и другой служебной информации в базе данных для удобства последующего поиска документов. В настоящий момент поддерживается архивирование в базах данных Microsoft SQL Server 2005, Microsoft SQL Server 2008 и последующих версий. Предполагается, что сама база данных создана и SQL сервер соответствующим образом сконфигурирован, а указанный в строке соединения с базой данных логин имеет права на создание / удаление таблиц и индексов, чтение и вставку в таблицы этой базы данных. Связь с базой данных осуществляется через механизм ODBC. Секция является опциональной.

Ключ	Описание
type	Задает тип SQL сервера (MSSQL2005, MSSQL2008 и т.д.).
connection	Строка соединения с базой данных. Формат строки: **connection=<Driver={SQL Server}>;<Server=>;<Database=>; <Uid=>; <Pwd=>;** где • **Driver** - наименование драйвера (SQL Server), • **Server** - имя компьютера, на котором работает ПО MS SQL Server, • **Database** - имя базы данных, созданной на этом сервере для хранения архива ЭДО, • **Uid** - имя пользователя (логин) MS SQL Server, имеющего права владельца базы данных, • **Pwd** — пароль для доступа к БД.
direction	Какие сообщения архивировать. Может принимать значения: • "in" - архивировать только входящие сообщения, • "out" - архивировать только исходящие сообщения, • "both" - архивировать все сообщения. Значения по умолчанию "both".
cs_collation	Способ сортировки/сравнения букв, с учетом регистра букв. По умолчанию SQL_Latin1_General_Cp1251_CS_AS (кириллица в кодировке Windows).
ci_collation	Способ сортировки/сравнения букв, без учета регистра букв. По умолчанию SQL_Latin1_General_Cp1251_CI_AS (кириллица в кодировке Windows).

[notification]

EDIMailService может по результатам запуска или проверки состояния своих клиентов, таких как файловый шлюз, производить генерацию и рассылку по электронной почте соответствующих уведомлений для системного администратора, поддерживающего работу EDIMailService. Настройки для рассылки e-mail уведомлений задаются в данной секции. Если эта секция отсутствует или закомментирована, никакие уведомления не посылаются.

По умолчанию устанавливаемые дистрибутивом скрипты посылают уведомления в следующих случаях:

- использование неверного адреса в настройках FileGate;
- невозможности запустить FileGate в указанных в секции [filegateDir] папках;
- если в ходе работы процесс FileGate был завершен и автоматически перезапущен.

Ключ	Описание
url	Url SMTP сервера, который получит уведомление от EDIMailService и положит его в почтовый ящик. ВНИМАНИЕ! Это не SMTP сервер системы ЭДО, а сервер обычной электронной почты, используемой в вашей организации. Обязательный параметр. Если он не заполнен, то уведомления посылаться не будут.
login	Логин для доступа к SMTP серверу.
password	Пароль для доступа к SMTP серверу.
address	Адрес электронной почты, на который будут приходить уведомления.
text	Шаблон текста уведомления в кодировке utf-8. В шаблоне два параметра: {0} - причина проблемы, {1} - рабочая папка клиента, вызвавшего проблему.
subject	Шаблон темы уведомления в кодировке utf-8. В шаблоне один параметр: {0} - имя хоста, где работает EDIMailService, пославший уведомление.
TLScheck	Нужно ли выполнять проверку валидности SSL-сертификата при работе с SMTP сервером по SSL/TLS протоколу. Допустимые значения: • "no" - не проверять сертификат, • "host" - проверять только совпадение имени хоста в сертификате и url,

Ключ	Описание
	• "all" - выполнить полную проверку сертификата. Значение по умолчанию "no".
TLSfirst	Какой протокол запускать раньше - SMTP или SSL/TLS: • "no" - сначала запускается SMTP, потом TLS, • "yes" - сначала запускается SSL, потом SMTP. Значение по умолчанию "no".
useTLS	Использовать ли TLS/SSL для шифрации обмена с SMTP сервером. Допустимые значения: • "no" - не использовать, • "yes" - использовать обязательно, при отсутствии зашифрованного соединения ничего не передавать, • "try" - использовать, если сервер поддерживает эту возможность. Значение по умолчанию "no".
verbose	Детализация информации, выводимой в лог: • "1" - делать подробный лог, • "0" - не делать подробного лога. Значение по умолчанию "0".
login_options	Способ аутентификации на сервере. Задается как AUTH=: • "AUTH=PLAIN" - аутентификационная информация (логин/пароль) передается по сети в открытом виде, • "AUTH=LOGIN" - аутентификационная информация передается по сети в кодировке Base64, • "AUTH=NTLM" - аутентификация по протоколу NTLM, аутентификационная информация по сети не передается.

[edimaillog]

В секции задаются параметры логирования работы EDIMailService.

