

Небанковская кредитная организация
акционерное общество
«НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ»

Часто задаваемые вопросы Q&A
Файловый шлюз НРД.

Москва, 2021

СОДЕРЖАНИЕ

1.	Настройка	4
1.1.	Как можно разделить приём и отправку в ФШ для одного кода участника, чтобы для приёма использовался один сертификат, а для отправки другой?	4
1.2.	Есть ли встроенная возможность архивирования содержимого папок INBOX, SENT, ERROR?	5
1.3.	Можно ли поменять пути по умолчанию для файлов логов, конфига и базы данных? ...	5
1.4.	Работает ли ФШ с сетевыми каталогами/путями?	5
1.5.	Можно ли на один компьютер установить боевой и тестовый ФШ?	6
1.6.	Как перенести/скопировать настройки ФШ на другую машину или другому пользователю?	7
2.	Общие ошибки в ФШ	8
3.	Ошибки отправки пакетов	10
4.	Обработка транзитных квитанций	12
5.	Принципы работы ФШ	13
5.1.	Что произойдет, если ФШ закроется (завершит работу) в процессе приёма сообщения?	13
5.2.	Как приостановить отправку и прием документов (например, для удаления или переноса архивных сообщений сторонними средствами)?	13
5.3.	Что делать, если ФШ не принимает и не отправляет документы, при этом никаких ошибок не выдается?	14
5.4.	Что такое рассылки по маске lxxxxxxx.zip и #NOTIFxxxxxxxxxxxxxxxxxxxxxxx.zip? Может быть есть список и описание списка рассылок, которые нам могут приходиться через ФШ?	14
5.5.	Что будет если в момент загрузки файла в ФШ папка в OUTBOX будет содержать только файл txt (т.е. файл config.xml будет отсутствовать)?	14
5.6.	Можем ли мы задавать период (например, с 8-00 до 20-00), внутри которого будут выгружаться входящие сообщения с соответствующей периодичностью?	14
5.7.	В отношении выгрузки исходящих сообщений периодичность настраивается параметром «Время ожидания перед отправкой»?	14
5.8.	Есть ли функционал ФШ, позволяющий отправлять уведомления по email об отсутствии загрузки/выгрузки в течение определенного времени и о новых сообщениях в папке ERROR? 15	
5.9.	Чем отличаются файлы .LOCK и INBOX.LOCK?	15
5.10.	Что происходит с файлами и папками в папке OUTBOX после окончания загрузки в ФШ? 15	
5.11.	Какая пропускная способность ФШ?	16
5.12.	Как самостоятельно прочитать лог-файл ФШ?	16
6.	Интерфейс ФШ	17
6.1.	Как повторно загрузить входящий пакет?	17

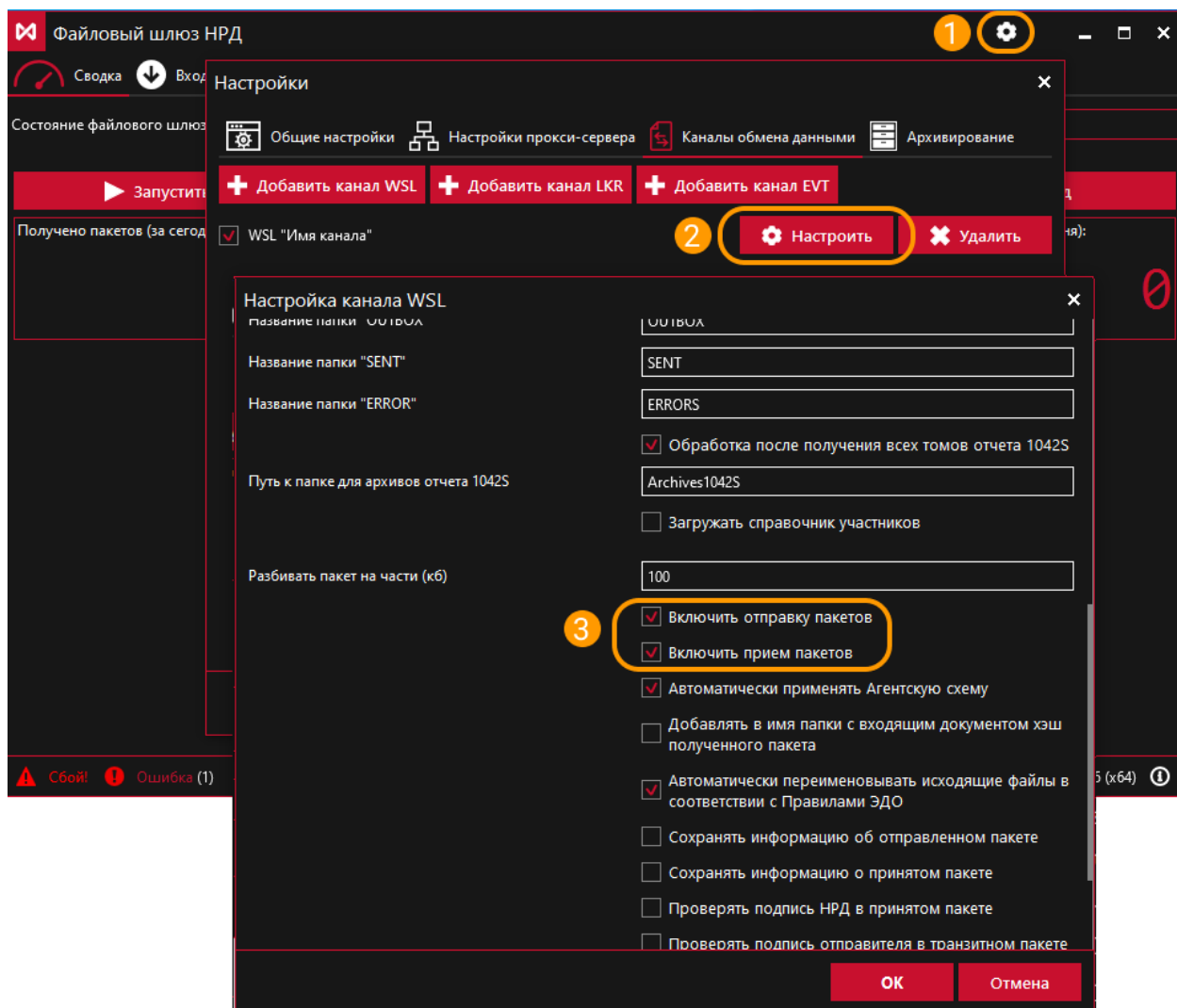
6.2.	Можно ли получить пакеты старше 14-ти дней?	17
7.	Криптография.....	18
7.1.	При использовании более одного профиля пользователя, как в рамках канала выбрать сертификат для подписи?	18
7.2.	Можно сохранять информацию проверки электронной подписи?.....	19
7.3.	Как проверить, что документ действительно подписан на сертификате НРД?	19
7.4.	Можно ли с помощью ФШ автоматически получать обновления СОС и/или сертификатов контрагентов? Нужны ли для этого дополнительные настройки/доступа?	21
7.5.	Как узнать какими ЭП были подписаны файлы во входящем пакете?	22
7.6.	Как реагировать на запись в журнале вида «skipped certificate...: not found in store».....	23
7.7.	Как реагировать на запись в журнале «Сертификат издателя не найден»	23
7.8.	Как реагировать на запись в журнале "Неверный контекст библиотеки или потоковой операции"	24
7.9.	Если получен новый сертификат, как заменить его в ФШ?	24
8.	ЭДО	25
8.1.	Какие требования предъявляются к наименованию файлов?	25
8.2.	Почему ответные сообщения или отчеты приходят раньше квитанций ЭДО?	25
8.3.	Можно ли обмениваться транзитными документами с контрагентом через Луч так, чтобы файлы дублировались в Файловый Шлюз?	26
8.4.	Что делать, если в течение дня приходят одноименные пакеты с разным содержимым?	26
8.5.	Можно ли получать только определенный тип пакетов?	27
8.6.	Какую проверку нужно сделать, чтобы узнать, какую информацию содержит файл? ...	28
8.7.	Идут ли через ФШ документы типа: счета-акты выполненных работ, счета-фактуры за оказанные услуги?	28
8.8.	Какой максимальный размер пакета может быть отправлен/принят через ФШ?	29
8.9.	В пакете типа CERRORxx могут содержаться разного рода ошибки? Где-то можно увидеть их перечень?	29
8.10.	Где в ФШ можно посмотреть, что документы доставлены клиенту/изменили статус?	
	30	
9.	Как обратиться в техническую поддержку НРД?	30

1. Настройка

1.1. Как можно разделить приём и отправку в ФШ для одного кода участника, чтобы для приёма использовался один сертификат, а для отправки другой?

Ответ:

У канала есть настройки "Включить приём пакетов" и "Включить отправку пакетов". На скриншоте ниже показано, как найти данные настройки:



Соответственно можно создать необходимое кол-во каналов под каждый криптопрофиль (для каждой ЭП нужно завести отдельный профиль в Справочнике сертификатов).

Оставить включенным прием пакетов только у какого-то одного канала, а у остальных оставить только отправку.

1.2. Есть ли встроенная возможность архивирования содержимого папок INBOX, SENT, ERROR?

Ответ:

Такой функциональности в ФШ нет. Нужно самостоятельно переносить/архивировать файлы или использовать стороннее ПО для этих целей.

1.3. Можно ли поменять пути по умолчанию для файлов логов, конфига и базы данных?

Ответ:

Можно изменить общий путь до папки конфигурации, для этого нужно запускать ФШ с ключом --data "ПУТЬ_К_ПАПКЕ" (ключ указывается при запуске из консоли или прописывается у ярлыка ФШ), подробнее можно прочитать в разделе "Консольная версия ФШ" Руководства пользователя ПО «Файловый шлюз НРД».

1.4. Работает ли ФШ с сетевыми каталогами/путями?

