ГАЗИНФОРМ СЕРВИС

Программный комплекс по защите
системно-технической инфраструктуры
«Efros Defence Operations»

Инструкция по миграции данных из ПК «Efros CI» в ПК «Efros DO»

Санкт-Петербург, 2024

Аннотация

Данный документ представляет собой инструкцию по миграции данных из программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4 (далее – ПК «Efros CI») в программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations» (далее – ПК «Efros DO»).

Документ содержит алгоритм выполнения миграции, описание работы используемой утилиты и описание возможных ошибок.

Содержание

1 Описание

Миграция выполняется со всех поддерживаемых ПК «Efros CI» операционных систем (ОС) – Astra Linux, РЕДОС, Windows, а также со всех поддерживаемых систем управления базами данных (СУБД) – PostgreSQL\Jatoba, MySQL, MS SQL.

Перед выполнением импорта в ПК «Efros DO» должна быть активирована лицензия на модули NA, FA, ICC, VC, сопоставимая по количеству объектов защиты, используемому в ПК «Efros CI».

2 Алгоритм выполнения миграции

Алгоритм выполнения миграции с ПК «Efros CI» на ПК «Efros DO» включает следующие этапы:

1) Консолидация данных с нескольких серверов ПК «Efros CI» на один сервер ПК «Efros CI».
2) Обновление сервера ПК «Efros CI» до актуальной версии.
3) Создание файла миграции данных утилитой MakeEdoImportFile с базой данных, используемой ПК «Efros CI».
4) Импорт файла миграции данных в ПК «Efros DO».

3 Консолидация данных с нескольких серверов ПК «Efros CI»

Выполнение консолидации данных требуется только в том случае, если необходимо перенести устройства и настройки с нескольких серверов ПК «Efros CI», в том числе серверов иерархии, на один сервер ПК «Efros DO». Если используется один сервер ПК «Efros CI» или миграция выполняется с нескольких серверов ПК «Efros CI» на сопоставимое количество серверов ПК «Efros DO», то данный пункт необходимо пропустить.

Консолидация данных с нескольких серверов ПК «Efros CI» выполняется с использованием функции экспорта\импорта настроек, доступной в версии ПК «Efros CI» 4.10 и выше. При использовании версии ниже, требуется обновить комплекс на актуальную версию.

Функция экспорта\импорта настроек выполняет перенос устройств, профилей устройств, настроек отчетов, проверок безопасности и проверок межсетевых экранов. События и загруженные отчеты не переносятся.

Встроенные по умолчанию профили устройств (и связанные с ними настройки отчетов и пользовательские отчеты) не могут быть дублированы. При импорте файла необходимо выбрать - заменить профиль из файла импорта или оставить текущий. В консоли будет выдано соответствующее предупреждение. Пользовательские профили устройств и проверки могут быть дублированы.

Для консолидации данных следует выбрать «основной» сервер ПК «Efros CI», с которого будет проводится дальнейшая миграция данных. При использовании иерархии рекомендуется выбирать в качестве «основного» сервера управляющий сервер иерархии ПК «Efros CI».

Для консолидации данных на «основном» сервере ПК «Efros CI» потребуется достаточное количество лицензий на объекты защиты. Консолидация может быть выполнена:

- с использованием демонстрационной 30 дневной лицензии, которая предоставляется при создании новой базы данных;
- с помощью запроса временной лицензии через ООО «Газинформсервис».

Способ с использованием демонстрационной лицензии включает следующие действия:

1) Если используется ключ защиты базы данных (БД) сервера ПК «Efros CI», то – убедиться, что ключ сохранен или повторно экспортировать ключ с помощью утилиты настройки сервера. Подробное описание приведено в документе «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство администратора» (далее – «Руководство администратора Efros CI»), в разделе 6.3 «Резервирование ключа защиты данных БД комплекса».
2) Через клиентскую консоль управления ПК «Efros CI» выполнить экспорт настроек со всех серверов ПК «Efros CI». Подробное описание экспорта настроек приведено в документе «Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4. Руководство пользователя. Часть 2. Настройки контроля» (далее – «Руководство пользователя. Часть 2»), в разделе 2.12 «Экспорт настроек комплекса».
3) Создать новую БД на «основном» сервере ПК «Efros CI» с помощью утилиты настройки сервера. Подробное описание создания новой БД для различных управляющих операционных систем приведено в документе «Руководство администратора Efros CI», в пунктах 2.2.3 и 2.3.3 «Создание БД комплекса».
4) Через клиентскую консоль управления ПК «Efros CI» выполнить импорт всех файлов настроек сервера ПК «Efros CI», полученных в пункте 2. Подробное описание выполнения импорта файла приведено в документе «Руководство пользователя. Часть 2», в разделе 2.13 «Импорт настроек комплекса».

Способ с получением временной лицензии через ООО «Газинформсервис» включает следующие действия:

1) Получить и активировать на «основном» сервере ПК «Efros CI» временный ключ с необходимым количеством лицензий на объекты защиты.
2) Через клиентскую консоль управления ПК «Efros CI» выполнить экспорт настроек со всех серверов ПК «Efros CI», кроме «основного». Подробное описание выполнения экспорта приведено в документе «Руководство пользователя. Часть 2», в разделе 2.12 «Экспорт настроек комплекса».
3) Через клиентскую консоль управления ПК «Efros CI» выполнить импорт всех файлов настроек сервера ПК «Efros CI», полученных в пункте 2. Подробное описание выполнения импорта файла приведено в документе «Руководство пользователя. Часть 2», в разделе 2.13 «Импорт настроек комплекса».

4 Обновление сервера ПК «Efros CI»

Миграция поддерживается, начиная с версии сервера ПК «Efros CI» 4.16 и версии ПК «Efros DO» 2.10 Для выполнения миграции версия ПК «Efros CI», с которой выполняется миграция, должна соответствовать версии ПК «Efros DO», на которую выполняется миграция (таблица 1).

Таблица 1 – Соответствие версий для миграции ПК «Efros CI» в ПК «Efros DO»

Версия ПК «Efros CI»	Версия ПК «Efros DO»
4.16	2.10
4.17	2.11
4.18	2.12

Если версия сервера ПК «Efros CI» соответствует необходимой, то данный пункт можно пропустить, иначе необходимо выполнить обновление сервера ПК «Efros CI» в соответствии с документом «Руководство администратора Efros CI».

Если была выполнена консолидация данных, то достаточно обновить только «основной» сервер ПК «Efros CI». Если консолидация данных не выполнялась, то необходимо выполнить обновление каждого сервера ПК «Efros CI», для чего в соответствии с документом «Руководство администратора Efros CI» необходимо произвести следующие действия:

1) Выполнить резервное копирование БД текущей версии ПК «Efros CI». Процесс описан в разделе 6.1.1 «Создание резервной копии БД».
2) Обновить сервер и консоль ПК «Efros CI» на актуальную версию. Процесс описан

в разделе 3 «Обновление компонентов комплекса».

3) Обновить используемые модули ПК «Efros CI» на актуальные версии. Процесс описан в разделе 3.2 «Обновление внешних модулей».

5 Создание файла миграции данных утилитой MakeEdoImportFile

Если была выполнена консолидация данных, то файл миграции данных необходимо создать только для «основного» сервера ПК «Efros CI». Если консолидация данных не выполнялась, то необходимо создать файл миграции для каждого сервера ПК «Efros CI».

Для миграции необходимо воспользоваться утилитой MakeEdoImportFile. Утилита предназначена для создания файла миграции данных ПК «Efros CI», который в будущем будет импортирован в ПК «Efros DO».

Утилита доступна для Windows и Linux систем.

Для запуска утилиты на ОС Windows, необходимо предварительно поместить исполняемый файл утилиты MakeEdoImportFile.exe в директорию с файлами сервера ПК «Efros CI» (по умолчанию – C:\Program Files\EFROS Config Inspector 4\Server) и выполнить в командной строке Windows (cmd) команду:

```
MakeEdoImportFile
```

Для запуска утилиты на ОС linux необходимо предварительно установить пакет efrosci_makeedoimportfile_4.xx.xxx.xxxx.deb(rpm) с помощью пакетного менеджера dpkg (yum) и выполнить команду:

```
sudo efrosci-makeedoimportfile
```

Далее представлено подробное описание работы утилиты, значения аргументов и примеры запуска утилиты.