Ключ	Описание
logfileperday	Задает порционность лог-файлов. Может принимать следующие значения: • "0" - новый лог-файл формируется каждый раз при запуске модуля (открытии лога). Старый лог-файл переименовывается путем добавления к его базовому имени "1". При этом в зависимости от значения параметра *logfilenametype* номер вставляется в середину названия файла (перед точкой), либо в конец названия (после расширения). При формировании очередного лог-файла номера предыдущих увеличиваются на единицу. Количество хранимых лог-файлов задается в параметре *logfiledepth*. • "1" - новый лог-файл создается на каждый день, если в этот день была хотя бы одна запись в лог. Если при открытии лога необходимый лог-файл уже существует, то новые сообщения дописываются в конец этого файла. При первом открытии лога к базовому имени лог-файла добавляется дата его создания в формате YYYYMMDD. При этом в зависимости от значения параметра *logfilenametype* дата вставляется в середину названия файла (перед точкой), либо в конец названия (после расширения). Количество хранимых лог-файлов задается в параметре *logfiledepth*. • "2" - новый лог-файл создается каждый час. Если при открытии лога необходимый лог-файл уже существует, то новые сообщения дописываются в конец этого файла. При первом открытии лога к базовому имени лог-файла добавляется дата и время его создания в формате YYYYMMDDHH. При этом в зависимости от значения параметра *logfilenametype* дата вставляется в середину названия файла (перед точкой), либо в конец названия (после расширения). При переходе через границу часа создается новый лог-файл с соответствующим именем. Количество хранимых лог-файлов задается в параметре *logfiledepth*. Значение по умолчанию "0".

Ключ	Описание
logfile	Базовое имя лога. Используется для формирования имени лог-файла. Если параметр не задан или задано пустое имя, то используется имя файла исполняемого модуля без расширения. Представляет собой левую часть имени лог-файла, может быть задан полный или относительный путь. Если задан относительный путь, то полный путь расположения лог-файлов вычисляется относительно текущего каталога в момент открытия лога.
logfilenametype	Способ формирования имени лог-файла. Может принимать следующие значения: • "0" - дополнительные параметры имени (номер или дата) добавляются в конец названия файла. • "1" - дополнительные параметры имени вставляются в середину названия файла. Значение по умолчанию "1".
logfiledepth	Количество хранимых лог-файлов, включая текущий. Значение должно быть больше нуля. Значение по умолчанию "3".
logtime	Определяет формат вывода времени. Может принимать следующие значения: • "0" - время не выводится. • "1" - время с точностью до секунд выводится на отдельной строке перед соответствующим сообщением, если с момента предыдущего сообщения прошло не менее секунды. Формат даты: *YYYY-MM-DD HH:MM:SS*. • "2" - время с точностью до тысячных долей секунды выводится в начале каждой строки с сообщением. Формат даты: *YYYY-MM-DD HH:MM:SS.mmm*. • "3" - время с точностью до тысячных долей секунды выводится в начале каждой строки с сообщением, но при этом календарная дата не выводится. Формат даты: *HH:MM:SS.mmm*. Опция может быть указана только для режимов *logfileperday=1* и *logfileperday=2*. • "4" - в начале каждой строки с сообщением выводится количество микросекунд, прошедших с момента инициализации библиотеки P2SysLog. Значение по умолчанию "2".
logtoconsole	Разрешает копирование всех лог-сообщений на консоль. Может принимать следующие значения: • "0" - выключено. • "1" - включено. Значение по умолчанию "1".
traceini	Задает имя ini-файла, куда необходимо заносить все трейсы. Использование параметра traceini позволяет избежать загромождения основного ini-файла. Также позволяет присваивать этому ini-файлу свойство Read only, что невозможно в случае, когда трейсы заносятся в него же.
logtosyslog	Отключает запись сообщений об ошибке в системный event log в случае, невозможности открытия log-файла или печати trace-записи в лог с P2LOG_SEVERITY_FATAL. Может принимать следующие значения: • "0" - выключено. • "1" - включено. Значение по умолчанию "1".
addthreadid	При включении данной настройки к каждой строке лог-файла будет добавляться информация о потоке, который это выводит (ThreadID). Настройка актуальна для многопоточных приложений. Может принимать следующие значения: • "0" - выключено. • "1" - включено.
logfilecache	Размер (в байтах) буфера в памяти процесса, в который кэшируется лог. Значение должно быть в диапазоне: 0-32767. Опция используется для управления кэшированием в памяти операций записи в лог-файл. При задании данного параметра (использовании кэша) следует помнить, что файловая операция записи в лог-файл не активизируется, пока не заполнится весь буфер. Поэтому слишком большой размер буфера может привести к ситуации, когда лог-файл будет пустым.