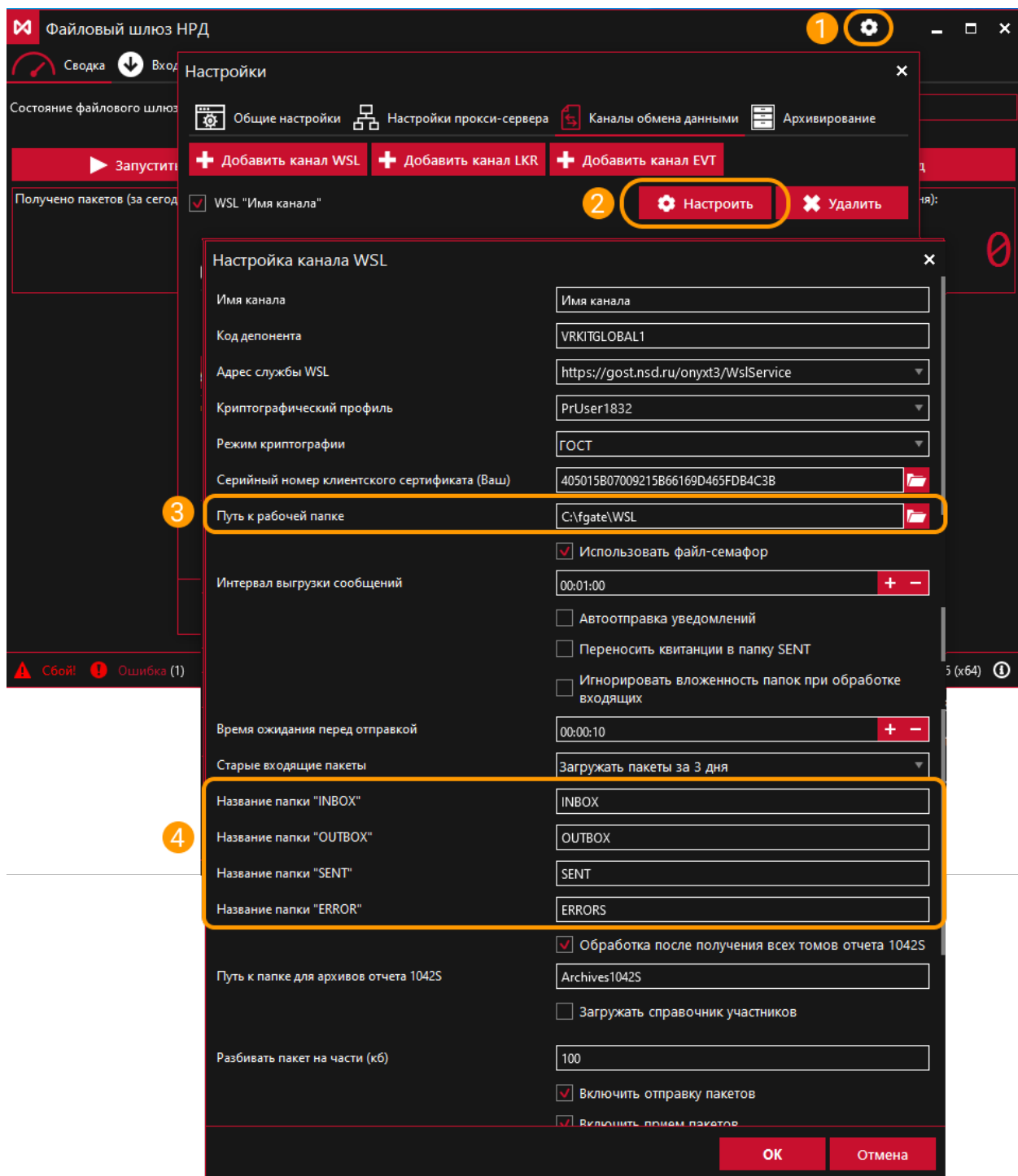
Ответ:

Работает, можно задать сетевой путь как всей «рабочей папке», так и отдельными её подпапкам (OUTBOX, INBOX и т.д.)

Для этого, вместо имени указанного в поле имени папки нужно указать нужный путь. Можно использовать как абсолютный/сетевой путь, так и относительный к рабочей папке.

Пример относительного пути: «..\OUTBOX» – в данном примере папка создастся на том же уровне, что и рабочая папка.

Пример указания абсолютного пути: «C:\ФШ\OUTBOX» – в данном примере папка создастся на диске С внутри папки ФШ, независимо от того, что указано в поле «Путь к рабочей папке».



1.5. Можно ли на один компьютер установить боевой и тестовый ФШ?

Ответ:

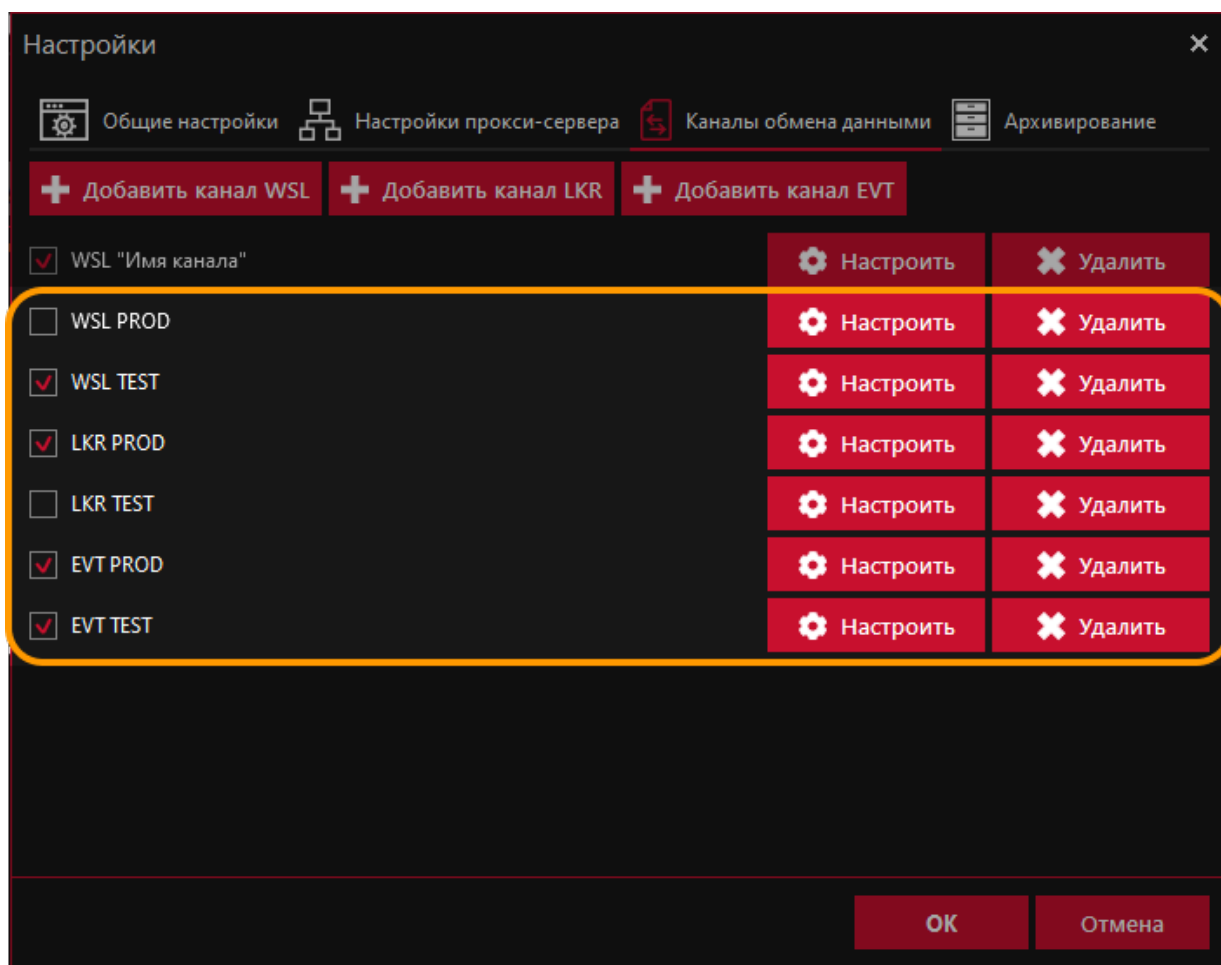
Можно, для этого достаточно в одном ФШ настроить отдельные каналы для боевого и тестового контуров.

Под ЭП боевого контура и ЭП тестового контура нужно завести отдельные профили в Справочнике сертификатов.

В ФШ создать каналы для профилей, в поле "Криптографический профиль" выбрать соответствующий профиль.

Сообщения будут подписываться головным сертификатом из этого профиля.

В одном ФШ можно использовать сколько угодно ЭП как тестовых, так и боевых.

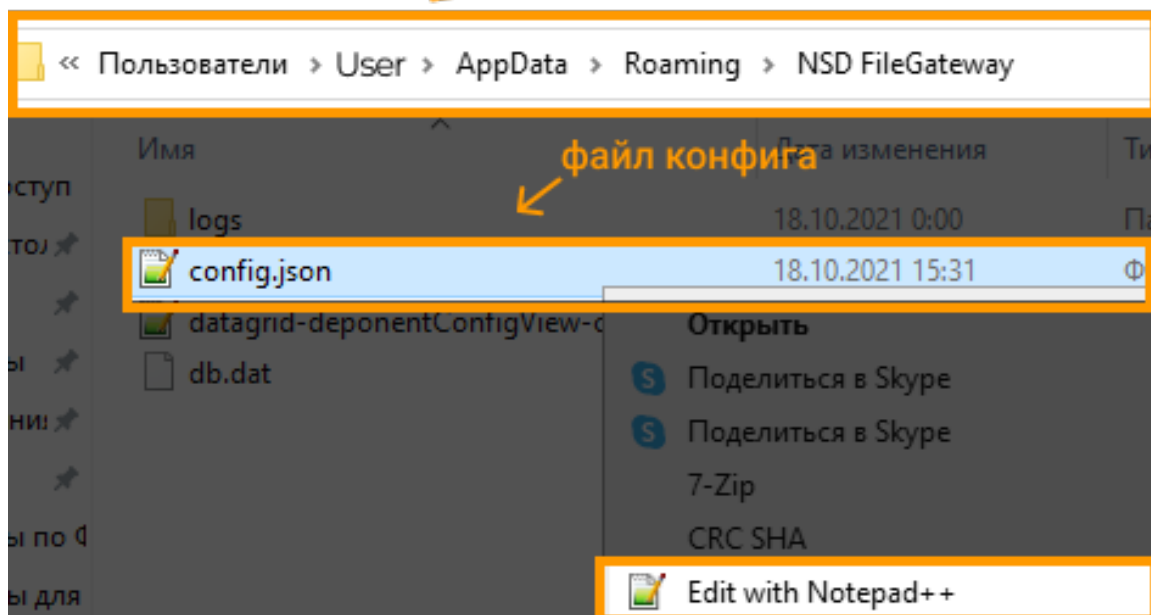


1.6. Как перенести/скопировать настройки ФШ на другую машину или другому пользователю?

Ответ:

Настройки хранятся в папке пользователя Windows, от имени которого запускается ФШ, в AppData "%AppData%\NSD FileGateway\". Файл "config.json" содержит все настройки, при его переносе нужно будет удостовериться в том, что настройки криптографии и пути до папок и базы данных корректные.