5.1 Описание работы утилиты MakeEdoImportFile

Утилита *MakeEdoImportFile* выполняет проверку типа используемой ОС в СУБД сервера ПК «Efros CI» и производит обновление до ОС Astra Linux, а также замену модулей под целевую ОС.

Данные для работы утилиты:

- путь к папке с zip-архивами модулей для работы с ОС Astra Linux SE (v.1.6, v.1.7);
- параметры для подключения к БД;
- параметр с числом дней для переноса записей событий;
- путь до формируемого выходного файла БД.

5.2 Алгоритм действий утилиты

Алгоритм выполнения миграции включает следующие этапы:

1) Осуществляется подключение к БД и выполняются проверки:

   а) отключены ли модули «Отправка писем по протоколу SMTP» и «Экспорт событий»;

   В ПК «Efros DO» данные модули не поддерживаются. Имеются собственные инструменты, эквивалентные возможностям данных модулей.

   б) изначальный тип ОС в БД. Если тип ОС не Astra Linux, то:
   - проверяется, что все установленные модули присутствуют в папке с zip-архивами, подаваемой на вход;
   - заменяются модули под ОС Astra Linux из папки с zip-архивами:

   Если модуль не найден в папке и модуль загружен, но не включен, то файлы модуля удаляются из БД. Если модуль не найден в папке, модуль загружен и включен – выполнение прерывается с ошибкой, что модуль не найден.

   - проводится обновление типа ОС в БД на целевую ОС.

2) Выполняется перенос данных из БД в формируемый выходной файл формата «*.db».
3) Выполняется тестовый запуск ядра, чтобы проверить возможность запуска с новыми данными.

5.3 Аргументы утилиты

Перечень аргументов утилиты *MakeEdoImportFile* приведен в таблице 2.

Таблица 2 – Перечень аргументов утилиты *MakeEdoImportFile*.

Аргумент	Описание
features_folder	Путь к папке с zip-архивами модулей под ОС Astra Linux
db_host	Адрес сервера СУБД
db_type	Тип СУБД (MYSQL, MSSQL, POSTGRESQL)
db_schema	Имя БД
db_login	Логин для подключения к БД
db_password	Пароль для подключения к БД
db_key_file_path	Путь к файлу с ключом БД (опционально)

Аргумент	Описание
db_key_password	Пароль ключа БД (опционально)
transfer_events_period_days	Количество дней, за которые будет выполнен перенос событий (опционально) Если аргумент не задан, то будет установлено значение по умолчанию 30 дней. Значение «0» – перенос всех событий
output_file	Путь к выходному файлу (опционально) Если аргумент не задан, то файл БД будет создан в директории запуска утилиты с именем по умолчанию «efrosci_edo.db»
remote_export_uri	URI-путь для удаленной выгрузки файла экспорта по протоколу sftp или smb (опционально). sftp://ip:port/<путь_до_директории> (порт обязателен). smb://(имя или ip):port/<путь_до_директории> (порт опционален)
remote_export_host_login	Логин для подключения к sftp или smb (опционально)
remote_export_host_password	Пароль для подключения к sftp или smb (опционально)
remote_export_host_domain	Домен от доменной учетной записи при подключении по протоколу smb (опционально)

Перед удаленной выгрузкой файл БД предварительно формируется локально на машине с запущенной утилитой. Следует убедиться в наличии свободного места (должно соответствовать размеру выгружаемой БД комплекса) на машине откуда выполняется запуск утилиты *MakeEdoImportFile.*

5.4 Пример запуска утилиты

Примеры запуска утилиты *MakeEdoImportFile*:

1) С минимальным набором аргументов:

   a) пример выполнения команды для запуска утилиты под ОС Windows:

   MakeEdoImportFile --features_folder="C:\Users\Администратор\Downloads\Modules" --db_host="10.72.11.135" --db_type="MYSQL" --db_schema="efrosci_4" --db_login="root" --db_password="****"

Предварительно необходимо создать директорию и поместить в неё файлы модулей ПК «Efros CI» для ОС Astra Linux в формате .zip. Версии модулей в директории должны соответствовать версиям модулей, установленным в ПК «Efros CI».