Имя файла лога формируется в зависимости от значений трех параметров: *logfile*, *logfilenametype*, *logfileperday*. Если значение параметра *logfilenametype=1*, то базовое имя файла (значение параметра *logfile*) разбивается на две части — имя и расширение (расширением считается часть базового имени, расположенная за последней точкой: <name>[.ext]), в противном случае базовое имя файла остается неделимым (расширение пустое). Ниже в таблице приведены правила формирования имени лог-файла.

logfilenametype	logfileperday	logfile	Результат
0	0	file	file file.1 file.2
		file.log	file.log file.log.1 file.log.2
1	0	file	file file.1 file.2
		file.log	file.log file.1.log file.2.log
0	1	file	file.20090911 file.20090910 file.20090909
		file.log	file.log.20090911 file.log.20090910 file.log.20090909
1	1	file	file.20090911 file.20090910 file.20090909
		file.log	file.20090911.log file.20090910.log file.20090909.log
0	2	file	file.2009091114 file.2009091113 file.2009091112
		file.log	file.log.2009091114 file.log.2009091113 file.log.2009091112
1	2	file	file.2009091114 file.2009091113 file.2009091112
		file.log	file.2009091114.log file.2009091113.log file.2009091112.log

Пример файла EdiMail.ini:

```
[dirs]
work_dir=C:\Moscow Exchange\EDIMail\ProgData\

[edimaillog]
logfileperday=1
logfilecache=0
addthreadid=1
traceini=C:\Moscow Exchange\EDIMail\ProgData\edimail_trace.ini
logfile=C:\Moscow Exchange\EDIMail\ProgData\log\edimail.log

[maintenance]
tick=24
maxsize=500
older=7

[xmlrpc]
tick=0.99
introspection=1
verbose=0
port=12069

[db]
work= "$(workdir)mail.sqlite3"
users= "$(workdir)export.sqlite3"

[crypto]
validata=xpki1.dll
url=ldap://vcert.pki.moex.com:50001/C=RU
local= "file://$(workdir)ediadmin.gdbm"
pse= "pse://$(workdir)ediadmin.pse"

[crypto_rsa]
validata=rpki1.dll
url=ldap://vcert.pki.moex.com:50003/C=RU
local= "file://$(workdir)ediadmin_rsa.gdbm"
pse= "pse://$(workdir)ediadmin_rsa.pse"

[global]
onShutdown=function() {for (var i in pid) {kill(pid[i]);}}
onInit=function() { load("startup.js"); }
onEvery1Min=function() { load("watchdog.js"); }

[filegateDir]
Filegate1=C:\Moscow Exchange\EDIMail\FileGate\
```

```
[notification]
TLScheck=host
verbose=0
TLSfirst=no
useTLS=try
text={0} in folder {1}
subject=EDIMail watchdog problem report from {0}
password=
login=
address=
url=
login_options=AUTH=LOGIN
```

7.2. Файл FileGate.ini

Файл содержит параметры настройки файлового шлюза (FileGate.exe). Ниже приведено описание секций FileGate.ini.

[FileGate]

В секции задаются глобальные параметры модуля FileGate.exe.

Ключ	Описание
protectionlevel	Параметр, устанавливающий уровень криптографической защиты передаваемых файлов. Может принимать следующие значения: • "0" - криптография не используется. • "1" - только ЭЦП. • "2" - ЭЦП и шифрование. • "3" - ЭЦП и шифрование с пересылкой по MIME стандарту.
sendparam	Имя секции с настройками почтового протокола для отправки сообщений (SMTP).
recvparam	Имя секции с настройками почтового протокола для приема сообщений (IMAP или POP3).
error	Каталог ошибочных сообщений, которые не могут быть отправлены. Если этот параметр не задан, то используется подкаталог ERROR в текущем каталоге, если такой существует, или ошибочные сообщения удаляются, если такой отсутствует. Если каталог задан, но отсутствует или недоступен, то пишется сообщение об ошибке и программа выходит с аварийным завершением.
sent	Каталог отправленных сообщений. Если этот параметр не задан, то все отправленные сообщения удаляются. Если каталог задан, но отсутствует или недоступен, то пишется сообщение об ошибке и программа выходит с аварийным завершением.
loops	Количество повторов в цикле до выхода из программы. Если этот параметр не задан или равен нулю, то количество повторов бесконечно – до принудительного выхода по Ctrl-C.
srvcini	Имя и путь к дополнительному настроечному файлу шлюза (EDIMailSrvs.ini), который содержит реквизиты дополнительной идентификации файлового шлюза и параметры криптографии.
sleeptime	Время ожидания цикла опроса EDIMailService и сканирования каталогов OUT (в секундах).
ncollect	Максимальное количество сообщений, читаемых за один запрос.
folderparam	Имя секции с настройками рассылки через файловые шары.

[SMTP]

Имя секции задается ключом *sendparam* в секции [FileGate]. В секции указываются параметры почтового протокола для отправки сообщений (SMTP).