путь к файлу конфига



файл конфига

программа для
чтения файла конфига

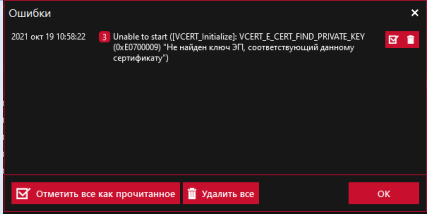
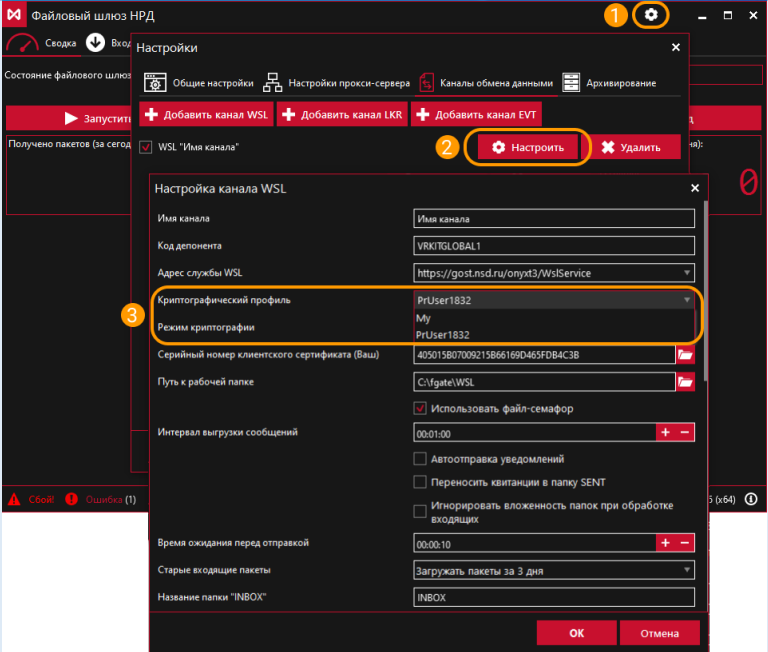
В случае если файл конфига повреждён или его структура не соответствует версии ФШ — файл будет перезаписан на настройки по умолчанию.

Файл "db.dat" хранит всю информацию о принятых/отправленных пакетах, если используется SQLite база данных. Если нужно избежать повторного скачивания ранее загруженных пакетов, данный файл нужно будет скопировать.

2. Общие ошибки в ФШ

Таблица 1.

Ошибки	Что предпринять
Unable to start ([VCERT_Initialize]: VCERT_E_CERT_FIND_PRIVATE_KEY (0xE0700009) «Не найден ключ ЭП, соответствующий данному сертификату»)	Проверьте, правильно ли указан профиль и режим криптографии в настройках канала.

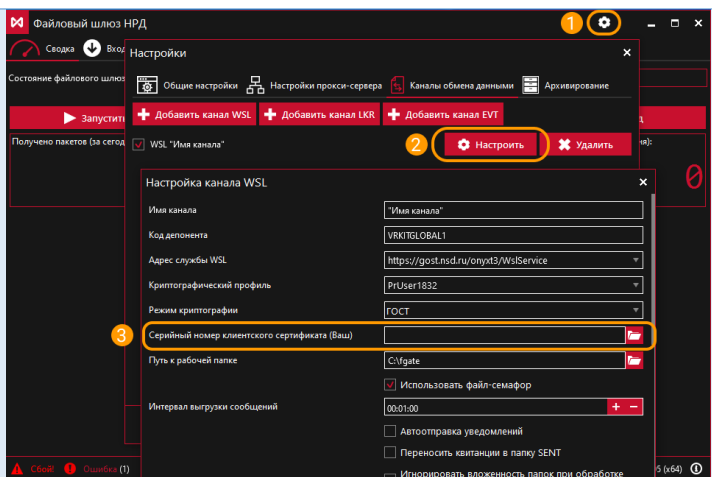
	 <p>Так же стоит убедиться, что носитель с закрытым ключом находится на месте (т.е. носитель вставлен в USB порт или ключ сохранен в реестре).</p>
<p>Ошибка: Unable to create ValidataCryptoProvider VCERT_E_INVALID_CONTEXT (0xE0700003) "Invalid cryptographic context"</p>	<p>Ошибка возникает в случаях, когда ФШ не может инициализировать крипто-профиль Справочника сертификатов. Нужно проверить что профиль и режим криптографии для каждого канала указаны верно.</p>
<p>Ошибка: Error calling "HttpSendRequest", code = 12029, message = "Не удается установить связь с сервером"</p>	<p>Причиной данной ошибки могут быть:</p> <ul style="list-style-type: none"> • Некорректные настройки антивируса • Некорректные настройки проксирующего ПО и оборудования • Запрет со стороны сетевого оборудование на установление соединений по протоколу TLS. <p>После устранения проблем перезапустите Windows на компьютере, на котором установлен ФШ. Если вышеперечисленные приемы не помогают, обратитесь в поддержку.</p>
<p>Ошибка: Error calling "HttpSendRequest", code = 12157, message = "Ошибка поддержки безопасных каналов" "An error occurred in the secure channel support"</p>	<p>Это стандартная сетевая ошибка. При её возникновении нужно удостовериться в доступности WEB-сервиса («Адрес службы WSL» в настройках WSL-канала), вбив этот адрес через браузер Internet Explorer, и проверить, что для канала верно указаны настройки криптографии (криптопрофиль и серийный номер вашего сертификата).</p>

	<p>Данная ошибка также возникает, если в локальной сети есть ограничения по криптографии с использованием сертификатов ГОСТ, например, ограничивающие политики GPO (в разделе <i>"Administrative Tools / Local Security Policy / Security Options"</i> есть политика <i>"Use FIPS compliant algorithms for encryption"</i>. Это означает - использовать (в частности для HTTPS) только алгоритмы, одобренные в США), либо установлены аналогичные ограничения на активном сетевом оборудовании. Если доступа нет, то воспользоваться рекомендациями из инструкции по настройке рабочего места → https://www.nsd.ru/upload/docs/edo/web_service_TLS.doc</p>
<p>Ошибка: Error calling "HttpSendRequest", code = 1223, message = "Операция была отменена пользователем." "The operation was canceled by the user."</p>	<p>Данная ошибка возникает, когда на стороне пользователя обрывается подключение к WEB-сервису ONYX. Причина может быть в Антивирусе, настройках Файрволла/Прокси или в каком-то другом ПО на машине пользователя. Проверьте настройки безопасности Антивируса/Файрволла/Прокси.</p>

3. Ошибки отправки пакетов

Таблица 2.

Ошибки	Что предпринять
<p>LKR-канал: Ошибка при отправке Error calling "HttpSendRequest", code = 12029, message = "Не удается установить связь с сервером"</p>	<p>Если сетевой доступ к кабинету Репозитория есть, то проблема в том, что указан "Серийный номер клиентского сертификата" в настройках LKR-канала. Поле нужно оставить пустым, оно заполняется только в случае использования «старого адреса» кабинета, начинающегося на edog/gost/edor/rsa.</p>

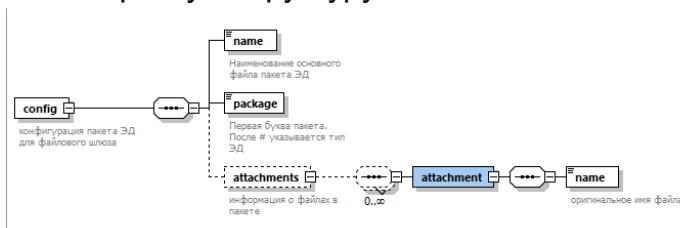


Файлы отправляемых документов из OUTBOX переносятся в папку ERRORS с ошибкой: Unrecognized message type (Unable to detect type of XML - root element is not recognized)

Причины этой ошибки могут быть следующие:

- 1) Документы нельзя отправлять непосредственно из OUTBOX. Нужно, чтобы файлы документов были внутри своей подпапки. Пример структуры: OUTBOX\<<подпапка>\<документ.xml> Название у подпапки может быть любым.
- 2) Если отправляете транзитный документ, в подпапку рядом с отправляемым документом обязательно должен быть добавлен WINF.XML
- 3) если документ не транзитный, необходимо помнить, что ФШ умеет распознавать по корневому тегу XML файла не все типы электронных документов.

Но любой известный НРД тип электронного документа, кроме транзитного, можно отправить из ФШ с использованием настроечного файла config.xml, который имеет очень простую структуру:



Настроечный файл config.xml выкладывается в ту же папку в папке OUTBOX, в которую выложен отправляемый файл. Файл config.xml должен содержать:

- В теге <name> - оригинальное имя отправляемого файла
- В теге <package> - первую букву в имени пакета ЭДО, в котором должен быть

	<p>отправлен файл (именно по этой букве НРД определяет тип документа). Если первый символ #, следующие 5 символов должны представлять собой тип ЭД.</p> <ul style="list-style-type: none"> Блок config/attachments заполняется только в том случае, если для данного типа документа предусмотрены вложения. В каждом теге attachment указывается оригинальное имя файла вложения
<p>Ошибка при отправке "[ERRORXML_NO_RECIPIENT_CERTIFICATE_ERROR] Не найдено ни одного сертификата для получателя XXXXXXXXXXXX"</p>	<p>Ошибка возникает в случае отправки зашифрованного сообщения (шифрование используется только при отправке транзитных документов закрытым конвертом), когда проверяется наличие действующего сертификата получателя в профиле Справочника участников и справочнике "Участники транзита" в ФШ.</p> <p>Причина может быть, как в отсутствии сертификата, так и в том, что действие сертификата ограничено доверенностью в рамках справочника «Участники транзита». Если доверенность введена корректно, необходимо обратиться в поддержку или к личному менеджеру.</p>

4. Обработка транзитных квитанций

Таблица 3.

Ошибки	Что предпринять
<p>Проблема с сертификатом: "По указанному сертификату {...} не удалось определить отправителя"</p>	<p>Ошибка обычно говорит о том, что в ЭДО НРД нет привязки пользователя с указанным сертификатом к указанному коду депонента. Возможно, истек срок доверенности ЭДО.</p> <p>С этой ошибкой нужно обратиться в тех. поддержку НРД.</p>
<p>Ошибка - «ERRORXML_NO_RECIPIENT_CERTIFICATE_ERROR File W0424841 is not signed with any appropriate deponent certificate»</p>	<p>Ошибка сигнализирует о том, что на стороне конечного получателя транзита не удалось успешно проверить подпись файла в пакете. Если конечный получатель также использует ФШ, причина может быть в том, что файл подписан сертификатом контрагента, которого нет в справочнике «Участники транзита» либо для</p>

сертификата добавлена доверенность, срок действия которой закончился или ещё не наступил.