б) пример выполнения команды для запуска утилиты под ОС Astra Linux:

```
sudo efrosci-makeedoimportfile --features_folder="/home/efros/astra_modules" --db_host="10.72.11.94" --db_type="POSTGRESQL" --db_schema="efrosci" --db_login="postgres" --db_password="********"
```

Если аргумент *output_file* не указан, то файл БД будет создан в директории запуска утилиты с именем по умолчанию «efrosci_edo.db».

2) Со всеми аргументами:

```
sudo efrosci-makeedoimportfile --features_folder="/home/efros/astra_modules" --db_host="10.72.11.94" --db_type="POSTGRESQL" --db_schema="efrosci" --db_login="postgres" --db_password="****" --db_key_file_path="/home/efros/key.ecikey" --db_key_password="****" --transfer_events_period_days="7" --remote_export_uri="smb://10.72.10.244/migrate_share" --remote_export_host_login="domain_user" --remote_export_host_password="****" --remote_export_host_domain="test.domain" --output_file="/home/efros/eci.db"
```

При указании аргумента *transfer_events_period_days* равным «0», процесс подготовки файла БД и импорта данных из него в ПК «Efros DO» может занимать длительное время, а также значительно увеличит размер самого файла БД.

6 Импорт файла миграции данных ПК «Efros CI» в ПК «Efros DO»

На один сервер ПК «Efros DO» можно импортировать только один файл миграции данных.

При импорте файла миграции данных в ПК «Efros DO» в разделе «Контроль устройств» будут перезаписаны устройства, проверки безопасности, проверки межсетевых экранов и профили устройств на информацию из файла миграции.

Для импорта файла миграции данных необходимо указать файл в веб-интерфейсе ПК «Efros DO» для загрузки из сетевой папки или по ssh.

Для импорта файла необходимо выполнить следующие действия:

1) Открыть в веб-интерфейсе ПК «Efros DO» раздел «Настройки» → «Импорт данных» (рисунок 1).
2) Выбрать тип загрузки «Efros CI (standalone)».
3) Выбрать вид расположения файла – «Сетевой» (сетевая папка) или «SSH подключение» (файл доступен по SSH).
4) Указать путь к файлу и выбрать параметры подключения.
5) Нажать кнопку «Загрузить».