Помимо стандартных параметров почтового протокола, описанных ниже, в секции могут задаваться параметры, используемые библиотекой cURL. Перечень и описание этих параметров можно посмотреть здесь: https://curl.haxx.se/libcurl/c/curl_easy_setopt.html. При задании параметра указывается его написание в нижнем регистре, без префикса CURLOPT_. Например, параметр библиотеки CURLOPT_LOGIN_OPTIONS из описания https://curl.haxx.se/libcurl/c/CURLOPT_LOGIN_OPTIONS.html задается параметром ini-файла *login_options*.

Ключ	Описание
useTLS	Параметр определяет, используется ли шифрование при взаимодействии с SMTP сервером. Может принимать следующие значения: • "use" - режим с шифрованием.

Ключ	Описание
	• "try" - сначала с шифрованием, если не получилось, то переходим в режим без шифрования. • "no" - режим без шифрования.
TLSfirst	Если шифрование используется, то данный параметр определяет порядок запуска протоколов шифрования и посылки: • "yes" - сначала шифрование потом посылка. • "no" - сначала посылка потом шифрование.
verbose	Детализация информации, выводимой в лог: • "1" - делать подробный лог, • "0" - не делать подробного лога. Значение по умолчанию "0".
TLScheck	Уровень проверки сертификата сервера, присланного в ходе установки зашифрованного соединения.
url	URL SMTP сервера.
port	Порт SMTP сервера. Порт можно задавать и в url-строке.
password	Пароль для доступа к SMTP серверу. Можно указывать либо пароль в открытом виде, либо JavaScript функцию, которая будет получать пароль из другого места.
login	Логин для доступа к SMTP серверу.
login_options	Способ аутентификации на сервере. Задается как AUTH=: • "AUTH=PLAIN" - аутентификационная информация (логин/пароль) передается по сети в открытом виде, • "AUTH=LOGIN" - аутентификационная информация передается по сети в кодировке Base64, • "AUTH=NTLM" - аутентификация по протоколу NTLM, аутентификационная информация по сети не передается.

[IMAP]

Имя секции задается ключом *recvparam* в секции [FileGate]. В секции указываются параметры почтового протокола для приема сообщений (IMAP или POP3).

Помимо стандартных параметров почтового протокола, описанных ниже, в секции могут задаваться параметры, используемые библиотекой cURL. Перечень и описание этих параметров можно посмотреть здесь: https://curl.haxx.se/libcurl/c/curl_easy_setopt.html. При задании параметра указывается его написание в нижнем регистре, без префикса CURLOPT_. Например, параметр библиотеки CURLOPT_LOGIN_OPTIONS из описания https://curl.haxx.se/libcurl/c/CURLOPT_LOGIN_OPTIONS.html задается параметром ini-файла *login_options*.

Ключ	Описание
service	Имя сервиса ЭДО.
useTLS	Параметр определяет, используется ли шифрование при взаимодействии с IMAP сервером. Может принимать следующие значения: • "use" - режим с шифрованием. • "try" - сначала с шифрованием, если не получилось, то переходим в режим без шифрования. • "no" - режим без шифрования.
TLSfirst	Если шифрование используется, то данный параметр определяет порядок запуска протоколов шифрования и посылки: • "yes" - сначала шифрование потом посылка. • "no" - сначала посылка потом шифрование.
verbose	Детализация информации, выводимой в лог: • "1" - делать подробный лог, • "0" - не делать подробного лога.

Ключ	Описание
	Значение по умолчанию "0".
TLScheck	Уровень проверки сертификата сервера, присланного в ходе установки зашифрованного соединения.
url	URL IMAP сервера.
port	Порт IMAP сервера. Порт можно задавать и в url-строке.
password	Пароль для доступа к IMAP серверу. Можно указывать либо пароль в открытом виде, либо JavaScript функцию, которая будет получать пароль из другого места.
login	Логин для доступа к IMAP серверу.
login_options	Способ аутентификации на сервере. Задается как AUTH=: • "AUTH=PLAIN" - аутентификационная информация (логин/пароль) передается по сети в открытом виде, • "AUTH=LOGIN" - аутентификационная информация передается по сети в кодировке Base64, • "AUTH=NTLM" - аутентификация по протоколу NTLM, аутентификационная информация по сети не передается.

[notification]

FileGate может по мере написания сообщений об ошибках в лог производить генерацию и рассылку по электронной почте соответствующих уведомлений для системного администратора, поддерживающего работу ЭДО. Настройки для рассылки e-mail уведомлений задаются в данной секции. Если эта секция отсутствует или закомментирована, никакие уведомления не посылаются.

Ключ	Описание
url	Url SMTP сервера, который получит уведомление от FileGate и положит его в почтовый ящик. ВНИМАНИЕ! Это не SMTP сервер системы ЭДО, а сервер обычной электронной почты, используемой в вашей организации. Обязательный параметр. Если он не заполнен, то уведомления посылаться не будут.
login	Логин для доступа к SMTP серверу.
password	Пароль для доступа к SMTP серверу.
address	Адрес электронной почты, на который будут приходить уведомления.
text	Шаблон текста уведомления в кодировке utf-8. В шаблоне два параметра: {0} - причина проблемы, {1} - рабочая папка клиента, вызвавшего проблему.
subject	Шаблон темы уведомления в кодировке utf-8. В шаблоне один параметр: {0} - имя хоста, где работает EDIMailService, пославший уведомление.
TLScheck	Нужно ли выполнять проверку валидности SSL-сертификата при работе с SMTP сервером по SSL/TLS протоколу. Допустимые значения: • "no" - не проверять сертификат, • "host" - проверять только совпадение имени хоста в сертификате и url, • "all" - выполнить полную проверку сертификата. Значение по умолчанию "no".
TLSfirst	Какой протокол запускать раньше - SMTP или SSL/TLS: • "no" - сначала запускается SMTP, потом TLS, • "yes" - сначала запускается SSL, потом SMTP. Значение по умолчанию "no".
useTLS	Использовать ли TLS/SSL для шифрации обмена с SMTP сервером. Допустимые значения: • "no" - не использовать, • "yes" - использовать обязательно, при отсутствии зашифрованного соединения ничего не передавать, • "try" - использовать, если сервер поддерживает эту возможность. Значение по умолчанию "no".
verbose	Детализация информации, выводимой в лог: Файловый Url каталога. Формат: ***url=file://C:*** .

Ключ	Описание
	• "1" - делать подробный лог, • "0" - не делать подробного лога. Значение по умолчанию "0".
login_options	Способ аутентификации на сервере. Задается как AUTH=: • "AUTH=PLAIN" - аутентификационная информация (логин/пароль) передается по сети в открытом виде, • "AUTH=LOGIN" - аутентификационная информация передается по сети в кодировке Base64, • "AUTH=NTLM" - аутентификация по протоколу NTLM, аутентификационная информация по сети не передается.

[FolderParam]

Имя секции задается ключом *folderparam* в секции [FileGate]. В секции указываются настройки механизма рассылки через файловые шары, который подразумевает наряду с отправкой файлов по электронной почте выкладывание их еще и в заданный каталог на диске. Механизм работает только для рассылки по правилу FILE (рассылка отчетов).

Ключ	Описание
url	Файловый Url каталога. Формат: **url=file://C:** . Пример: `url=file://C:\Moscow Exchange\SHARED_GATE\REPORT\USER1`

[RULES]

В секции задаются имена правил приема/отправки сообщений.

Ключ	Описание
MAIN	Имя основного правила.
RULE1	Имя дополнительного правила.
RULE2	Имя дополнительного правила.

[имя правила]

В секции задаются параметры правил приема/отправки сообщений.

Ключ	Описание
type	Формат обмена (BBS, MSG или FILE).
in	Каталог входящих сообщений. Для основного правила значение по умолчанию "IN". Для правила на отсылку не задается. Если каталог входящих сообщений задан, но отсутствует или недоступен (например, это сетевой диск) то пишется сообщение об ошибке и программа выходит с аварийным завершением.
out	Каталог исходящих сообщений. Для дополнительного правила на прием не задается. Если этот параметр не задан, то используется подкаталог OUT в текущем каталоге, если такой существует, или программа работает только на прием, если такого нет (при старте выдается предупреждение). Если каталог сообщений задан, но отсутствует или недоступен (например, это сетевой диск), то пишется сообщение об ошибке и, если определен каталог IN, программа продолжает работать на прием.
sent	Каталог отправленных сообщений. Если этот параметр не задан, то все отправленные сообщения удаляются. Если каталог отправленных сообщений задан и в общих настройках шлюза, то каталог, заданный в правиле, является приоритетным.
subject	Тема сообщения. Для входящих — это условие, по которому сообщение попадает под это правило, для исходящих — эта тема указывается в отправляемых сообщениях.

Ключ	Описание
	Игнорируется при приеме сообщений по основному правилу. Игнорируется при отправке сообщений по форматам BBS и MSG. Поле заканчивается концом строки и может содержать пробелы. Пробелы между двоеточием и значением поля игнорируются при передаче.
address	Адрес (отправителя для входящих, получателя для исходящих). Игнорируется при приеме сообщений по основному правилу. Игнорируется при отправке сообщений по форматам BBS и MSG.
coretype	Шестнадцатеричное значение типа сообщений, присваиваемое отправляемым сообщениям, и требуемое для принимаемых. Значение по умолчанию для отправляемых "0x1200".
firm	Определяет необходимость сохранения файла (файлов) с именем, состоящим из даты, кода компании и порядкового номера файла (см. раздел 4.1.3.3). Может принимать следующие значения: • "0" - опция отключена. • "1" - сквозная нумерация файлов по всем правилам. Нумерация не сбрасывается при переходе на новую дату и при перезапуске шлюза. Начальный номер для сквозной нумерации можно настраивать. • "2" - нумерация файлов ведется в рамках одного правила для сообщений одного адресата. Нумерация сбрасывается при каждом переходе на новую дату. Данный параметр используется только для формата FILE и только на прием. Для всех правил на отправку этот параметр игнорируется.
compatibility_ option	Опция обеспечения совместимости со старыми форматами обмена (EDIGATE). Может принимать следующие значения: • "0" - совместимость отключена. • "1" - совместимость конвертов, несовместимость имен файлов. • "2" - несовместимость конвертов, совместимость имен файлов. • "3" - совместимость конвертов, совместимость имен файлов Значение по умолчанию "1". Опция используется только для форматов BBS и MSG.

[p2syslog]

В секции задаются параметры логирования работы модуля FileGate.exe. Описание параметров см. раздел 7.1 секция **[edimaillog]**.

Пример файла FileGate.ini:

```
[p2syslog]
logtime=1
logfileperday=1
logfilecache=0
traceini=C:\Moscow Exchange\EDIMail\ProgData\FileGate_trace.ini
logfile=C:\Moscow Exchange\EDIMail\ProgData\log\FileGate.log

[FileGate]
protectionlevel=2
sendparam=SMTP
recvparam=IMAP
ERROR=C:\Moscow Exchange\EDIMail\FileGateMail\error\
srvcini=EDIMailSrvs.ini
sleeptime=20
folderparam=FolderParam

[IMAP]
service=REPORTS
useTLS=use
TLSfirst=yes
verbose=0
TLScheck=host
url=imap://mars.moex.com:993
```

```
password=password
login=your_login
login_options=AUTH=PLAIN

[SMTP]
useTLS=try
TLSfirst=no
verbose=0
TLScheck=host
url=smtp://mars.moex.com:25
password=password
login=your_login
login_options=AUTH=LOGIN

[notification]
TLScheck=host
verbose=0
TLSfirst=no
useTLS=try
text={0} in folder {1}
subject=EDIMail watchdog problem report from {0}
password=
login=
address=
url=
login_options=AUTH=LOGIN

[FolderParam]
url=file://C:\Moscow Exchange\SHARED_GATE\REPORT\USER1

[RULES]
RULE7=RULE7
RULE6=RULE6
RULE5=RULE5
RULE4=RULE4
RULE3=RULE3
RULE2=RULE2
RULE1=RULE1
MAIN=MAIN

[MAIN]
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\MAIN_OUT\
IN=C:\Moscow Exchange\EDIMail\FileGateMail\MAIN_IN\
TYPE=BBS

[RULE1]
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_MOEX\
ADDRESS=EMAIL@NPRTS.REPORT
TYPE=FILE

[RULE2]
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_FO_REPORT\
ADDRESS=EMAIL@FORTS.REPORT
TYPE=FILE

[RULE3]
ADDRESS=EMAIL@AORTS.OTCMON
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\TO_OTC_REPORT\
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_OTC_REPORT\
TYPE=FILE

[RULE4]
ADDRESS=EMAIL@AORTS.TECHDOSTUP
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\TO_MBTECH\
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_MBTECH\
TYPE=FILE

[RULE5]
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_HELPDESK\
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\TO_HELPDESK\
TYPE=FILE
ADDRESS=EMAIL@AORTS.HELP
```

```
[RULE6]
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\TO_FO_CLIENT_DEPT\
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_FO_CLIENT_DEPT\
ADDRESS=EMAIL@FORTS.CLIENTS
TYPE=FILE

[RULE7]
OUT=C:\Moscow Exchange\EDIMail\FileGateMail\TO_NCC_CLIENT_DEPT\
IN=C:\Moscow Exchange\EDIMail\FileGateMail\FROM_NCC_CLIENT_DEPT\
ADDRESS=EMAIL@NPRTS.CLIENTS
TYPE=FILE
```

7.3. Файл EDIMailSrvs.ini

Файл содержит реквизиты дополнительной идентификации файлового шлюза и параметры криптографии. Ниже приведено описание секций EDIMailSrvs.ini.

[self]

В секции задаются реквизиты для идентификации файлового шлюза.

Ключ	Описание
service	Код сервиса ЭДО.
ticker	Код ЭДО.
email	Почтовый адрес.
key	Название фирмы или ее ИНН.

[crypto]

В секции задаются параметры криптографии с шифрованием ГОСТ.

Ключ	Описание
validata	Имя или полный путь к файлу библиотеки, используемой для работы криптографии с шифрованием ГОСТ (xpki1.dll).
pse	Полный путь до файла персонального справочника администратора ЭДО (файл обычно имеет расширение ".pse").
local	Полный путь до файла локального справочника сертификатов администратора ЭДО (файл обычно имеет расширение ".gdbm"). В случае установки нескольких шлюзов, каждый шлюз должен использовать свой отдельный файл справочника.
cleartext	Разрешение принимать незашифрованные и неподписанные файлы. • "allow" - принимать разрешено, • "deny" -запрещено. Значения по умолчанию "deny". НЕ РЕКОМЕНДУЕТСЯ ИЗМЕНЯТЬ НАСТРОЙКУ ЭТОГО ПАРАМЕТРА ПО УМОЛЧАНИЮ.
search	Поиск сертификатов для адресов получателей сообщений ЭДО. • "strict" - должны быть найдены сертификаты для всех получателей сообщения, • "weak" -должен быть найден хотя бы один сертификат. Значения по умолчанию "strict".
pin	Пин код/пароль,используемый для доступа к носителям криптоключей. Можно указать либо непосредственной пин код/пароль, либо JavaScript функцию, которая будет получать пароль из другого места (см. раздел 6.12).

[crypto_rsa]

В секции задаются параметры криптографии с шифрованием RSA.

Ключ	Описание
validata	Имя или полный путь к файлу библиотеки, используемой для работы криптографии с шифрованием RSA (rpki1.dll).

Ключ	Описание
pse	Полный путь до файла персонального справочника администратора ЭДО (файл обычно имеет расширение ".pse").
local	Полный путь до файла локального справочника сертификатов администратора ЭДО (файл обычно имеет расширение ".gdbm"). В случае установки нескольких шлюзов, каждый шлюз должен использовать свой отдельный файл справочника.
cleartext	Разрешение принимать незашифрованные и неподписанные файлы. • "allow" - принимать разрешено, • "deny" - запрещено. Значения по умолчанию "deny". НЕ РЕКОМЕНДУЕТСЯ ИЗМЕНЯТЬ НАСТРОЙКУ ЭТОГО ПАРАМЕТРА ПО УМОЛЧАНИЮ.
search	Поиск сертификатов для адресов получателей сообщений ЭДО. • "strict" - должны быть найдены сертификаты для всех получателей сообщения, • "weak" - должен быть найден хотя бы один сертификат. Значения по умолчанию "strict".
pin	Пин код/пароль,используемый для доступа к носителям криптоключей. Можно указать либо непосредственной пин код/пароль, либо JavaScript функцию, которая будет получать пароль из другого места (см. раздел 6.12).

[global]

В этой необязательной секции задаются параметры настройки реакции на события и содержимое глобального контекста JavaScript для данного экземпляра файлового шлюза. EDIMailService может выполнять скрипты на языке JavaScript для файлового шлюза при наступлении определенных событий. На данный момент предусмотрена обработка следующих событий:

- Запуск EDIMailService (событие onInit);
- Остановка EDIMailService (событие onShutdown);
- Отправка сообщения (событие onMsgSend);
- Прием сообщения (событие onMsgReceive);
- Ошибка при обновлении списка отозванных сертификатов (событие onCRLUpdate);
- Ошибка поиска сертификатов (событие onCertFindError);
- Периодический запуск скриптов по истечении определенного интервала времени (события onEveryNNNsec, onEveryNNNmin, onEveryNNNhour).

При наступлении события выполняется одноименная событию функция, определенная в глобальном контексте JavaScript. Содержимое глобального контекста JavaScript можно задавать в секции.

Ключ	Описание
onInit	Функция JavaScript без параметров, выполняемая при запуске EDIMailService.
onShutdown	Функция JavaScript без параметров, выполняемая при остановке EDIMailService.
onMsgSend	Функция JavaScript без параметров, выполняемая при отправке сообщения.
onMsgReceive	Функция JavaScript без параметров, выполняемая при приеме сообщения.
onCRLUpdate	Функция JavaScript с одним параметром — текстом сообщения об ошибке обновления СОС с указанием ini-файла, содержащего ссылки на криптографические справочники и другие параметры криптографии, точки распространения СОС, выполняемая при ошибке в обновлении списка отозванных сертификатов Может использоваться, например, для посылки уведомления об ошибке на электронную почту администратора сервера.
onCertFindError	Функция JavaScript с одним параметром — текстом сообщения об ошибке поиска сертификата. Может использоваться, например, для посылки уведомления об ошибке на электронную почту администратора сервера.
onEveryNNNsec	Функция JavaScript, выполняемая через каждые NNN секунд.
onEveryNNNmin	Функция JavaScript, выполняемая через каждые NNN минут.
onEveryNNNhour	Функция JavaScript, выполняемая через каждые NNN часов.

Пример файла EDIMailSrvs.ini:

```
[self]
service=REPORTS
[crypto]
local= "file://C:\Users\AppData\Roaming\Validata\xcs\local.gdbm"
pse= "pse://C:\Users\AppData\Roaming\Validata\xcs\local.pse"
validata= xpki1.dll
```

8. Ошибки ПО и способы их устранения

Вид ошибки	Возможные причины возникновения	Способы устранения
Can't determine self address for working certificate … service	Использование устаревшей базы данных пользователей ЭДО, которая находится в файле export.sqlite3.	
Cryptography initialize error Ошибка проверки целостности ПСП	Возможно, установлена старая версия ПО Валидаты. Не Справочник АПК Клиент ММВБ, а еще предыдущая версия ПКЗИ СЭД ММВБ.	
;RPC;error;IMAP poller can't start Exception: Can't load crypto DLL xpki1.dll;TID 296	В EdiMail.ini указано значение параметра validata=xpki1.dll, но при этом не удается загрузить эту библиотеку. Причина — некорректно установленный справочник сертификатов. Например, установлен под другим пользователем, нежели тот, от которого запускают УФШ, или установлена 64бит версия АПК Клиента, а не 32бит.	
EDIGate;error;Can't post message: Exception: Login denied	Проблема в настройках CISCO ASE на маршрутизаторе у клиента. Там запрещены расширенные SMTP команды.	Обратиться к системному администратору для настройки соответствующего сетевого оборудования.
;PostTo;error;Message message-id to service failed to post to url smtp://mars.moex.com:25 login "тут логин" with error CURL error: Login denied;TID 2576	На компьютере клиента не работает отправка сообщений ЭДО, из-за того, что на его офисном маршрутизаторе запрещена возможность переключения протокола SMTP в режим работы по зашифрованному каналу.	Есть два варианта решения проблемы: • Перенастроить отправку сообщений так, чтобы не использовалось SSL/TLS шифрование. Для этого необходимо в файле FileGate.ini в секции с настройками почтового протокола для отправки сообщений (SMTP) выставить useTLS=no. Не рекомендуется использовать этот вариант, так как пароли/логины на доступ к почтовому ящику будут передаваться по сети в незашифрованном виде. • Обратиться к системному администратору для настройки соответствующего сетевого оборудования.
SSL connect error schannel: failed to receive handshake, SSL/TLS connection failed		Необходимо отредактировать файл EDIMail.ini, включив туда секцию: [V8] forceGC=15
EDIGate;error;Can't init EDIMail message, Null value: You can't send mail - read-only EDI access	В админке ЭДО пользователю, от имени которого работает клиент, задан доступ "только для чтения", поэтому он не может ничего отправлять.	
Data error: Error finding recepients certificate for ___ Certificate not found	В базе export.sqlite3 нет требуемого сертификата.	
Приложению не удалось запуститься, поскольку ASRDLL.dll не был найден		Нужно проверить наличие на компьютере остатков от системы криптозащиты "Сигнатура", используемой ЦБ РФ, конфликтующей с криптографией от Валидаты.
Не найден соответствующий сертификату секретный ключ	Служба EDIMailService устанавливается инсталлятором, как работающая под логином LocalSystem. Устройства загрузки ключей настраиваются программой конфигурации СКЗИ Валидата индивидуально для каждого логина. То, что справочник сертификатов нормально работает для интерактивного пользователя, не означает, что все необходимые настройки сделаны для логина LocalSystem.	Для настройки СКЗИ Валидата под логином LocalSystem (см. раздел 5.4.1).
У клиента служба EDIMailService не имеет связи с рабочим LDAP сервером	В файле EDIMail.ini в секции [crypto] неверно указан url.	Поправить ini-файл.

Вид ошибки	Возможные причины возникновения	Способы устранения
	Настройки офисной сети клиента блокируют доступ для пользователя «XXXXX\LocalSystem» с компьютера «XXXXX» на сервер.	Проверить доступ (см. раздел 5.4.2). [V8]
Не приходят ответные файлы на сообщения о внебиржевых сделках	У клиента установлен Outlook, настроенный на тот же почтовый ящик, что и файловый шлюз. Этот Outlook может: • Перехватывать сообщения УФШ • Перекладывать по правилу сообщения шлюза в отдельную папку • Из-за настроек Outlook создает квитанции о прочтении на каждое рабочее сообщение и забивает почтовый ящик клиента	
Дублируются файлы много раз	В папке Progdata в файле mail.sqlite3 должны быть права на изменение. В нем ставятся отметки о пришедших сообщениях.	Проверить наличие соответствующих прав.
Не может быть определен путь к базам Валидаты	Ошибка в пути к базам.	Поправить настройки.
	Пути ведут к общим папкам, типа: local="file://\\dfs\HomeDir\local.gdbm	Это будет работать для консольного режима. Для работы в режиме сервиса нужно изменить скрипт startup.js, (добавить system(“net use …”); как описано в раздел 6.5.