5. Принципы работы ФШ

5.1. Что произойдет, если ФШ закроется (завершит работу) в процессе приёма сообщения?

Ответ:

Файловый шлюз делает запись в БД о том, что сообщение принято, уже после успешной загрузки на диск файлов пакета.

Если система оборвёт процесс после записи файлов на диск и до того как произойдет запись в базу, то при повторном включении Файловый шлюз повторно загрузит сообщение на диск, добавив постфикс к имени папки пакета.

Вероятность попасть в такую ситуацию мала, так как запись в базу и запись файлов из памяти на диск занимает мало времени (миллисекунды) и обычно записи успевают отработать.

5.2. Как приостановить отправку и прием документов (например, для удаления или переноса архивных сообщений сторонними средствами)?

Ответ:

Для приостановки работы канала ФШ нужно использовать файлы-семафоры (LOCK файлы). Для приостановки приема или отправки достаточно создать файл-семафор, а для восстановления работы канала удалить его.

Файловый шлюз использует два файла-семафора:

— ".LOCK" используется для работы с файлами из папок OUTBOX, SENT и ERROR

— "INBOX.LOCK" используется для INBOX и ERROR

Оба файла создаются в корне "рабочей папки", указанной в настройках канала. Перед созданием нужно проверить наличие файла-семафора, созданного Файловым шлюзом, если он есть, то нужно подождать или повторить попытку создания, когда он будет удален Файловым шлюзом.

Соответственно, если кто-то другой создаст эти файлы, то ФШ будет ждать, пока их не удалят для продолжения работы с файлами.

Так же при перезапуске Файловый шлюз попытается принудительно удалить файлы-семафоры. То есть если файл-семафор был создан заранее до запуска ФШ, то он всё равно будет удалён.

5.3. Что делать, если ФШ не принимает и не отправляет документы, при этом никаких ошибок не выдается?

Ответ:

Проверьте, не остались ли в рабочей папке канала файлы-семафоры INBOX.LOCK и .LOCK. Они могли остаться там при сбое ПО и привести к тому, что ФШ не будет принимать и отправлять документы. В этом случае эти файлы нужно удалить вручную.

5.4. Что такое рассылки по маске lxxxxxxx.zip и #NOTIFxxxxxxxxxxxxxxxxxxxxxxxx.zip? Может быть есть список и описание списка рассылок, которые нам могут приходиться через ФШ?

Ответ:

В Руководстве пользователя ПО «Файловый шлюз НРД» в разделе «Правила наименования файлов ЭД» приведен первый символ в наименовании пакета. По нему можно определить, какой тип документа был получен. Например, если первая буква L – это опись, если первые буквы #NOTIF – это информационное сообщение.

5.5. Что будет если в момент загрузки файла в ФШ папка в OUTBOX будет содержать только файл txt (т.е. файл config.xml будет отсутствовать)?

Ответ:

Если ФШ без config.xml не поймет, какого типа файл должен быть отправлен (а понимает он это по корневому тегу в XML, причем «знает» он не все корневые теги), он не сможет сформировать пакет, и файл из OUTBOX\ABC будет перемещен в ERRORS\ABC.

5.6. Можем ли мы задавать период (например, с 8-00 до 20-00), внутри которого будут выгружаться входящие сообщения с соответствующей периодичностью?

Ответ:

Нет, период задать нельзя.

5.7. В отношении выгрузки исходящих сообщений периодичность настраивается параметром «Время ожидания перед отправкой»?

Ответ:

Это не периодичность отправки. Это время, которое ФШ ждет, пока в подпапку папки OUTBOX будут добавлены все файлы, предназначенные для отправки, например, все транзитные файлы, перечисленные в WINF.XML, или аттачмент, указанный в репозитарном FrML файле. И только после истечения указанного времени ФШ начнет проверять файлы, и вот тогда, если каких-то из указанных файлов в папке не будет, содержимое папки будет перемещено в папку ERROR.

Причем если в течение времени ожидания перед отправкой в папке с файлами произошли какие-то изменения, время ожидания начинает отсчитываться по новой.

5.8. Есть ли функционал ФШ, позволяющий отправлять уведомления по email об отсутствии загрузки/выгрузки в течение определенного времени и о новых сообщениях в папке ERROR?

Ответ:

Нет, в ФШ нет механизма, который бы мог уведомлять внешнюю систему о своих событиях, в том числе по почте.

5.9. Чем отличаются файлы .LOCK и INBOX.LOCK?

Ответ:

Оба файла являются семафорами и размещаются в корне рабочей папки канала.

.LOCK используется при отправке (папка OUTBOX), INBOX.LOCK – при приёме (папка INBOX). Оба этих файла внутри пустые.

Пока не удален .LOCK, ФШ не осуществляет отправку документов.

Пока не удален INBOX.LOCK, ФШ не осуществляет прием документов.

5.10. Что происходит с файлами и папками в папке OUTBOX после окончания загрузки в ФШ?

Ответ:

В случае успешной отправки пакета все файлы, участвовавшие в формировании пакета, вместе с подписями перемещаются в подпапку в папке SENT, в случае ошибки – в подпапку папки ERRORS.

Путь к папкам назначения будет вычисляться следующим образом:

- Файлы, отправленные из корня папки OUTBOX, будут перемещены в папку SENT или ERRORS.
- Файлы, отправленные из подпапки OUTBOX\ABC, будут перемещены в папку SENT\ABC или ERRORS\ABC.
- Файлы, отправленные из подпапки OUTBOX\ABC\DEF, будут перемещены в папку SENT\ABC\DEF или ERRORS\ABC\DEF.

В случае, если папка уже существует, то формируется новое уникальное название папки путем добавления суффикса _N, где N – десятичное целое число. Нумерация начинается с 1. Если же файл или папка с полученным именем уже существует, то число увеличивается на 1. Процесс повторяется при необходимости до тех пор, пока не будет сформировано уникальное имя файла или папки.

Папка из OUTBOX с перемещенными в SENT или ERRORS файлами в общем случае удаляется. Но есть исключения:

- в случае если в подпапке с сообщением были «лишние» файлы, которые не были связаны с основным файлом, то папка с этими несвязанными файлами останется в OUTBOX.
- если файл транзита был успешно прочитан, но не было, например, сертификата контрагента, то по аналогии с успешной отправкой перенесётся в ошибки только то, что относится к пакету, а несвязанные файлы останутся в папке в OUTBOX.
- при этом если не удалось определить тип xml файла или если winf.xml в транзите повреждён, то в ERRORS переносится вся папка целиком, независимо от того, связаны файлы или нет.

5.11. Какая пропускная способность ФШ?

Ответ:

Пропускная способность или возможность обработки входящих/исходящих сообщений в ФШ зависит от технических возможностей компьютера, на котором работает файловый шлюз и расположена его база данных.

В среднем ФШ может обработать не меньше 2,5 тысяч сообщений в час входящих и столько же исходящих.

5.12. Как самостоятельно прочитать лог-файл ФШ?

Ответ:

Рассмотрим на примере:

```
#2816 2077-12-10 09:08:07.6543 T8 DEBUG WSL Production: fetching incoming messages for 2077 дек 10
```


- #2816 — ID процесса ФШ в операционной системе
- 2077-12-10 09:08:07.6543 — время события
- T8 — номер потока/треда, в рамках которого происходит событие
- DEBUG — уровень логирования или тип события. Бывает TRACE, DEBUG, INFO, WARN, ERROR, FATAL
- WSL — тип канала ФШ. бывает WSL, LKR, EVT
- Production — наименование канала, указывается в настройках канала
- fetching incoming messages for 2077 дек 10 — сообщение, чёткой структуры нет — может быть любым.

6. Интерфейс ФШ

6.1. Как повторно загрузить входящий пакет?

Ответ:

Если входящий пакет был принят с ошибкой, его можно принять повторно, но сделать это можно только вручную. Для этого на закладке «Входящие пакеты» нужно выбрать сообщение в статусе «Ошибка» и в контекстном меню, открываемом правой кнопкой мыши, выбрать пункт «Загрузить заново».

Если входящий пакет ранее был принят без ошибок, повторно его загрузить нельзя.

6.2. Можно ли получить пакеты старше 14-ти дней?

Ответ:

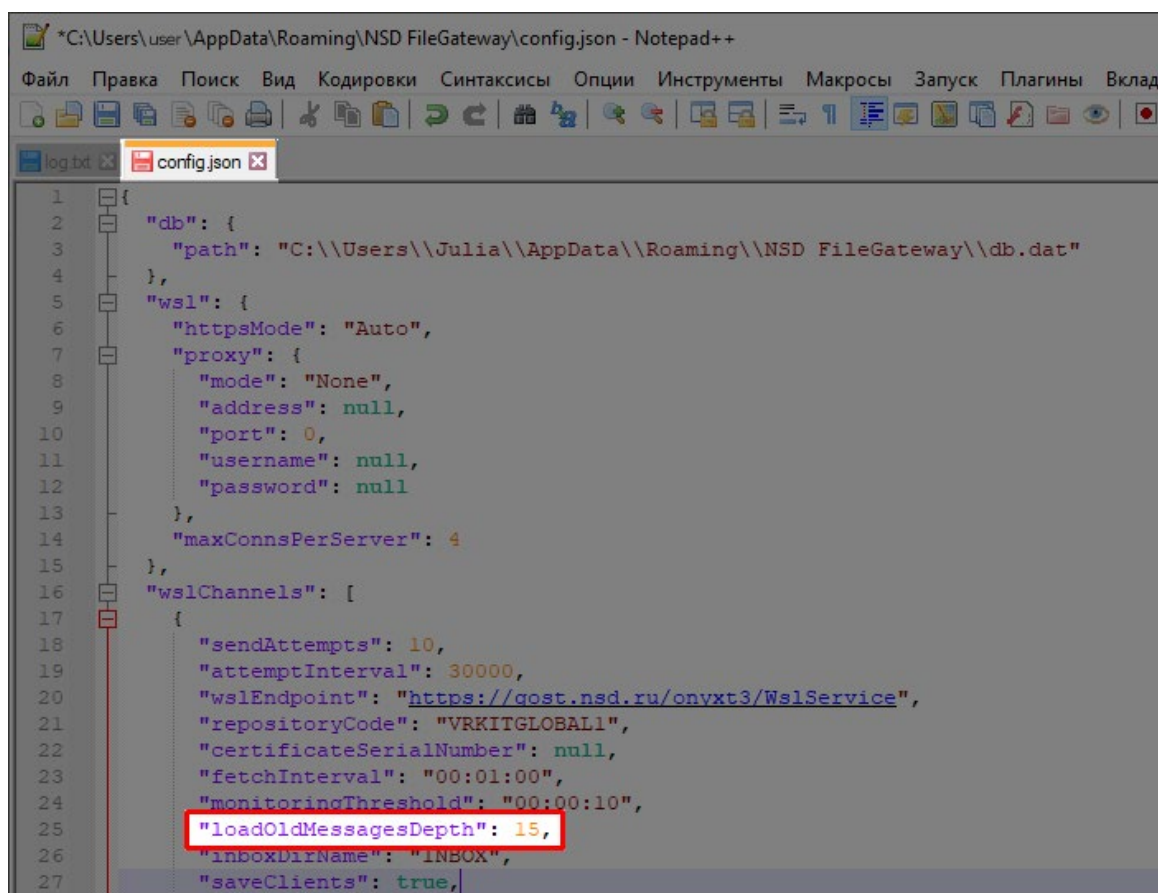
Да, такое возможно, для этого нужно вручную изменить параметр в конфигурационном файле ФШ.