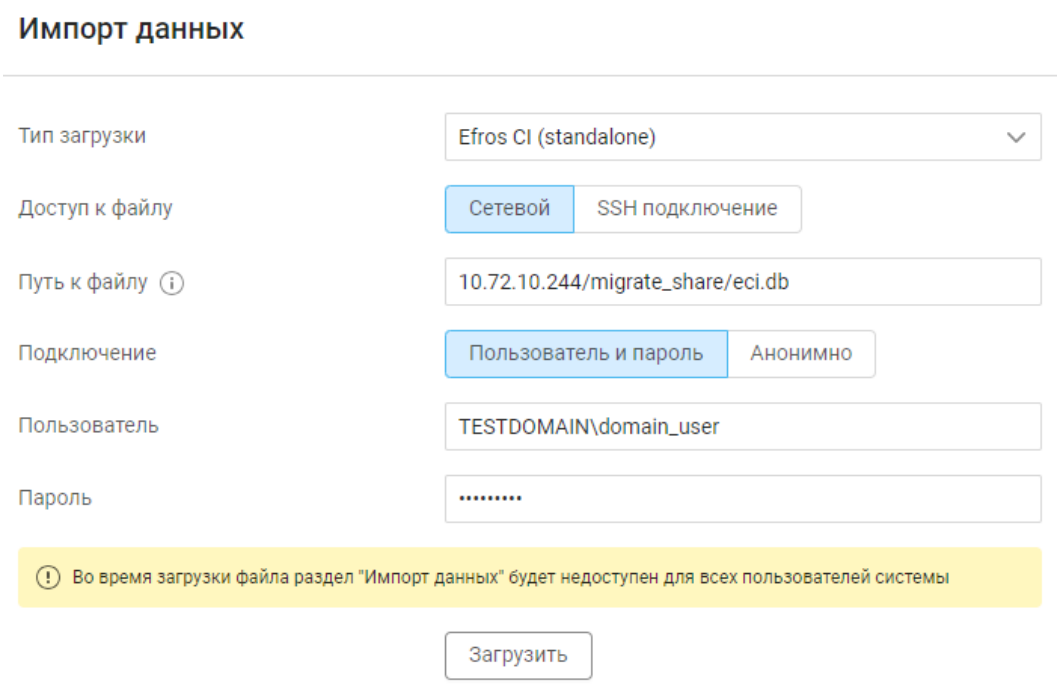

Рисунок 1 – Импорт файла миграции данных через веб-интерфейс ПК «Efros DO»

7 Возможные ошибки при миграции

При выполнении утилиты *MakeEdoImportFile* могут возникнуть ошибки:

1) «Текущая версия схемы БД отличается от требуемой» (рисунок 2).

   Используется утилита MakeEdoImportFile не соответствующей версии.

   Для устранения ошибки, необходимо использовать утилиту MakeEdoImportFile, соответствующую версии ПК «Efros CI».

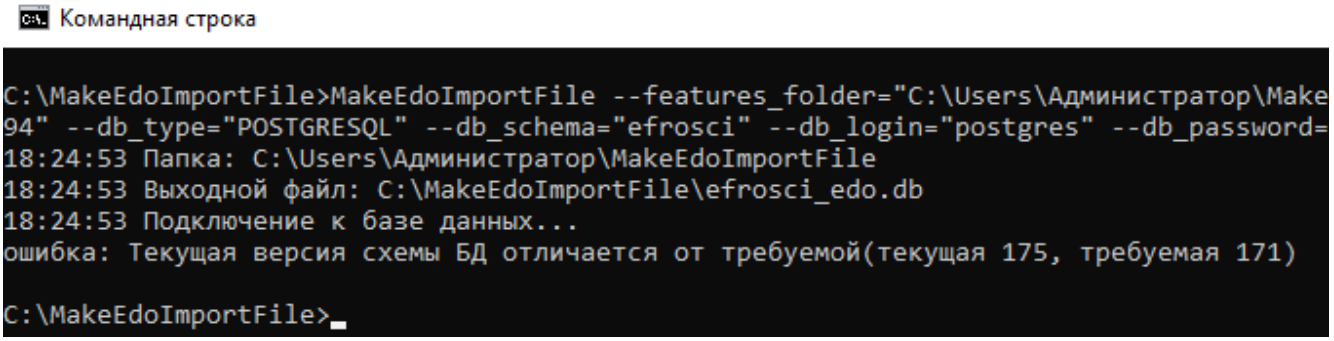

Рисунок 2 – Ошибка «Текущая версия схемы БД отличается от требуемой»

2) «Для продолжения требуется отключить встроенные модули» (рисунок 3).

   Не отключены модули отправки писем и экспорта событий, работа которых не поддерживается в ПК «Efros DO».

   Для устранения ошибки необходимо отключить указанные модули в подразделе ***Модули*** раздела **Настройки** клиентской консоли ПК «Efros CI».

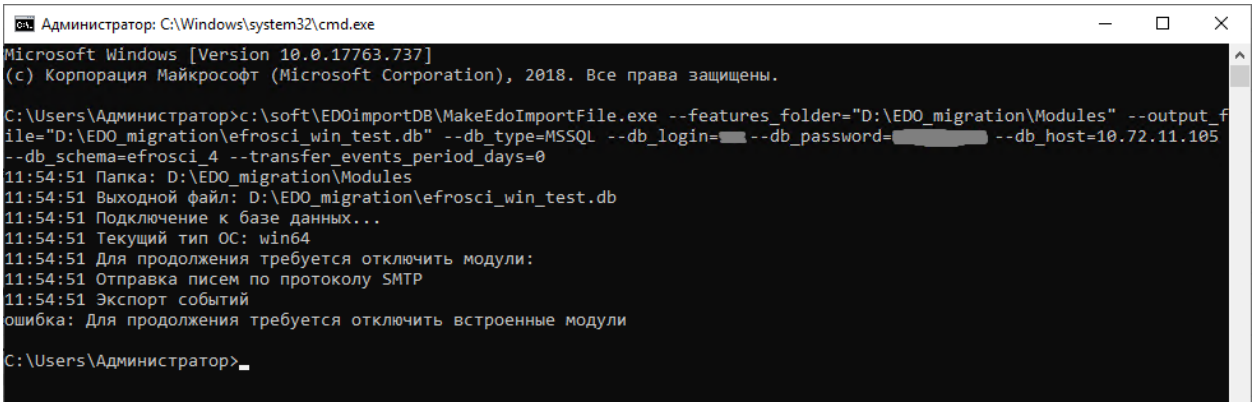

Рисунок 3 – Ошибка «Для продолжения требуется отключить встроенные модули»

3) «Не все установленные модули найдены в папке» (рисунок 4).

   В директории, указанной в аргументе features_folder, отсутствуют модули

поддержки устройств, или, при наличии модулей, отличается их версия от используемой в ПК «Efros CI».

Модуль может не поддерживаться в Linux-версии ПК «Efros CI» и отсутствовать.

Для устранения ошибки необходимо добавить zip-архив модуля в папку либо отключить данный модуль в подразделе ***Модули*** раздела **Настройки** клиентской консоли ПК «Efros CI», если он не требуется (не используется).

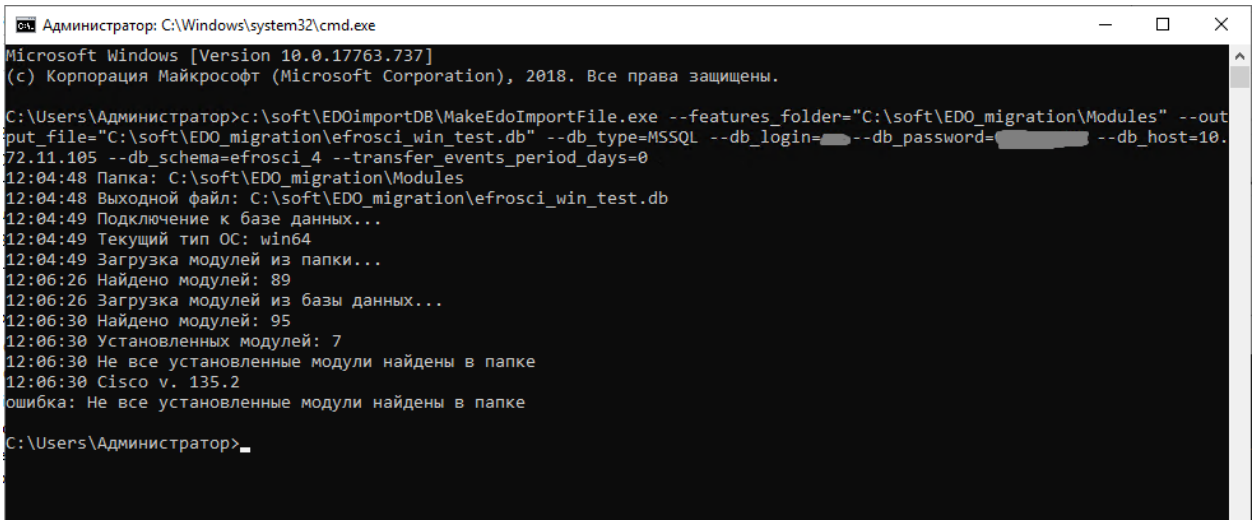

Рисунок 4 – Ошибка «Не все установленные модули найдены в папке»

4) «Не удалось перенести базу данных» (рисунок 5).