Конфигурационный файл ФШ (config.json) по умолчанию находится в папке AppData пользователя Windows: «%AppData%\NSD FileGateway\». Нужно перейти в эту папку или открыть «Папку конфигурации» из настроек ФШ.

Перед редактированием настроек нужно завершить работу ФШ (иначе при перезапуске ФШ перезапишет ваши изменения). Также рекомендуется сделать копию файла настроек, чтобы в случае ошибки можно было вернуть предыдущие настройки.

После открытия файла config.json в любом текстовом редакторе нужно найти в блоке wslChannels параметр loadOldMessagesDepth. В

нем указать необходимое целое число дней (см. скриншот) и сохранить файл конфигурации.



```
1 {
2   "db": {
3     "path": "C:\\Users\\Julia\\AppData\\Roaming\\NSD FileGateway\\db.dat"
4   },
5   "wsl": {
6     "httpsMode": "Auto",
7     "proxy": {
8       "mode": "None",
9       "address": null,
10      "port": 0,
11      "username": null,
12      "password": null
13    },
14    "maxConnsPerServer": 4
15  },
16  "wslChannels": [
17    {
18      "sendAttempts": 10,
19      "attemptInterval": 30000,
20      "wslEndpoint": "https://gost.nsd.ru/ovvxt3/WslService",
21      "repositoryCode": "VRKITGLOBAL1",
22      "certificateSerialNumber": null,
23      "fetchInterval": "00:01:00",
24      "monitoringThreshold": "00:00:10",
25      "loadOldMessagesDepth": 15,
26      "inboxDirName": "INBOX",
27      "saveClients": true,
```

После запуска Файловый шлюз запросит и проверит наличие всех пакетов за указанное кол-во дней назад. Те пакеты, о которых не было записи о загрузке в базе данных (файл db.dat), будут загружены.

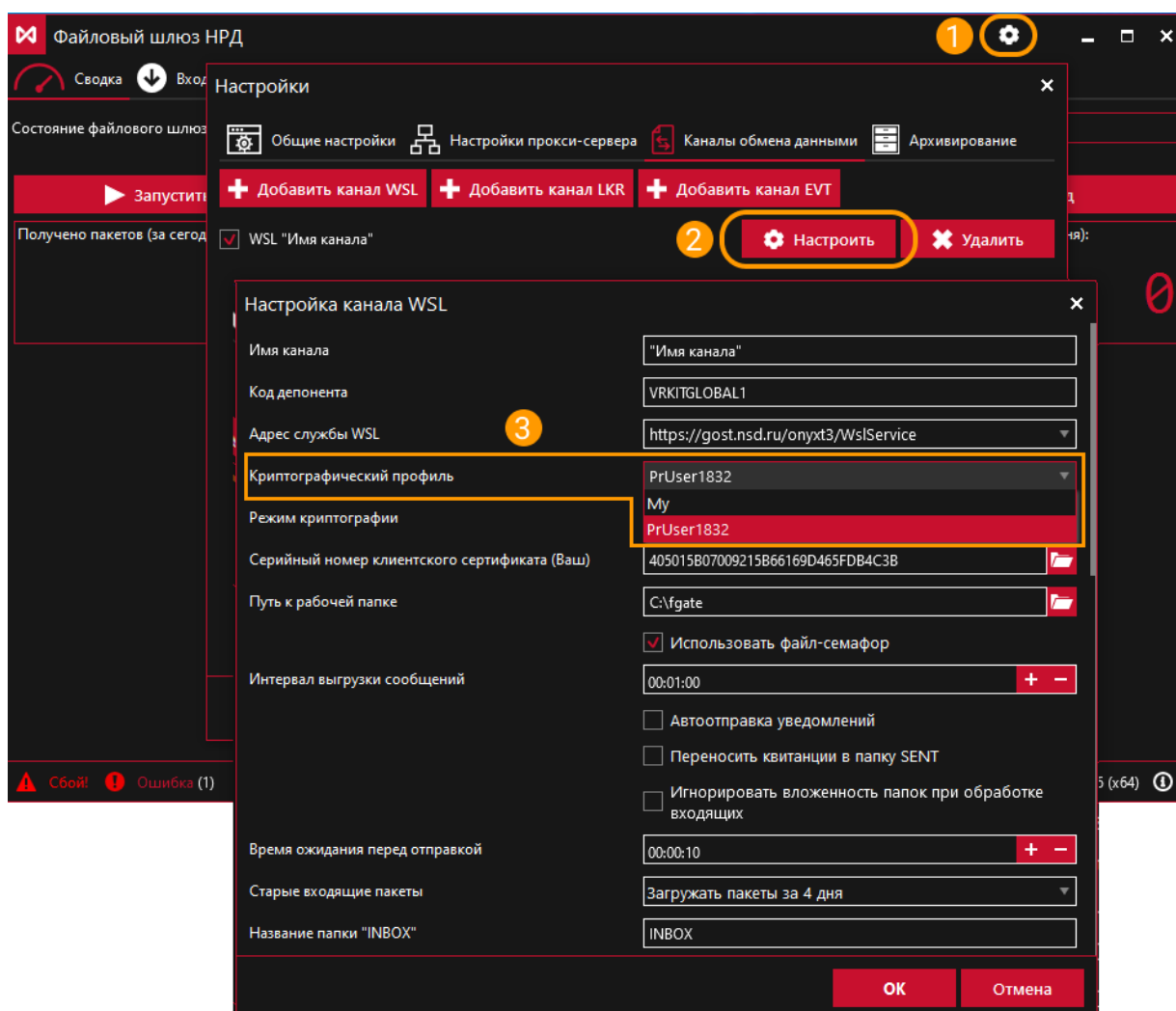
Для того чтобы вернуть настройки ФШ, достаточно открыть окно настроек и применить их, нажав кнопку «ОК».

7. Криптография

7.1. При использовании более одного профиля пользователя, как в рамках канала выбрать сертификат для подписи?

Ответ:

В настройках канала в поле "Криптографический профиль" нужно выбрать из выпадающего списка вместо значения "My" название профиля Справочника сертификатов. Для подписи/шифрования будет использоваться головной сертификат из выбранного профиля.



7.2. Можно сохранять информацию проверки электронной подписи?

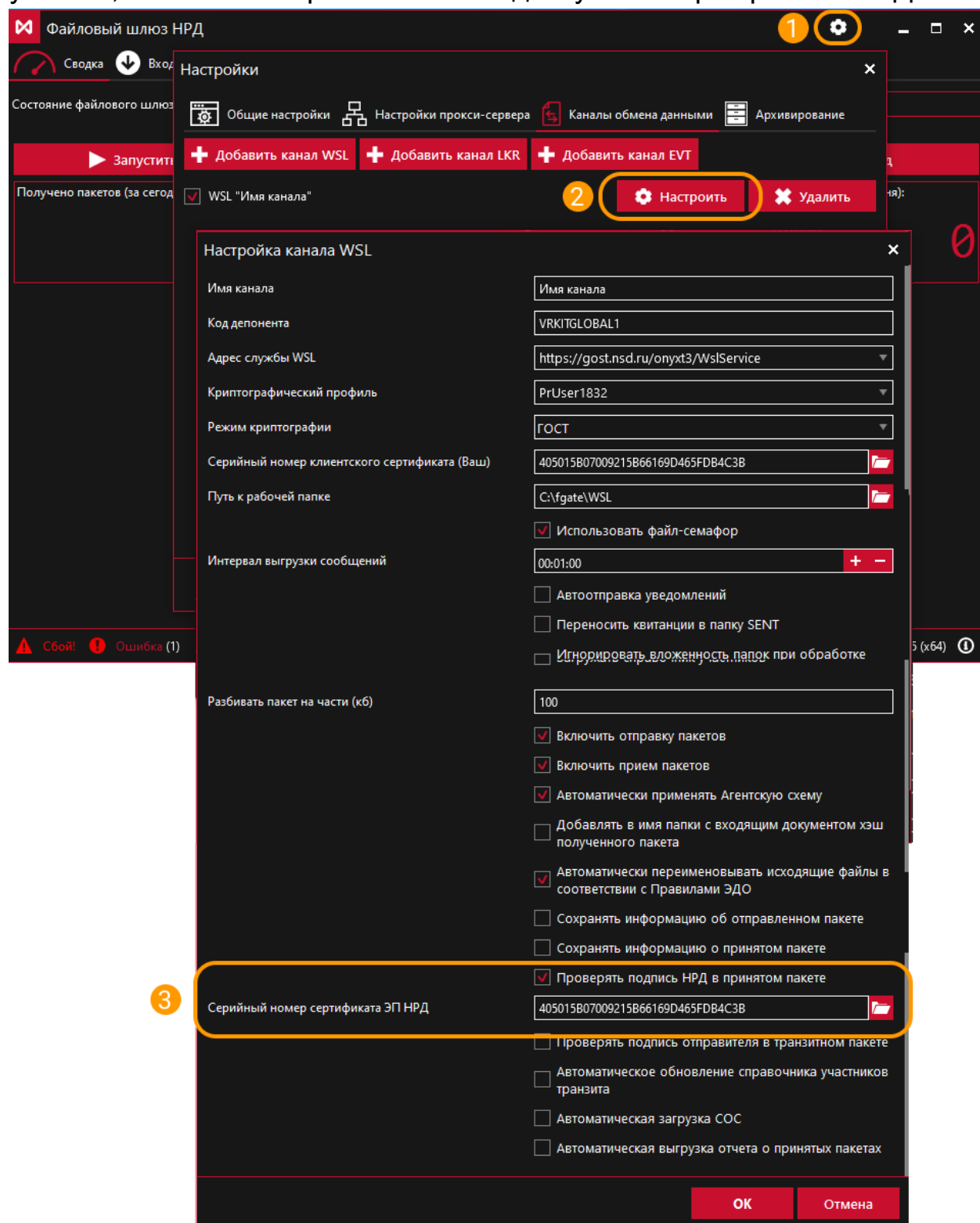
Ответ:

В настройках канала ФШ есть опция "Сохранять информацию о принятом пакете". Если её включить, то в папке с загруженным пакетом будет создаваться файл `packageInfo.xml` с информацией о пакете, в том числе там будут указаны данные о сертификатах электронной подписи принятых файлов.

7.3. Как проверить, что документ действительно подписан на сертификате НРД?

Ответ:

Для проверки подписи НРД нужно для канала включить настройку "Проверять подпись НРД в принятом пакете", также нужно будет указать, а точнее выбрать из списка доступных сертификаты НРД.

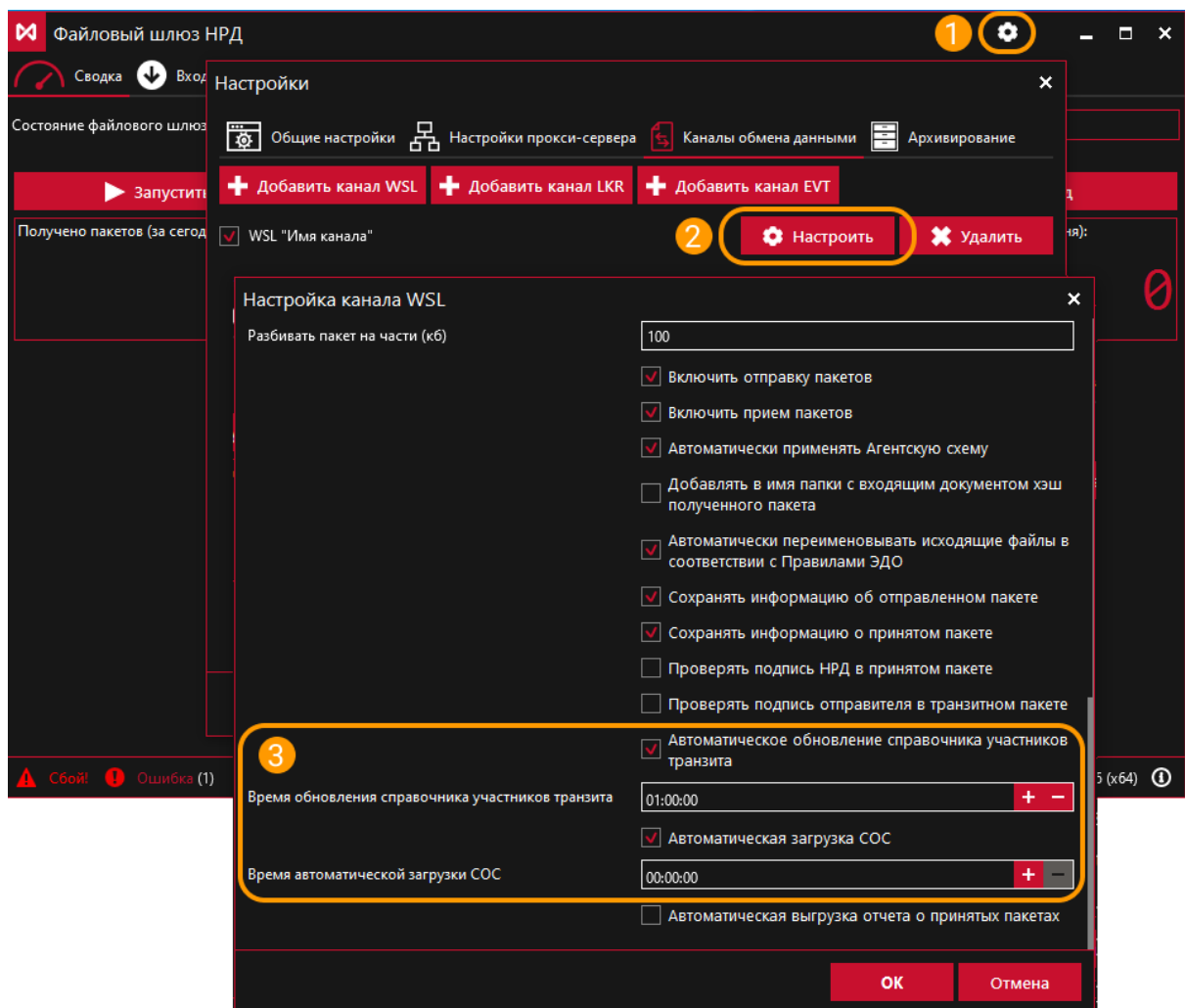


При этом нужно самостоятельно следить за выходом новых сертификатов НРД и своевременно обновлять/добавлять новые значения серийного номера сертификата в настройках ФШ. Если этого не делать вовремя, то все пакеты будут переноситься в папку ERROR с ошибкой о неуспешной проверке подписи НРД.

7.4. Можно ли с помощью ФШ автоматически получать обновления СОС и/или сертификатов контрагентов? Нужны ли для этого дополнительные настройки/доступа?

Ответ:

Если включить в настройках канала WSL «Автоматическая загрузка СОС» и/или «Автоматическое обновление справочников участников транзита», то в указанное в настройках время автоматически будут запрашиваться обновления.



Обновления СОС и Сертификаты контрагентов будут приходить отдельным пакетом ЭДО и автоматически добавляться в Справочник сертификатов для указанного в канале крипто-профиля, никаких дополнительных настроек или доступов, помимо имеющихся, для этого не требуется.

Необходимо только учесть, что операции обновления справочника участников транзита и СОС должны быть разнесены по времени, в

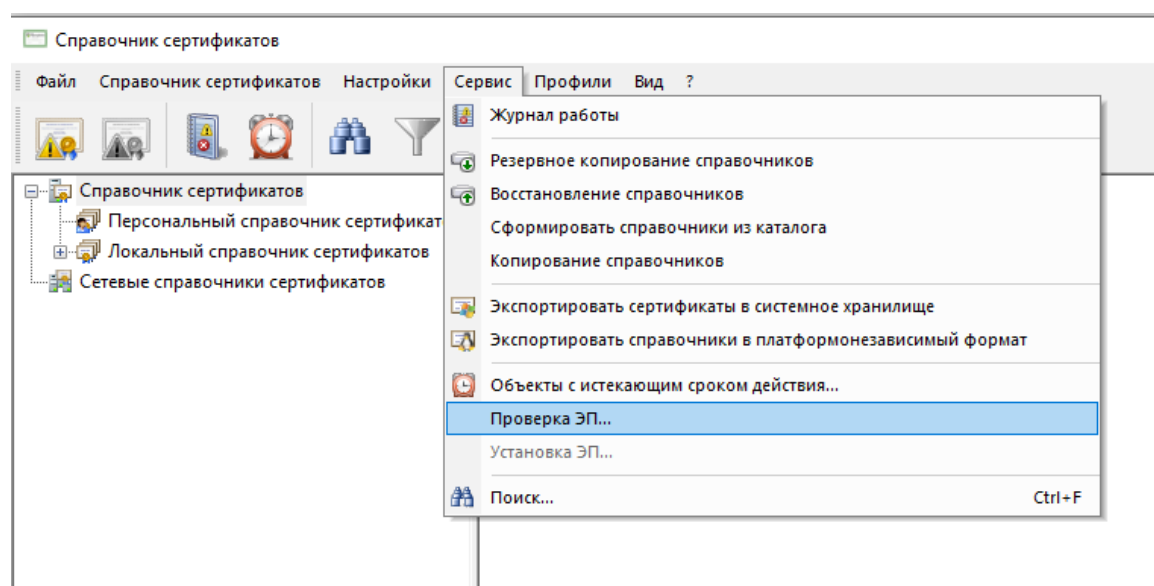
противном случае может возникнуть ошибка при выполнении одной из операций либо ошибка выполнения обеих операций.

7.5. Как узнать какими ЭП были подписаны файлы во входящем пакете?

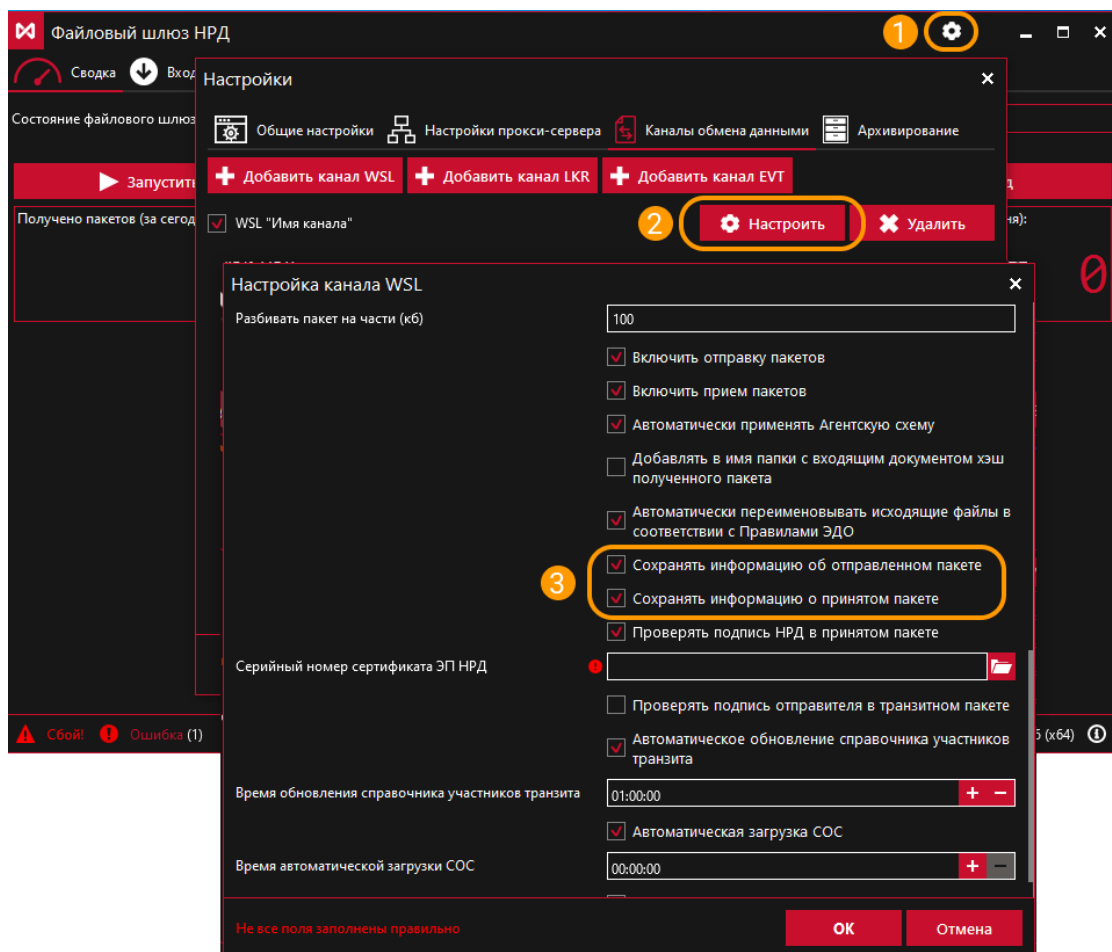
Ответ:

Для каждого файла внутри папки пакета сохраняется файл с отсоединённой ЭП (*.SGN), которую можно проверить с помощью средств Справочника сертификатов.

Для этого нужно в верхнем меню Справочника сертификатов выбрать пункт Сервис → "Проверка ЭП...".



Также, если включить настройку канала "Сохранять информацию о принятом пакете", то в папке пакета будет создан файл "packageInfo.xml", в котором будет информация обо всех подписях принятых файлов.



7.6. Как реагировать на запись в журнале вида «skipped certificate...: not found in store»

Такая запись в логе говорит о том, что по указанному сертификату получателя не обновился соответствующий СОС и соответственно по этому сертификату не будет произведено шифрование пакета для получателя при отправке транзитного пакета закрытым конвертом. Решается эта проблема перезагрузкой ФШ на стороне Отправителя. В редких случаях дополнительно требуется выполнить в Справочнике сертификатов «Экспорт сертификатов в системное хранилище» - выполняется при закрытом ФШ и в случае, если ошибка «not found in store» повторяется после перезагрузки ФШ.

7.7. Как реагировать на запись в журнале «Сертификат издателя не найден»

Ошибка вида «[VCERT_AddCRL]: VCERT_E_CERT_MISSING (0xE0700035) "Сертификат издателя не найден» говорит об отсутствии одного из корневых сертификатов Издателей либо об истечении срока действия СОС Издателя. Данная ошибка возникает при попытке добавить новый сертификат в ручном режиме через интерфейс ФШ или при автоматическом обновлении

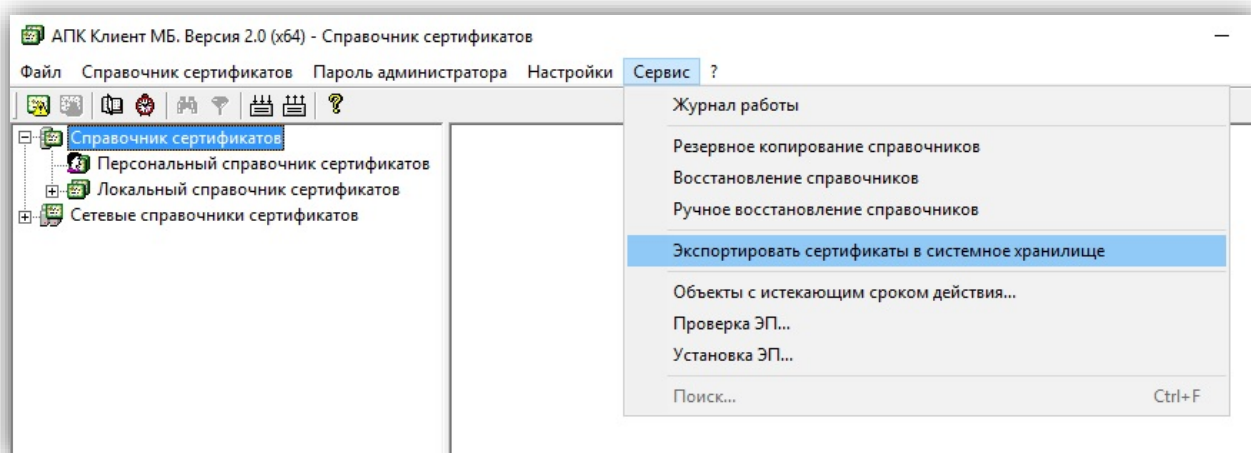
справочника «Участники транзита», когда актуализируется информация по имеющимся сертификатам.
 Решается эта проблема либо добавлением отсутствующего корневого сертификата Издателя, либо обновлением необходимых СОС средствами ФШ или Справочника сертификатов.

7.8. Как реагировать на запись в журнале "Неверный контекст библиотеки или потоковой операции"

Ошибка вида VCERT_E_INVALID_CONTEXT (0xE0700003) "Неверный контекст библиотеки или потоковой операции" возникает, если в настройках канала ФШ выбран неверный профиль Справочника сертификатов, в котором отсутствует указанный в параметре «Серийный номер клиентского сертификата».


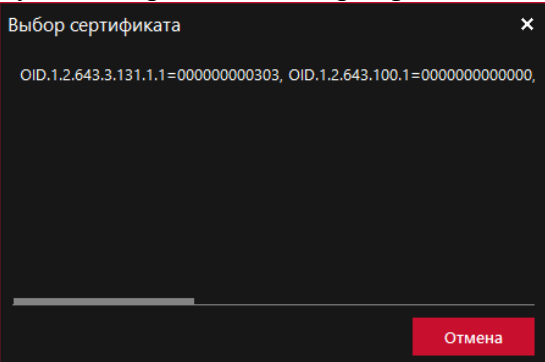
7.9. Если получен новый сертификат, как заменить его в ФШ?

- Выключите ФШ.
- Загрузите новый сертификат в Справочник сертификатов либо в имеющийся профиль, либо создайте для него новый. Запомните имя криптографического профиля для этого сертификата.
- После окончания импорта сертификата в Справочнике сертификатов **обязательно** выполните пункт меню «Сервис – Экспортировать сертификаты в системное хранилище» – данная операция должна завершиться без ошибок.



- Закройте Справочник сертификатов.
- Запустите ФШ.
- Для каждого из каналов, для которых использовался старый сертификат, актуализируйте следующие настройки:

Криптографический профиль	Выбрать новый криптографический профиль
Режим криптографии	Тип криптографии нового сертификата

Серийный номер клиентского сертификата (Ваш)	Серийный номер клиентского сертификата. При нажатии на кнопку  откроется окно, в котором нужно выбрать новый сертификат: 
--	---

Примечание: Запрашивать выпуск нового сертификата необходимо заблаговременно. Настоятельно рекомендуется перед использованием нового сертификата ФШ уведомить контрагентов, с которыми Вы обмениваетесь транзитными документами закрытым конвертом, о смене Вашего сертификата и попросить их нажать в ФШ кнопку «Загрузить сертификаты» на форме «Участники транзита», чтобы получить открытую часть ключа вашего сертификата. Если контрагенты не используют ФШ, передайте им открытую часть ключа нового сертификата любым удобным способом. В противном случае при использовании нового сертификата ваш ФШ не сможет расшифровать принятые транзитные пакеты, отправленные закрытым конвертом, т.к. они будут зашифрованы на старом сертификате.

8. ЭДО

8.1. Какие требования предъявляются к наименованию файлов?

Ответ:

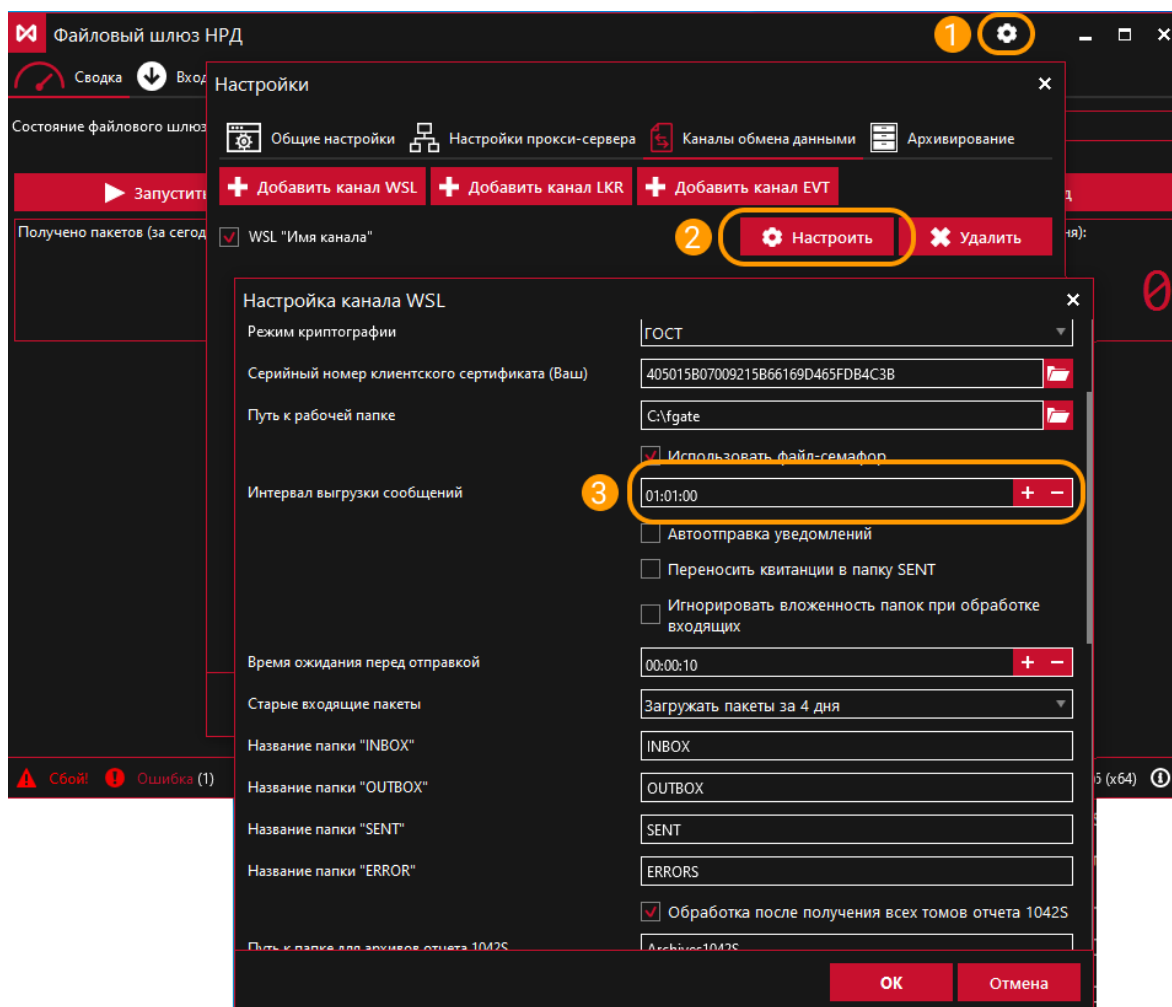
В имени файла могут содержаться только символы: '0'..'9', 'A'..'Z', '.', ' ', '_', '-', '(', ')', '[', ']', '~', '#'. Полный путь к файлу (т.е. Имя_каталога+Имя_файла) не должен превышать 255 символов. . Это относится ко всем файлам внутри пакета.

8.2. Почему ответные сообщения или отчеты приходят раньше квитанций ЭДО?

Ответ:

Сообщения из НРД не всегда отправляются в том же порядке, в котором они были сгенерированы во внутренних системах НРД. Это связано с многопоточностью обработки сообщений в системах и в ЭДО НРД. Этот факт надо учитывать при обработке сообщений,

поступающих из НРД. В ФШ можно увеличить интервал времени (см. рисунок), с которым он забирает исходящие из НРД сообщения. Тогда вероятность того, что отчет придет раньше квитанции, станет меньше.



8.3. Можно ли обмениваться транзитными документами с контрагентом через Луч так, чтобы файлы дублировались в Файловый Шлюз?

Ответ:

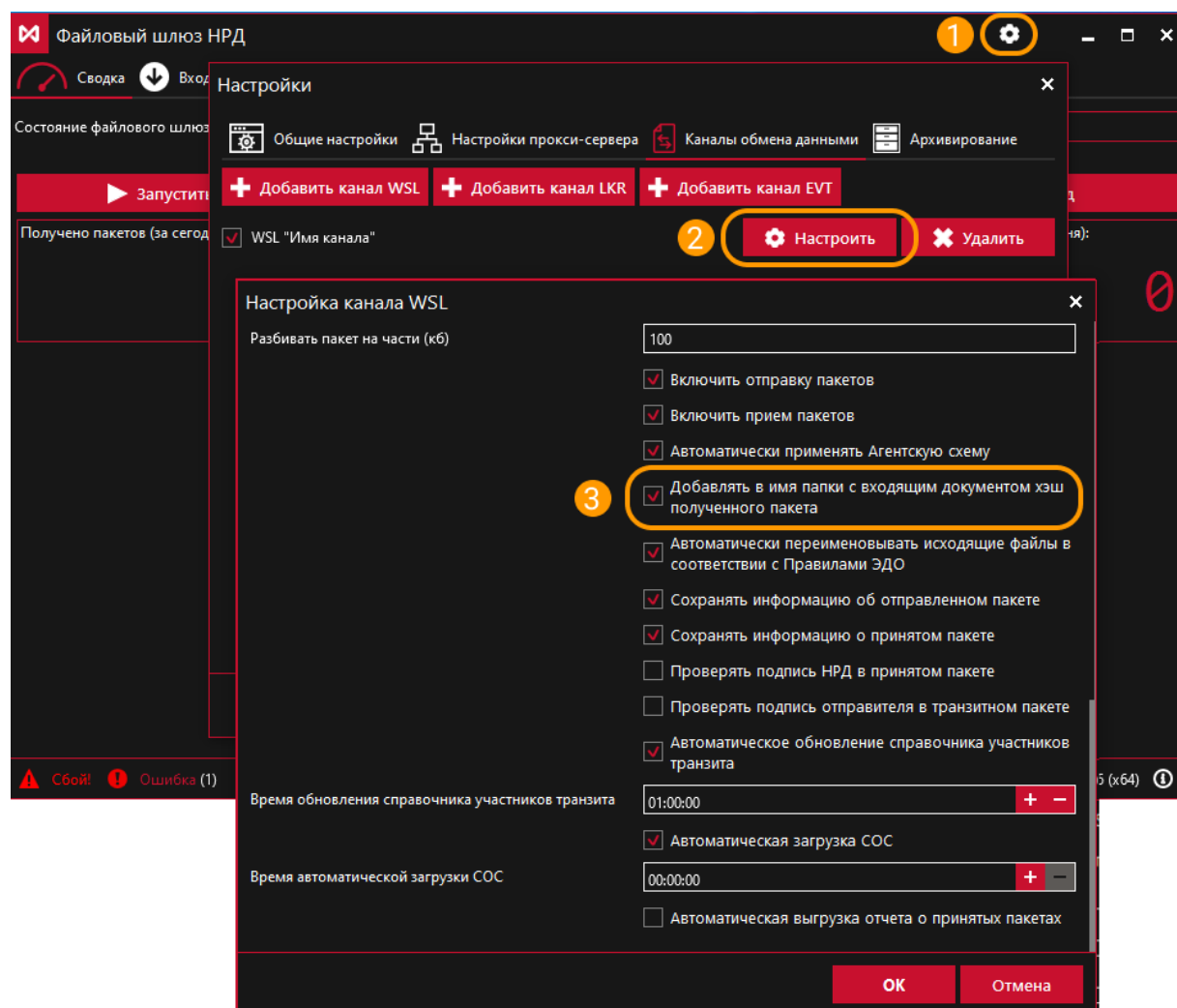
Прием/отправку транзитных документов поддерживают и Луч, и ФШ. Транзитный пакет, отправленный контрагентом А контрагенту В, может быть скачан контрагентом В и через Луч, и через ФШ - никаких ограничений для этого нет.

8.4. Что делать, если в течение дня приходят одноименные пакеты с разным содержимым?

Ответ:

Это нормальная ситуация, названия пакетов не уникальны и могут совпадать в течении одних суток. В случае, если в целевой папке уже

есть папка с таким же названием, то ФШ автоматически добавляет в конец названия загружаемой папки постфикс (пример названия с постфиксом: W01A0001_1). Если требуется уникальность имен папок для принимаемых пакетов, то в настройках канала можно включить настройку "Добавлять в имя папки с входящим документом хэш полученного пакета".



8.5. Можно ли получать только определенный тип пакетов?

Ответ:

Такой возможности нет. Файловый шлюз загружает все пакеты в рамках кода участника.

Но можно по наименованию папки пакета частично определить его тип. В Руководстве пользователя для ФШ есть таблица соответствия, какая первая буква в имени пакета к какому типу документа относится.

Также можно в настройках канала WSL поставить флаг «Сохранять информацию о принятом пакете». Тогда в каждой подпапке папки INBOX будет создаваться файл packageInfo.xml, в котором отображены все свойства и типы принятых документов. Тип документа находится в теге doctype.

8.6. Какую проверку нужно сделать, чтобы узнать, какую информацию содержит файл?

Ответ:

По наименованию папки пакета частично определяется его тип. В Руководстве пользователя для ФШ есть таблица соответствия, какая первая буква в имени пакета к какому типу документа относится. Для точного определения, что за документ был получен, нужно проанализировать содержимое этого документа, учитывая его формат.

Форматы документов представлены на сайте НРД на странице <https://www.nsd.ru/documents/workflow/>

Информация о типах принятых документов содержится в отчете о принятых пакетах InPackageList.xml. Он представляет собой агрегированную информацию из файлов packageInfo.xml.

Этот отчет можно выгрузить вручную с закладки «Входящие пакеты» при нажатии кнопки «Выгрузить» или автоматически при установленных настройках канала WSL:

- Автоматическая выгрузка отчета о принятых пакетах
- Интервал выгрузки отчета о принятых пакетах
- Путь к папке с отчетом о принятых пакетах

8.7. Идут ли через ФШ документы типа: счета-акты выполненных работ, счета-фактуры за оказанные услуги?

Ответ:

Да. Их можно найти в папке с первой буквой Z. Но т.к. с первой буквы Z начинаются также папки с депозитарно-клиринговыми отчетами в формате Crystal Repots, нужно дополнительно анализировать тип документа в файле packageInfo.xml или в отчете о принятых пакетах InPackageList.xml. Расчетные документы имеют тип INV.

8.8. Какой максимальный размер пакета может быть отправлен/принят через ФШ?

Ответ:

В Приложении 4 к Правилам ЭДО (<https://www.nsd.ru/documents/workflow/>) написано ограничение для транзитных документов: «Размер одного Пакета транзитных электронных документов не должен составлять более 200 Мбайт, а количество ТЭД (транзитный электронный документ), передаваемых в Пакете - не более 100».

Для остальных типов документов максимальный объем передаваемых данных не регламентирован, но может быть ограничен техническими возможностями системного и криптографического ПО.

8.9. В пакете типа CERRORxx могут содержаться разного рода ошибки? Где-то можно увидеть их перечень?

Ответ:

Пакеты CERROR содержат квитанции ЭДО с сообщением об ошибках.

Основные возможные сообщения об ошибке:

- "Тип документа не определен"
- "Не допускается отправка электронного документа типа <тип вложения>"
- "Пакет документов был обработан ранее" (в случае, когда совпадает хэш с предыдущим пакетом)
- "Файл подписан некорректно и не был обработан."
- "Файл не подписан"
- "Ошибка в процессе распаковки вложения и проверки его подписи"
- "Для данного типа документа разрешена отправка только одного файла в пакете"
- "Сертификат ключа ЭП № ... отозван"
- "ЭП № ... неверна"
- "Файл не подписан"
- "Сертификат, на котором подписан документ, не зарегистрирован в НРД"
- "Сертификат не зарегистрирован или был deregистрирован как устаревший"

- "Сертификат на представителя <x500 имя представителя> не зарегистрирован или был deregистрирован как устаревший"
- "Доверенность на владельца сертификата ... не предоставлена (закончилась)"
- "В доверенности ... на сертификат ... недостаточно полномочий для подписи данного документа"

8.10. Где в ФШ можно посмотреть, что документы доставлены клиенту/изменили статус?

Ответ:

ФШ не отслеживает статусы и состояние отправленных пакетов. Пользователю нужно самостоятельно разбирать содержимое входящих квитанций.

9. Как обратиться в техническую поддержку НРД?

Ответ:

Если у вас есть регистрация на <https://passport.moex.com>, можно перейти на сайт техподдержки по ссылке <https://cabinet.nsd.ru/SUPPORT>, авторизоваться и предоставить в поддержку лог-файлы ФШ, скриншоты ошибок, описание проблемы и шагов, которые привели к ошибкам.

Можно также задать вопрос через сайт НРД, открыв страницу <https://www.nsd.ru/contacts/?tab=175> и перейдя в форму «Задайте вопрос» по ссылке «Мне нужна консультация специалиста».

Также на этой странице опубликованы номер телефона и адрес электронной почты технической поддержки.