В пути выходного файла содержится кириллица. При этом кириллица поддерживается в пути к папке с zip-архивами модулей под ОС Astra Linux и в пути к файлу с ключом защиты БД.

Для устранения ошибки необходимо запускать утилиту из директории, в пути которой не содержатся символы кириллицы, или использовать аргумент output_file без содержания символов кириллицы.

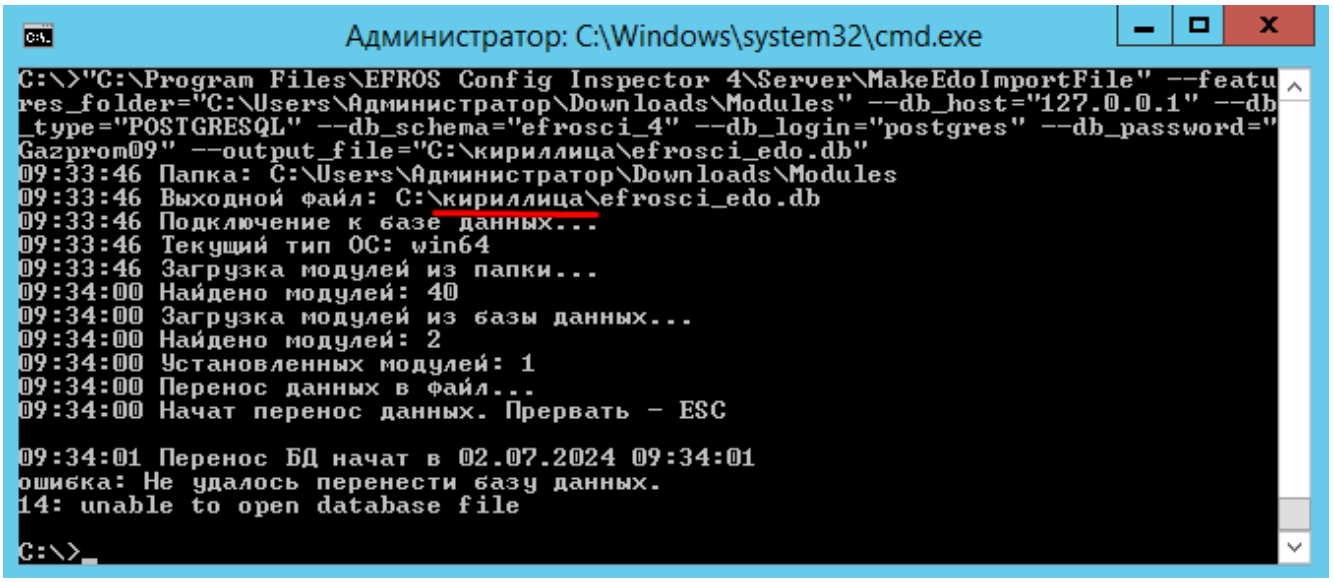

Рисунок 5 – Ошибка «Не удалось перенести базу данных»

5) « … (code56): Failure when receiving data from the peer » (рисунки 6 и 7).

Отключен протокол smb версии 1 на машине, которая используется для удаленной работы с файлом миграции по протоколу smb.

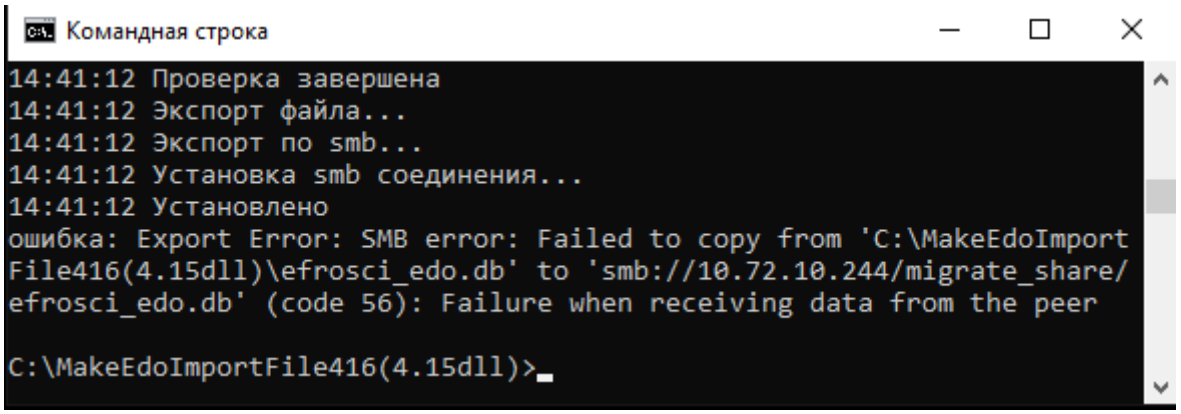

Рисунок 6 – Ошибка (code56): Failure when receiving data from the peer

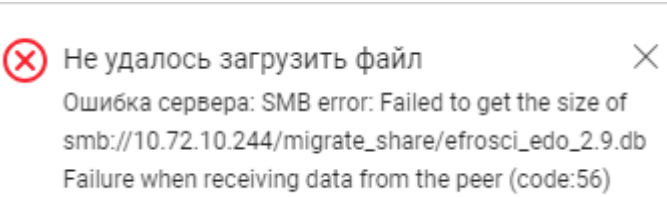

Рисунок 7 – Ошибка Failure when receiving data from the peer (code:56)

Для проверки на ОС WIndows 2012R2 и выше необходимо выполнить в PowerShell команду:

(Get-SmbServerConfiguration).EnableSMB1Protocol

Получение в выводе false указывает, что протокол smb 1-й версии отключен.

Для устранения ошибки на ОС WIndows 2012R2 и выше необходимо включить протокол smb версии 1 в PowerShell командой:

Enable-WindowsOptionalFeature -Online -FeatureName smb1protocol

6) «Ошибка сервера: Verify import file error» (рисунок 8).

Версия ПК «Efros DO» не соответствует версии ПК «Efros CI», для которой подготовлен файл миграции данных.

Для устранения ошибки необходимо обновить ПК «Efros CI» или ПК «Efros DO» до соответствующих друг другу версий и при необходимости повторить миграцию.

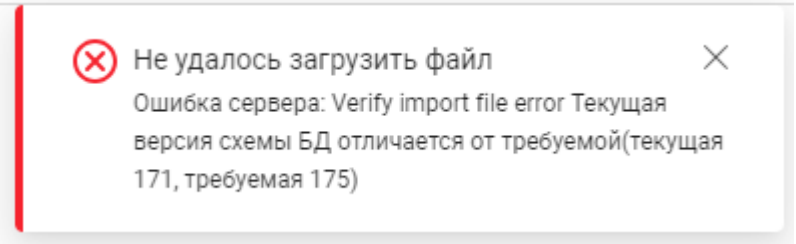

Рисунок 8 – Ошибка сервера: Verify import file error

7) «Ошибка сервера: boost::filesystem::path codecvt to string: error» (рисунок 9).

Ошибка возникает при импорте в ПК «Efros DO» из сетевой папки, если в пути содержится кириллица.

Для устранения ошибки необходимо переименовать название директории или файла, исключив кириллицу.

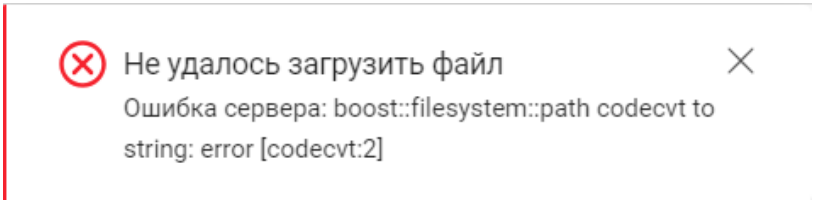

Рисунок 9 – Ошибка сервера: boost::filesystem::path codecvt to string…

.

Перечень сокращений

БД	–	База данных
ОС	–	Операционная система
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных