АСУРЭО

Версия 11.X

Руководство системного администратора

2025

Россия, 443013, г. Самара, Московское шоссе, 4, корп. 4,
Бизнес-центр «Монте Роза», 12 этаж, тел: (846) 2-150-150

Содержание

1 НАЗНАЧЕНИЕ РУКОВОДСТВА 7
2 КОМПОНЕНТЫ СИСТЕМЫ И ИХ НАЗНАЧЕНИЕ 8
3 ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ 12
3.1 Серверная часть 12
3.1.1 Серверная часть с абонентами 12
3.2 Клиентская часть 13
4 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ 15
4.1 Сервер приложений и баз данных 15
4.2 Почтовый сервер 16
4.3 Рабочие станции 16
4.4 Настройки браузера Яндекс и политик безопасности для него 18
4.4.1 Запросы на отправку 18
4.4.2 Настройка размера шрифта в браузере 18
4.4.3 Настройка работы через прокси-сервер 19
4.4.4 Настройка доверенных сайтов 21
4.4.5 Установка расширения для браузера «Помощник ЗРП.Net» 21
4.4.6 Особенности отображения уведомлений в ОС Linux 26
5 КОМПЛЕКТ ПОСТАВКИ НА ОС MS WINDOWS 28
6 КОМПЛЕКТ ПОСТАВКИ НА ОС СЕМЕЙСТВА LINUX 29
7 ПОСЛЕДОВАТЕЛЬНОСТЬ УСТАНОВКИ ПК «АСУРЭО» НА ОС MS WINDOWS 30
8 ПОСЛЕДОВАТЕЛЬНОСТЬ УСТАНОВКИ ПК «АСУРЭО» НА ОС СЕМЕЙСТВА LINUX 31
9 УСТАНОВКА И НАСТРОЙКА СИСТЕМНОГО ПО 33
9.1 Установка ОС Linux 33
9.2 Установка docker и docker-compose 38
9.3 Настройка прав и доступов для управления СП и docker 38
9.4 Настройка сети docker 38
9.5 Установка и настройка веб-сервера IIS 39
9.5.1 Установка веб-сервера IIS 39
9.5.2 Дополнительные настройки web-сервера IIS 41
9.5.3 Рекомендации 42
9.6 Настройка конфигурационного файла веб-сервер nginx 43
9.7 Настройка отображения шифров 46
9.8 Установка и настройка СУБД на ОС MS Windows 50
9.8.1 Установка СУБД MS SQL на ОС MS Windows 50
9.8.2 Настройка СУБД MS SQL на ОС MS Windows 51
9.8.3 Установка СУБД PostgreSQL на ОС MS Windows 56

9.9 Установка и настройка СУБД на ОС семейства Linux ... 62
9.9.1 Установка СУБД PostgreSQL ... 62
9.9.2 Установка СУБД на ОС семейства Linux ... 68
9.9.3 Настройка СУБД на ОС семейства Linux ... 72
9.10 Установка и настройка etcd на ОС MS Windows ... 74
9.11 Установка etcd на ОС Linux ... 75
10 УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА ПК «АСУРЭО» ... 76
10.1 Создание и настройка БД MS SQL ... 76
10.1.1 Создание базы данных ... 76
10.1.2 Создание учетной записи пользователя ... 79
10.1.3 Настройка прав учетной записи пользователя ... 80
10.2 Создание БД PostgreSQL ... 82
10.2.1 Создание БД с использованием «SQL Shell (psql)» ... 83
10.2.2 Создание БД с использованием инструментария PGAdmin ... 83
10.2.3 Создание учетной записи пользователя в инструментарии PGAdmin ... 84
10.2.4 Настройка прав учетной записи пользователя ... 85
10.3 Настройка взаимодействия через DataPower ... 86
10.4 Настройка HTTPS ... 87
10.4.1 Общая информация ... 87
10.4.2 Установка и настройка сертификата для IIS 7.x ... 87
10.4.3 Настройка сайта на веб-сервере IIS для работы с SSL ... 88
10.5 Настройка basic-авторизации ... 90
10.5.1 Общие сведения ... 90
10.5.2 Настройка web-сервера IIS на Windows Server 2008 ... 91
10.5.3 Настройка ПК в части basic-авторизации ... 94
10.6 Установка АСУРЭО на СУБД MSSQL/PostgreSQL на ОС Windows ... 95
10.6.1 Выбор производимых действий ... 97
10.6.2 Выбор дополнительных компонентов ... 99
10.6.3 Выбор версии веб-сервера ... 100
10.6.4 Настройка сервера приложений ... 102
10.6.5 Выбор базы данных ... 104
10.6.6 Настройка подключения к MSSQL/PostgreSQL ... 105
10.6.7 Настройка параметров ключа защиты ... 107
10.6.8 Завершение сбора информации ... 108
10.7 Установка АСУРЭО на ОС семейства Linux ... 110
10.8 Настройка ПК «АСУРЭО» с помощью конфигуратора ... 113
10.8.1 Дополнительные настройки ... 115
10.8.2 Настройка Сервера приложений ... 116
10.8.3 Настройка Сервера авторизации ... 121

10.8.4 Настройка Сервера Delphi приложений 123
10.9 Описание параметров файла web.config 128
10.10 Описание параметров файла zvk.ini 129
10.11 Описание параметров файла sms.ZRP.WebApi.settings.json для ЗРП.Net 145
10.11.1 Настройки базы данных 146
10.11.2 Настройки логирования запросов к базе данных 146
10.11.3 Настройки для подключения 147
10.11.4 Настройка доступа к серверу приложений Delphi_ 148
10.11.5 Настройки подключения к etcd серверу 148
10.11.6 Настройки кэширования веб-запросов 149
10.11.7 Настройки коммуникации с внешними сервисами 149
10.11.8 Настройки оповещений 150
10.11.9 Настройка Cross-Origin Resource Sharing 150
10.11.10 Настройки JWT_ 150
10.11.11 Запланированные задачи 151
10.11.12 Системные настройки 152
10.11.13 Настройки интеграции с SAP 153
10.11.14 Настройки менеджера дополнительно подключаемых функций 153
10.11.15 Настройки Swagger 154
10.11.16 Настройки лицензирования 155
10.11.17 Настройки сжатия ответов 155
10.12 Описание параметров файла authServer.settings.json сервера авторизации 155
10.12.1 Настройки базы данных и подключения 156
10.12.2 Настройки NT авторизации 156
10.12.3 Настройки безопасности 158
10.12.4 Настройки клиентов 158
10.13 Описание параметров файла config.json сервера авторизации 160
10.14 Настройка взаимодействия сервера приложений и пользовательских интерфейсов 161
10.14.1 Дополнительные настройки журналирования действий сервера приложений 162
10.15 Обновление ПК «АСУРЭО» на ОС MS Windows 162
10.16 Обновление ПК «АСУРЭО» на ОС семейства Linux 168
10.16.1 Последовательность действий на клиентах после обновления Системы 171
10.17 Интеграция с Avanpost FAM 175
10.18 Настройка клиентского рабочего места 175
10.18.1 Настройка браузера Internet Explorer 175
10.18.2 Настройка ClickOnce 176
10.18.3 Запуск приложений через ClickOnce 178
10.18.4 Первый запуск ПК на рабочей станции 181

10.18.5 Создание ярлыка интерфейса пользователя на рабочей станции 187
10.18.6 Обновление клиентской части ПК 188
10.18.7 Хранимые версии 189
10.18.8 Установка клиентской части Системы на ОС Astra Linux 190
10.19 Проверка работоспособности ПК после установки 201
10.20 Откат к предыдущей версии ПК 201
10.21 Удаление ПК «АСУРЭО» на ОС MS Windows 202
10.22 Удаление ПК «АСУРЭО» на ОС семейства Linux 204
11 РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ ПК НА СУБД MS SQL 206
11.1 Общие сведения 206
11.2 Создание устройства 206
11.3 Предварительные условия 207
11.4 Последовательность действий по настройке плана обслуживания БД 208
11.5 Настройки процедуры резервного копирования 227
11.6 Восстановление БД 227
11.7 Восстановление работы интерфейсов 229
12 РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ ПК НА СУБД POSTGRESQL 230
12.1 Создание резервной копии базы данных средствами pg_dump 230
12.1.1 Создание bat-файла 230
12.1.2 Создание задания планировщика Windows 232
12.2 Создание резервной копии базы данных в инструментарии PGAdmin 237
12.3 Восстановление БД из резервной копии средствами pg_restore 238
12.4 Восстановление БД из резервной копии в инструментарии PGAdmin 239
13 НАСТРОЙКА КАРТЫ МНОГОЭКЗЕМПЛЯРНОЙ КОНФИГУРАЦИИ 242
13.1 Использование карты 242
13.2 Создание карты 242
13.3 Настройка карты многоэкземплярной конфигурации на сервере 247
14 ЛОГИРОВАНИЕ ПК 250
14.1 Удаление старых логов 251
15 РЕКОМЕНДАЦИИ ДЛЯ АДМИНИСТРАТОРОВ 252
15.1 Рекомендации по обновлению PostgreSQL версии 12 до 15 252
15.2 Рекомендации о периодическом ребилдинге индексов в базе ПК 252
15.3 Рекомендации об усечении лога транзакций 261
15.4 Рекомендации по обработке ошибок 261
15.4.1 Ошибка при установке ПК 261
15.4.2 Ошибка при обновлении ПК 262
15.4.3 Ошибка при запуске сервера приложений 262

15.4.4 Ошибка при установке соединения с сервером приложений 263
15.4.5 Ошибка при запуске приложения 263
15.4.6 Ошибка при удалении HTTPS 264
15.5 Рекомендации по ограничению объема занимаемой памяти 264
15.6 Рекомендации по штатному останову серверов приложений 265
15.7 Рекомендации по настройке параметра «client_max_body_size» 265
15.8 Рекомендации по увеличению лимитов по открытым файлам на ОС Linux....266
ПРИЛОЖЕНИЕ 1. НАБОР ФАЙЛОВ УСТАНОВЛЕННОГО ЭКЗЕМПЛЯРА 268
ПРИЛОЖЕНИЕ 2. СКРИПТ ДЛЯ ШТАТНОГО ОСТАНОВА СЕРВЕРОВ ПРИЛОЖЕНИЙ АСУРЭО 271

1 Назначение руководства

Данное руководство предназначено для системных администраторов автоматизированной системы управления ремонтами энергетического оборудования (далее – АСУРЭО).

2 Компоненты системы и их назначение

ПК представляет собой распределенную систему, включающую клиентские рабочие станции и сервера, на которых располагается ПО серверов баз данных (далее - БД) и / или серверов приложений.

Структурно ПК состоит из следующих составных частей (Рисунок 2.1):

- хранилище данных;
- сервер приложений;
- интерфейс администратора;
- интерфейс по работе с оборудованием;
- интерфейс по работе с заявками;
- расширения, интерфейсные модули связи с другими системами.

При работе с заявками используется клиент - серверная архитектура. Сервер приложений представляет собой службу Windows. Доступ возможен по прямому TCP / IP соединению или через Web-сервер. В качестве хранилища данных используется СУБД Microsoft SQL Server. Взаимодействие между клиентскими рабочими станциями и серверами приложений осуществляется посредством вызова серверных процедур по одному из протоколов: HTTP / HTTPS или TCP / IP.

При запуске пользовательского интерфейса на рабочей станции с сервера запрашивается информация о протоколах, поддерживаемым данным экземпляром сервера приложений.

Если для экземпляра настроена поддержка обоих протоколов (как для HTTP / HTTPS, так и для TCP / IP), то сначала выполняется попытка обращения клиента к серверу по протоколу TCP / IP. Если связь установлена, то взаимодействие между клиентом и сервером приложений осуществляется посредством протокола TCP / IP в течение текущей сессии пользователя. В случае, если для экземпляра установлен только один порт протокола HTTP или попытка связи по TCP / IP не удалась, то взаимодействие клиента с сервером осуществляется по протоколу HTTP / HTTPS в рамках текущей сессии пользовательского интерфейса. При следующем старте пользовательского интерфейса информация о настроенных открытых портах запрашивается с сервера вновь.

В АСУРЭО версии 5.X и выше протокол HTTP / HTTPS поддерживает асинхронные вызовы и по нему осуществляется взаимодействие клиента с сервером. Для обмена

сообщениями по SOAP используется дополнительный протокол NativeHTTP, который поддерживает синхронные вызовы.

На рисунке 2.2 представлена схема обмена данными между серверами приложений, включающего передачу заявок между уровнями и синхронизацию НСИ. Данные передаются в XML-формате, при этом для передачи используется существующий канал связи: прямое соединение сервер-сервер или почта.

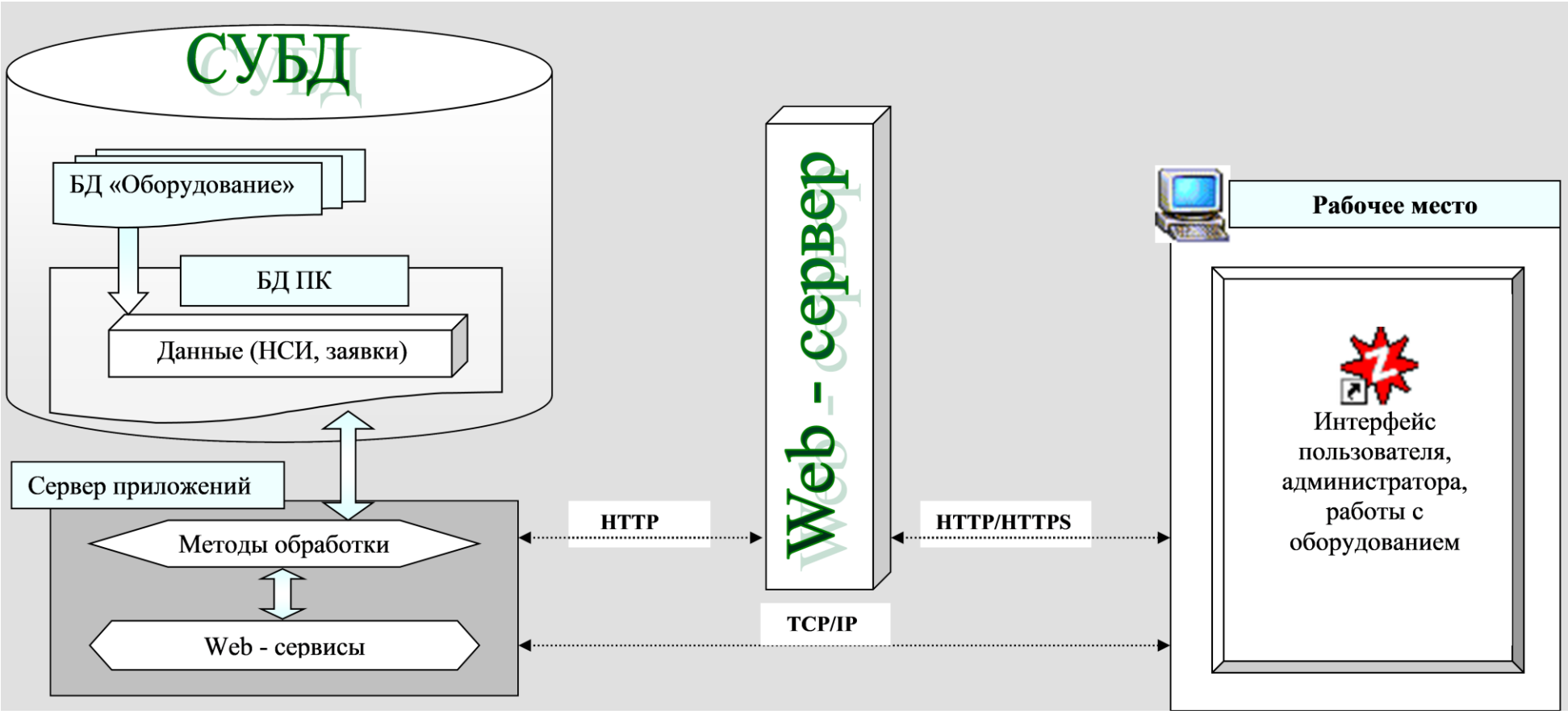

Рисунок 2.1 – Компоненты ПК

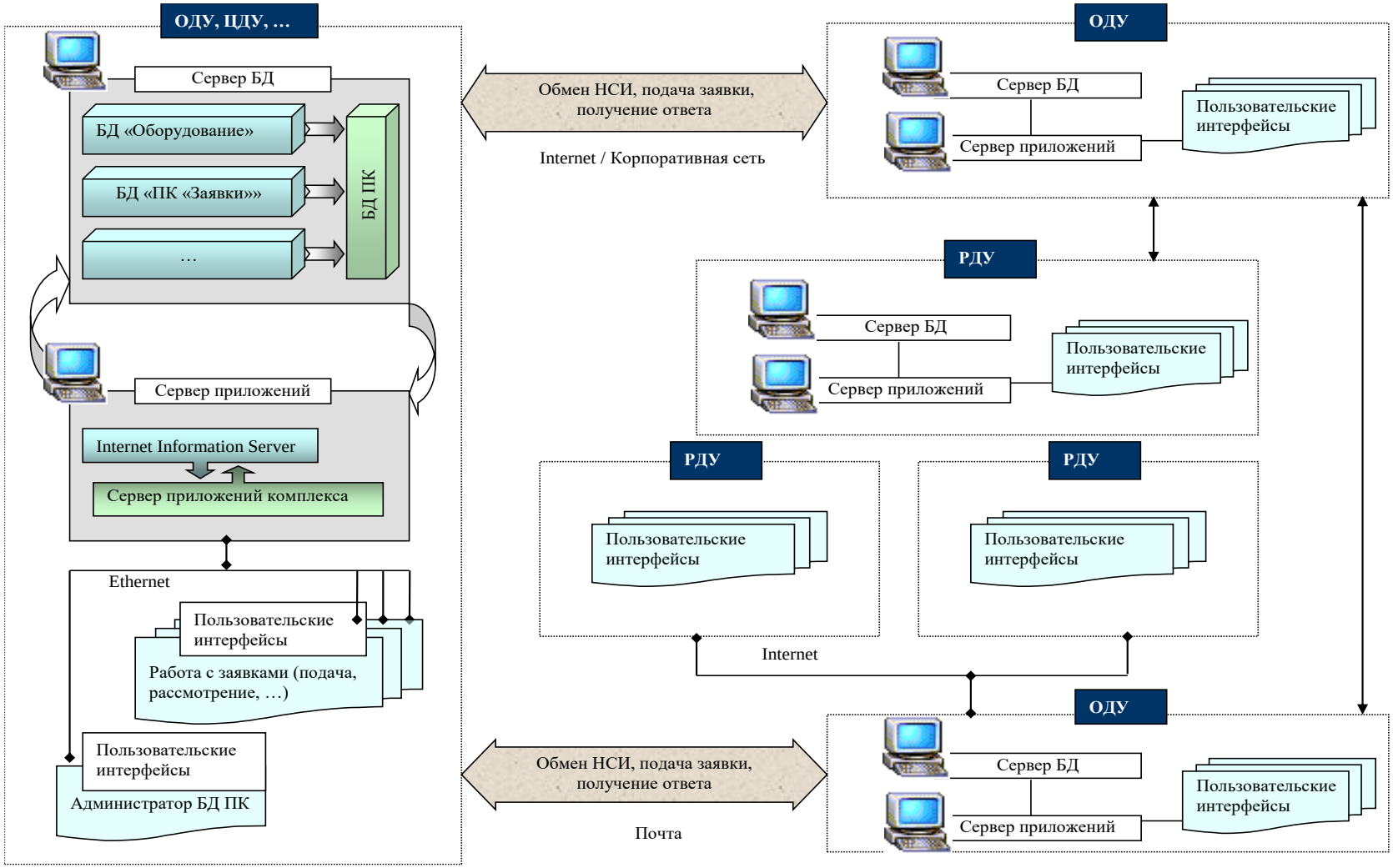

Рисунок 2.2 – Схема взаимодействия составных частей ПК

3 Требования к аппаратному обеспечению

3.1 Серверная часть

Для функционирования приложения необходимо следующее аппаратное обеспечение сервера приложений и / или БД:

- **Минимальная конфигурация сервера:**
  - Процессор: не ниже Intel Xeon 4130 3,4 ГГц;
  - Оперативная память не ниже 4 Гб для сервера приложений и 4 Гб для СУБД MSSQL / PostgreSQL (желательна установка на разных серверах);
  - Жесткий диск: не менее 160-200 ГБ;
  - Наличие USB порта;
  - Наличие сетевой платы Ethernet 100/1000.
- **Рекомендуемая конфигурация сервера:**
  - Процессор: Intel Xeon L5630 2,13 ГГц (4 Cores);
  - Оперативная память не ниже 8 Гб для сервера приложений и 8 Гб для СУБД MSSQL / PostgreSQL (желательна установка на разных серверах);
  - Жесткий диск: 500 ГБ;
  - Наличие USB порта;
  - Наличие сетевой платы Ethernet 100/1000.

С ростом объема данных в БД требования к аппаратному обеспечению возрастают, для корректного функционирования комплекса необходимо использовать «Рекомендуемую конфигурацию сервера».

3.1.1 Серверная часть с абонентами

Для функционирования приложения на одном предприятии-абоненте с количеством одновременно работающих пользователей до 40 и с количеством оборудования порядка 60 тысяч единиц в БД необходимо следующее аппаратное обеспечение сервера приложений и / или БД:

- ЦПУ: 4 ядра;
- Оперативная память 8 Гб (4 Гб – СУБД и 4 Гб – АСУРЭО);

– Жесткий диск: 20 Гб.

Для расчета нужной конфигурации необходимо выполнять следующие действия:

1. При добавлении нового предприятия-абонента необходимо добавлять 1 Гб оперативной памяти и место на жёстком диске примерно 5 Гб (зависит от числа заявок и других НСИ предприятия-абонента, активностей из-за которых будет расти лог транзакций и лог ПК).
2. При добавлении 40 активных пользователей следует добавлять по 1 ядру ЦПУ.

Все расчёты приблизительные: при реальной работе возможно, какие-то характеристики могут оказаться избыточными или наоборот недостаточными и тогда следует менять конфигурацию сервера.

3.2 Клиентская часть

Для функционирования приложения необходимо следующее аппаратное обеспечение рабочей станции:

- **Минимальная конфигурация клиентского рабочего места:**
  - Процессор: не ниже Intel Core Celeron D 331 2.66 ГГц;
  - Оперативная память не ниже 2 ГБ;
  - Жесткий диск: не менее 500 МБ свободного места;
  - Наличие сетевой платы Ethernet 100;
  - Видеосистема (монитор ЖКИ–17 дюймов + видеоплата) с разрешением экрана не ниже 1024*768.
- **Рекомендуемая конфигурация клиентского рабочего места:**
  - Процессор: не ниже Intel Core i3 3,3 ГГц;
  - Оперативная память не ниже 4 ГБ;
  - Жесткий диск: не менее 500 МБ свободного места;
  - Наличие сетевой платы Ethernet 100;
  - Видеосистема (монитор ЖКИ–17 дюймов + видеоплата) с разрешением экрана не ниже 1024*768.

Для сокращения времени запуска приложения и первоначального входа пользователя в Систему для видеоплаты должны быть установлены самые последние обновления драйверов.

4 Требования к программному обеспечению

4.1 Сервер приложений и баз данных

Сервер приложений ОС Windows:

- MS Windows Server 2016 (IIS9, 10); MS Windows Server 2019 (IIS10);
- PowerShell 1.0, 2.0;
- Microsoft XML (MSXML 4.0 и 6.0);
- Microsoft Internet Information Server (IIS) версии 9 и выше;
- Microsoft .Net Framework:
  - Microsoft .Net Framework версии 3.5.1 – для запуска инсталлятора АСУРЭО;
  - Microsoft .Net Framework версии 4.5.1 – для возможности подключения дополнительных модулей;

  Примечание. Начиная с версии В9, для обновления ПК «АСУРЭО» необходимо наличие на сервере Microsoft .Net Framework версии 4.7 и выше.

Сервер баз данных (MS SQL) ОС Windows:

- Microsoft SQL Server 2016 / 2019;
- SQL Native Client 2016 (10.x).

Сервер баз данных (PostgreSQL) ОС Windows:

- PostgreSQL 15.

Сервер приложений на ОС семейства Linux:

- Astra Linux;
- Docker 20.10.2;
- библиотека классов – MS .Net Core;
- СУБД Postgres Pro 15;
- веб-сервер nginx 1.21.4.

Внимание!

Поддержка PostgreSQL 13 завершается, и мы рекомендуем перейти на более новую версию - PostgreSQL 15. PostgreSQL 13 перестанет поддерживаться 14.11.2024 г. (подробнее см. https://postgrespro.ru/services/support).

Для установки и обновления MS SQL 2016 / 2019 на сервере ПК должен быть обязательно установлен SQL Native Client 2016 (версия клиента 10.x).

Для корректного выполнения скриптов PowerShell при инсталляции политика выполнения (ExecutionPolicy) должна позволять выполнять неподписанные локальные сценарии (RemoteSigned), либо выполнять все сценарии (Unrestricted), иначе у пользователя, запускающего инсталляцию должна быть привилегия на смену политик.

Для выполнения скриптов PowerShell необходимо обладать правами администратора на операционной системе сервера, а также указанная в команде политика не должна противоречить групповым политикам компании.

Важно! Необходимо производить перезапуск серверов приложений ЗВК.Net совместно с Delphi.

4.2 Почтовый сервер

В качестве базового ПО для почтового сервера может быть использовано любое ПО почтового сервера, поддерживающее протоколы SMTP и POP3.

Внимание! В случае использования защищенного соединения SSL на сервер ПК необходимо установить криптографический пакет OpenSSL.

4.3 Рабочие станции

На рабочих станциях возможно использование ОС MS Windows 8.1, MS Windows 10 с установленной программой браузером MS Internet Explorer (IE) версии 11, или Microsoft Edge (версии 95 и выше), Yandex.browser (версии 21 и выше), Chrome (версии 94 и выше). Работа в ОС MS Windows Vista в ПК «АСУРЭО» не поддерживается. Поддержка ОС MS Windows 7 завершена Microsoft (https://support.microsoft.com/ru-ru/windows/поддержка-windows-7-закончилась-14-января-2020-г-b75d4580-2cc7-895a-2c9c-1466d9a53962).

На рабочих станциях возможно использование указанной ОС Astra Linux только с использованием средств эмуляции. Работоспособность всех функций не гарантируется. Работоспособность клиентской части ПК «АСУРЭО» гарантирована только в веб-версии. Для работы с интерфейсами администратора («Интерфейс оборудования», «Интерфейс администратора») рекомендуется использоваться ОС Windows.

Клиент Delphi необходимо запускать только на физическом хосте с ОС Linux.

Установка клиентских приложений осуществляется с помощью технологии ClickOnce, которая позволяет пользователю устанавливать и запускать Windows-приложения, по нажатию на ссылку на веб-странице либо в сетевом окружении. Основной принцип ClickOnce — простое развёртывание Windows-приложений пользователем. Для запуска ClickOnce приложений требуется наличие Microsoft .NET Framework версии 4.0 на рабочей станции.

Браузеры Internet Explorer и Edge не требуют установки дополнительных приложений для поддержки ClickOnce, но требуют наличия возможности загрузки файлов (см. раздел «10.18.1 Настройка браузера Internet Explorer»). Для удобного запуска интерфейсов в других браузерах на стартовой HTML странице указаны рекомендации по установке специальных приложений:

- в Chrome и Yandex.browser - Meta4 ClickOnce Launcher;
- в Firefox - Meta4 ClickOnce Launcher или аналогичное, позволяющее запуск приложений ClickOnce.

Для установки указанных специальных приложений в браузер могут понадобиться соответствующие права.

Требования к настройке браузеров:

- для автоматического запуска ClickOnce в разных браузерах должно быть установлено расширение под необходимый браузер. После скачивания файла его необходимо будет запустить;
- если расширение не установлено, то браузер будет скачивать файл установщика каждый раз при переходе по ссылке экземпляра ПК.

При установленных плагинах ClickOnce будет скачиваться и запускаться сразу.

Без установки рекомендованных плагинов, по нажатию на ссылки будет осуществляться скачивание ClickOnce и выдаваться предупреждение о скачивании потенциально опасного ПО. После скачивания файла его необходимо будет запустить.

Для корректной работы ПК необходимо, чтобы на рабочей станции был установлен пакет MS XML (версии 4.0, 6.0).

Для возможности печати и экспорта списка заявок в формат Excel, Word необходимо, чтобы на рабочих станциях также был установлен Microsoft Excel, Word не ниже версии 2003.

4.4 Настройки браузера Яндекс и политик безопасности для него

Для настройки клиентского рабочего места необходимо назначить Yandex.browser, как браузер по умолчанию.

4.4.1 Запросы на отправку

Для корректной работы уведомлений в Yandex.browser необходимо включить опцию «Показывать запросы на отправку» (Рисунок 4.1).

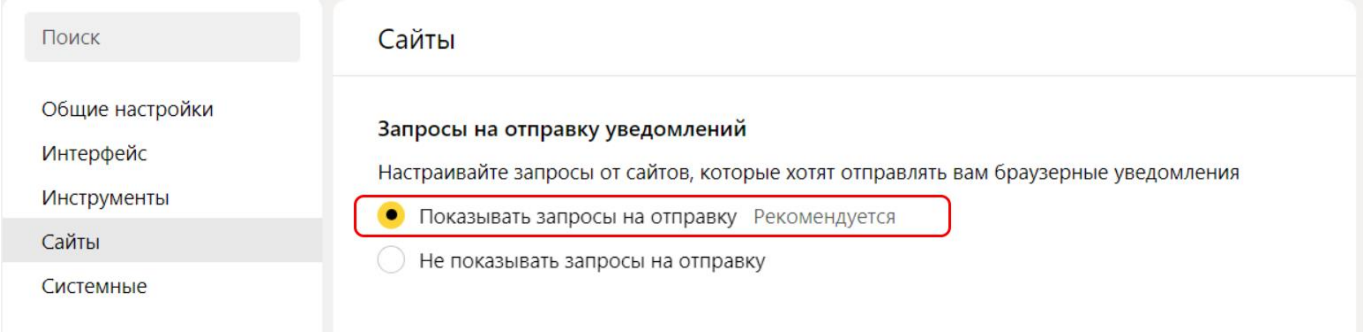

Рисунок 4.1 – Включение опции «Показывать запросы на отправку»

4.4.2 Настройка размера шрифта в браузере

В любом браузере в настройках есть возможность изменения размера шрифта в браузере (Рисунок 4.2).

Настройка размера шрифта в браузере не влияет на размер шрифта в Системе.

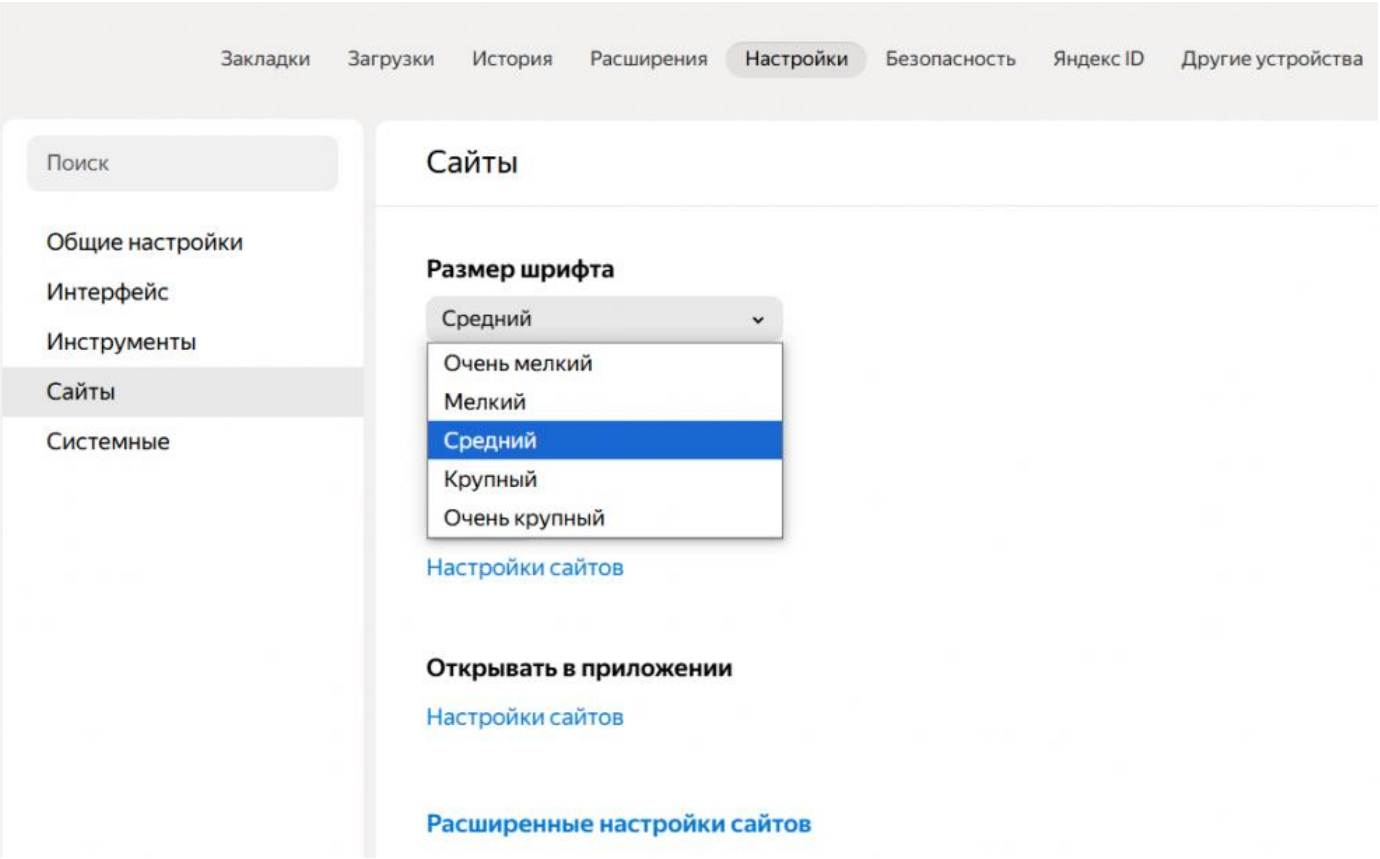

Рисунок 4.2 – Настройка размера шрифта в браузере

4.4.3 Настройка работы через прокси-сервер

Если предполагается работа клиентского приложения через прокси-сервер, то необходимо в настройках подключений указывать конкретные протоколы, для которых применима работа через прокси-сервер (Рисунок 4.3).

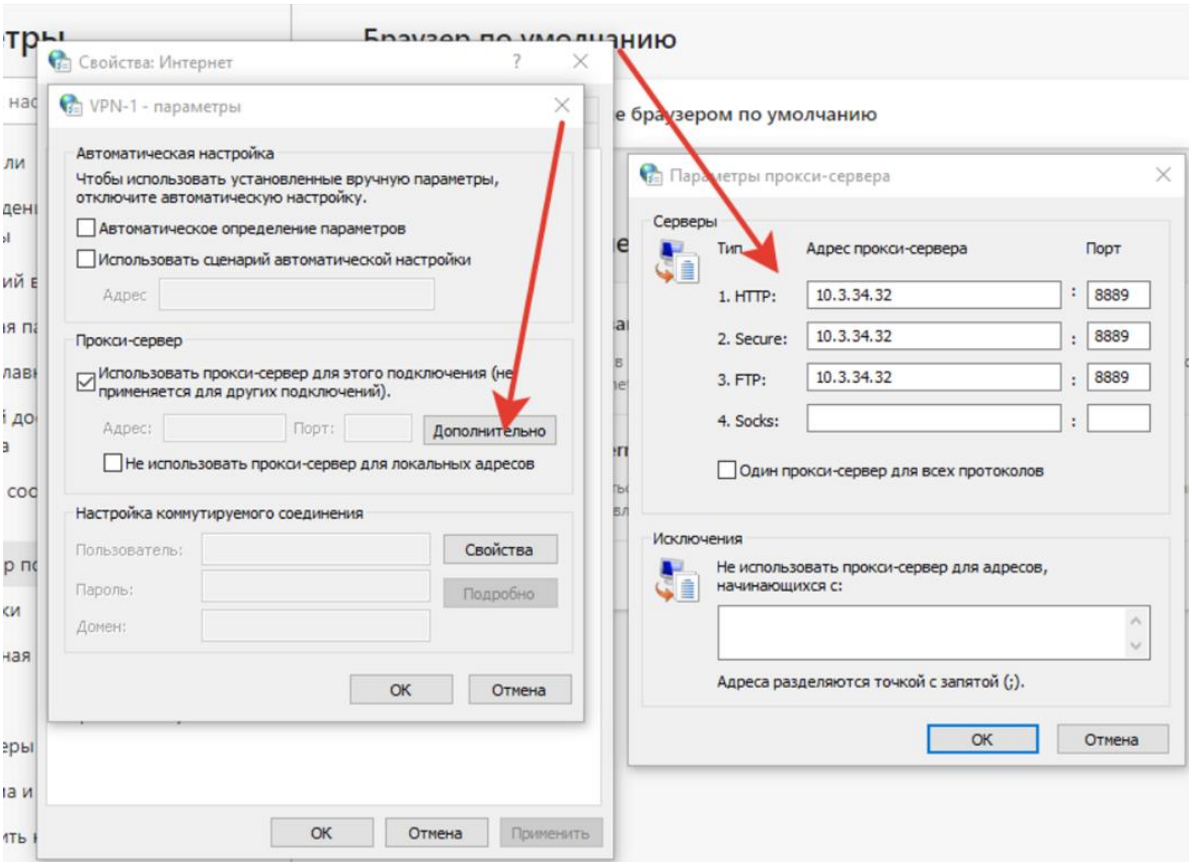

Рисунок 4.3 – Настройки подключений

При этом в системном реестре обязательно эти параметры тоже должны прописаться для каждого протокола в секции ProxyServer (Рисунок 4.4).

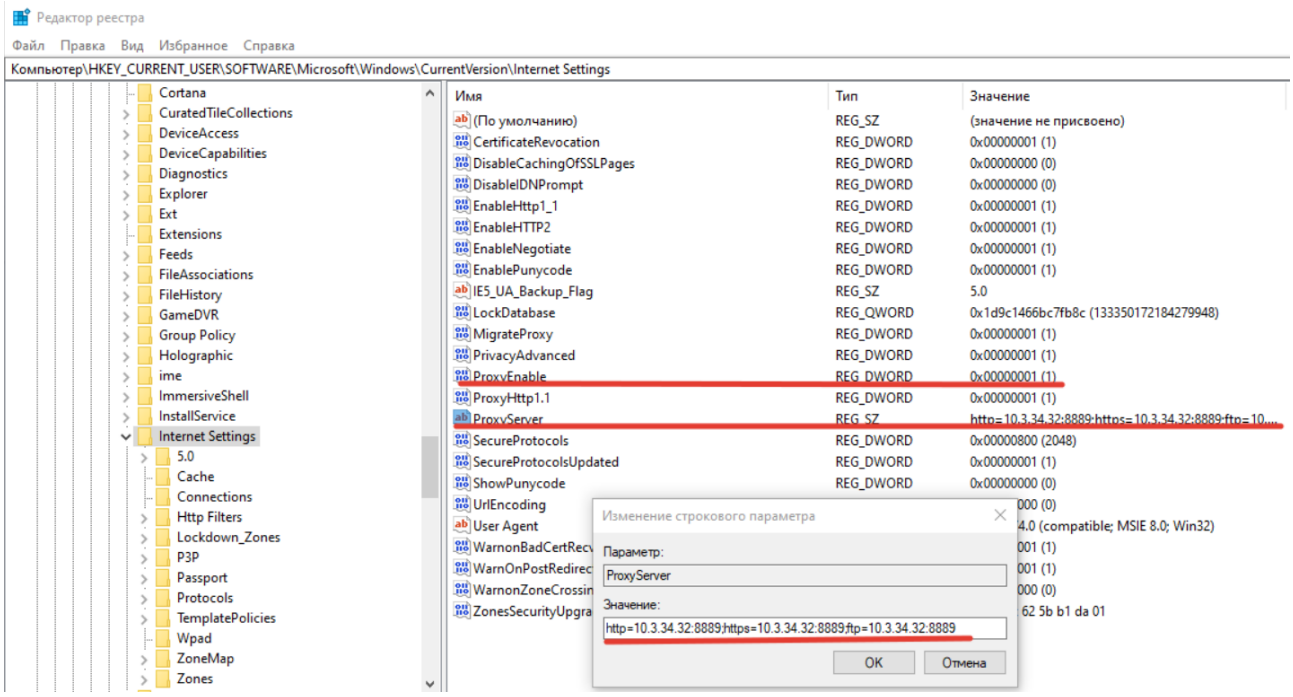

Рисунок 4.4 – Пример системного реестра

4.4.4 Настройка доверенных сайтов

Для того чтобы работала сквозная NT-аутентификация необходимо, чтобы сайты ЗРП.Net находились в доверенных сайтах или в зоне интрасети (настраивается политиками безопасности).

Необходимо настроить политику для конфигурации компьютера, по пути: «Политика Яндекс браузер» -> «Конфигурация компьютера» -> «Политики» -> «Административные шаблоны» -> «Яндекс» -> «Яндекс браузер» -> «Настройки прокси-сервера и аутентификации»:

- включить политику AuthServerAllowlist (Разрешить аутентификацию на серверах из списка) и задать список серверов Kerberos для передачи прав.
  - Задан: *.stand.local
- включить политику AuthNegotiateDelegateAllowlist (Разрешить делегирование прав по протоколу Kerberos на серверах) и указать список серверов (в том числе прокси-серверов), для которых вход sso login будет включен по умолчанию.
  - Задан: *.stand.local.

Аналогично настроить политику для конфигурации пользователя.

4.4.5 Установка расширения для браузера «Помощник ЗРП.Net»

Для полноценной работы приложения на АРМ пользователей рекомендуется установить расширение «Помощник ЗРП.Net».

Для установки расширения «Помощник ЗРП.Net» необходимо на рабочем месте пользователя настроить политики для браузера. Политики можно настроить для текущего пользователя и для локального компьютера.

Важно!

- Настройки для локального компьютера приоритетнее, чем настройки текущего пользователя, поэтому следует проверить, что настроена только одна из политик.
- В приведенных ниже примерах указан url = <all_urls> и идентификатор (ключ) расширения mellbkaobpfhbghncnhloeggbmkmcokb.

- Данные параметры могут быть изменены.

Существуют разные способы редактирования групповых политик. Далее рассмотрен пример редактирования через редактор реестра.

1. В системном поиске необходимо ввести regedit.
2. Правой кнопкой мыши нужно нажать на Редактор реестра (или regedit.exe) и выбрать «Запуск от имени администратора». Если нужно, ввести пароль администратора.
3. В строку пути вставить «Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies» или открыть этот путь в панели слева.
4. Нажать «Правка» → «Создать» → «Раздел».
5. Ввести Yandex.Browser.
6. В новом разделе создать разделы «ExtensionInstallAllowlist» и «ExtensionInstallSources».
7. В раздел «ExtensionInstallAllowlist» внесите строковый параметр с идентификатором расширения mellbkaobpfhbghncnhloeggbmkmcokb
8. В раздел «ExtensionInstallSources» внесите строковый параметр с указанием url для скачивания, по возможности <all_urls>.

   Пример редактора реестра (Рисунок 4.5).

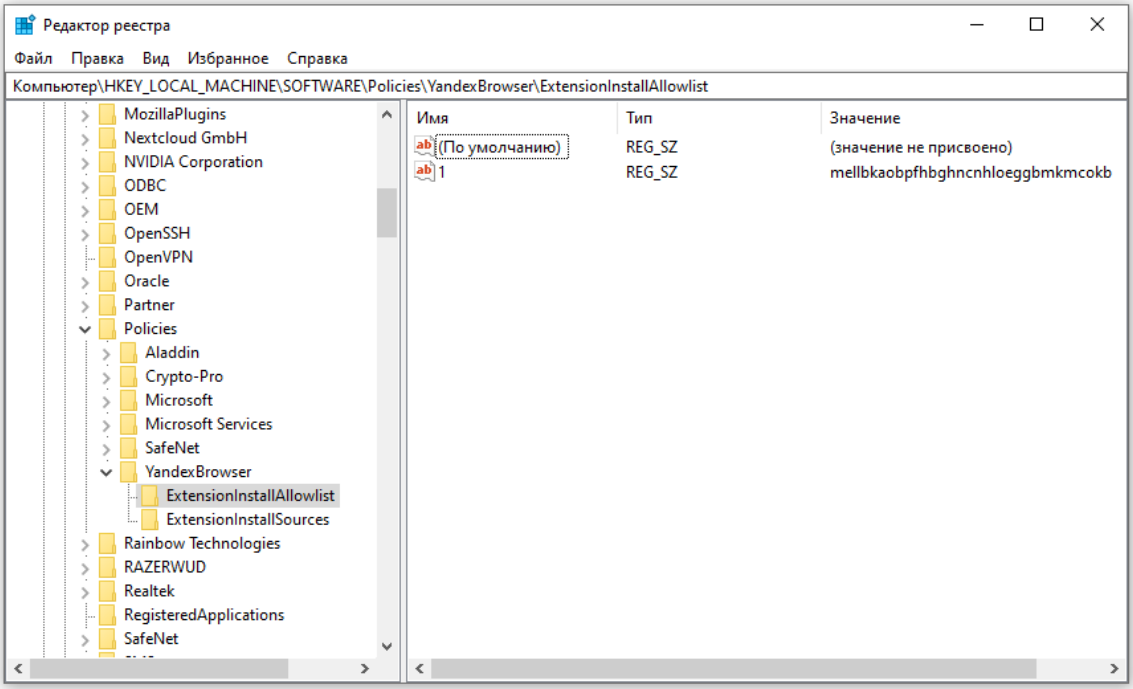

Рисунок 4.5 – Пример редактора реестра

Политики применяются после перезапуска браузера или перезапуска компьютера пользователя. Чтобы убедиться, что политики применились необходимо открыть в браузере страницу *«browser://policy»*. Новые политики должны присутствовать в списке (Рисунок 4.6).

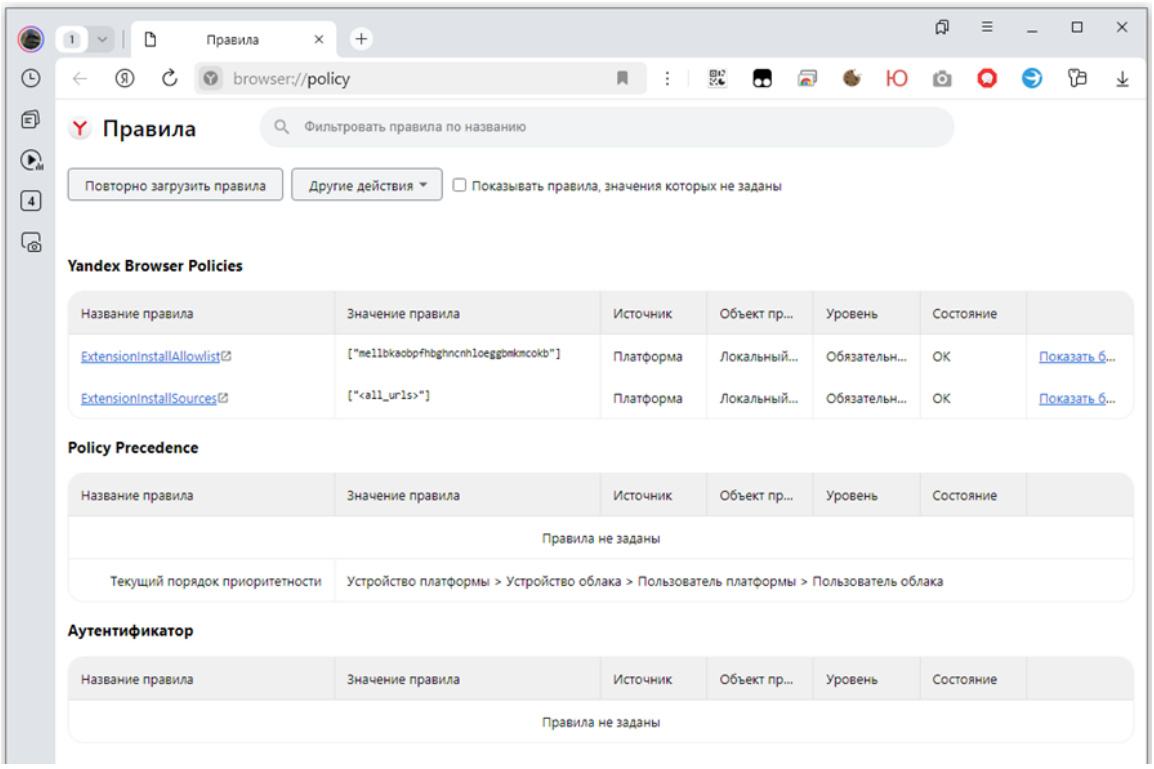

Рисунок 4.6 – Просмотр политик

Есть два варианта установки расширения «Помощник ЗРП.Net»:

Вариант 1. Для установки расширения необходимо в браузере перейти по ссылке: https://chromewebstore.google.com/detail/помощник-zrpnet/mellbkaobpfhbghncnhloeggbmkmcokb?hl=ru (Рисунок 4.7).

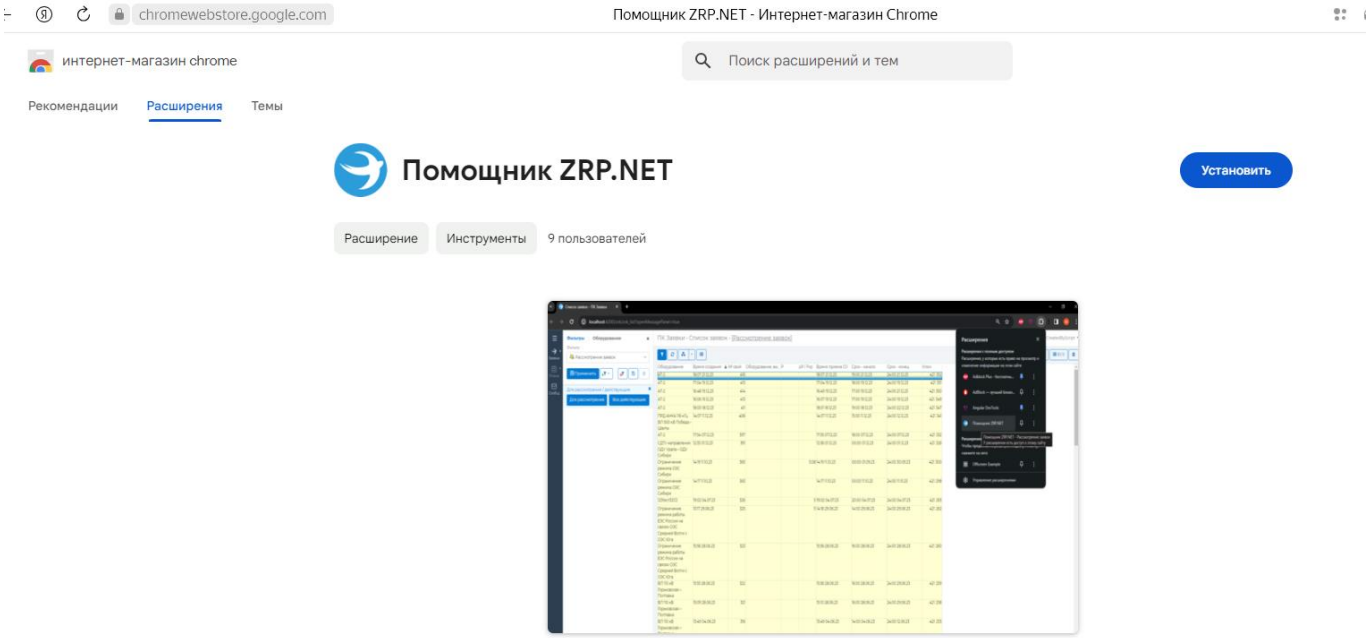

Рисунок 4.7 – Копирование файла .crx

Вариант 2. Если у пользователя нет доступа к интернету, то необходимо использовать файл расширения из комплекта поставки из папки «ZRP_helper».

В YandexBrowser открыть страницу browser://tune/ и скопировать файл .crx, как показано на рисунке 4.8.

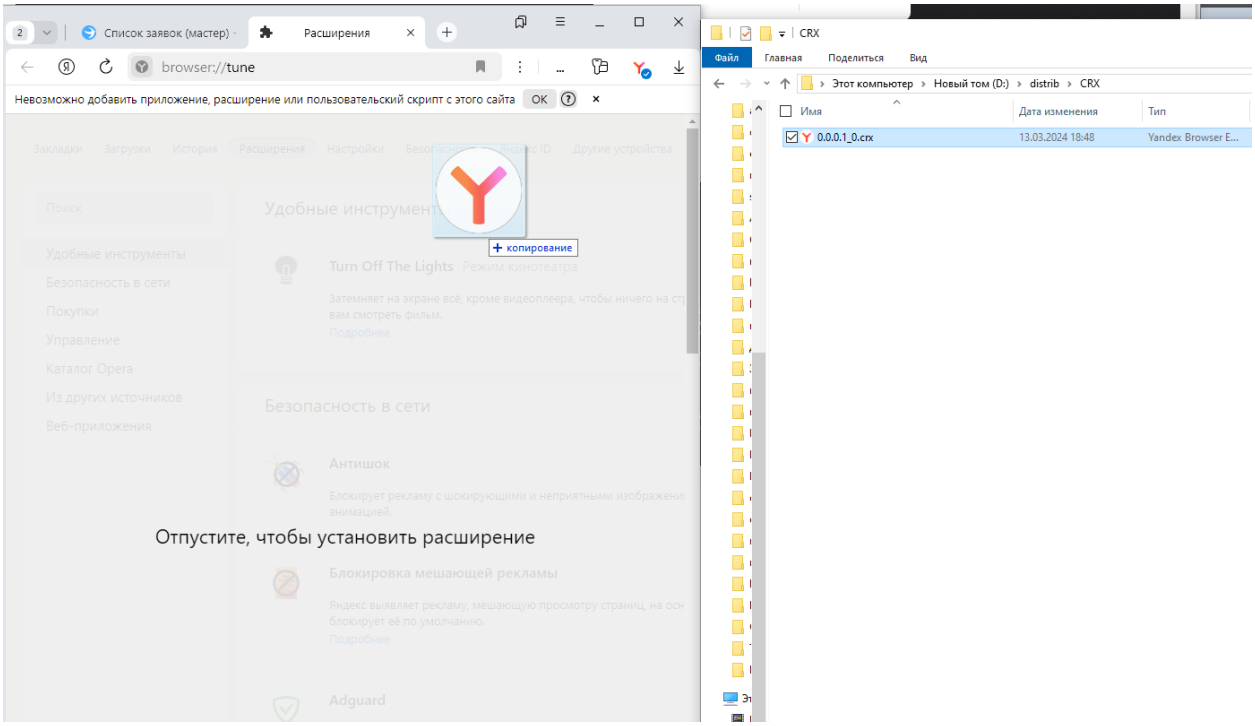

Рисунок 4.8 – Копирование файла .crx

Далее должно появиться окно с предложением установить расширение (Рисунок 4.9).

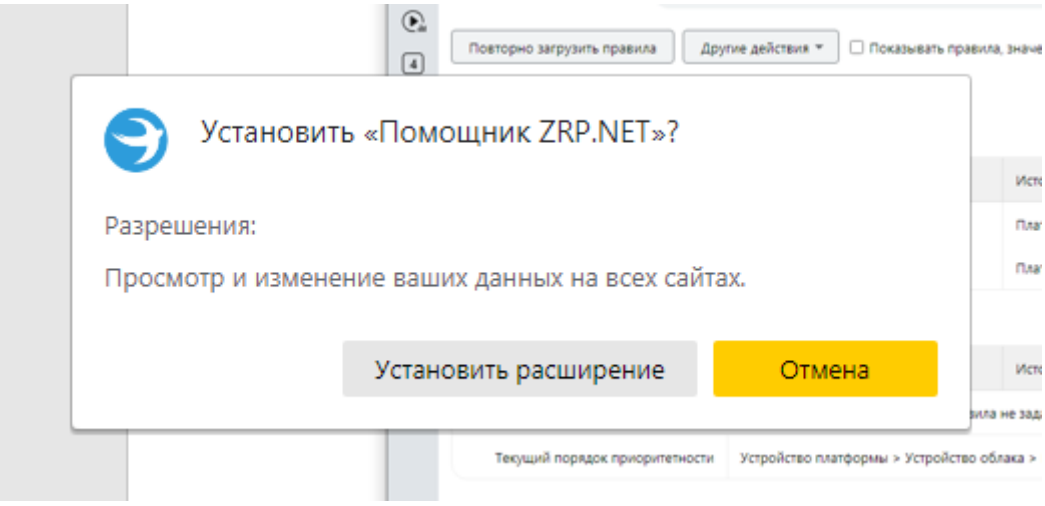

Рисунок 4.9 – Установка «Помощник ZRP.Net»

Необходимо выбрать пункт «Установить расширение». После установки расширения появится уведомление об успешности установки (Рисунок 4.10).

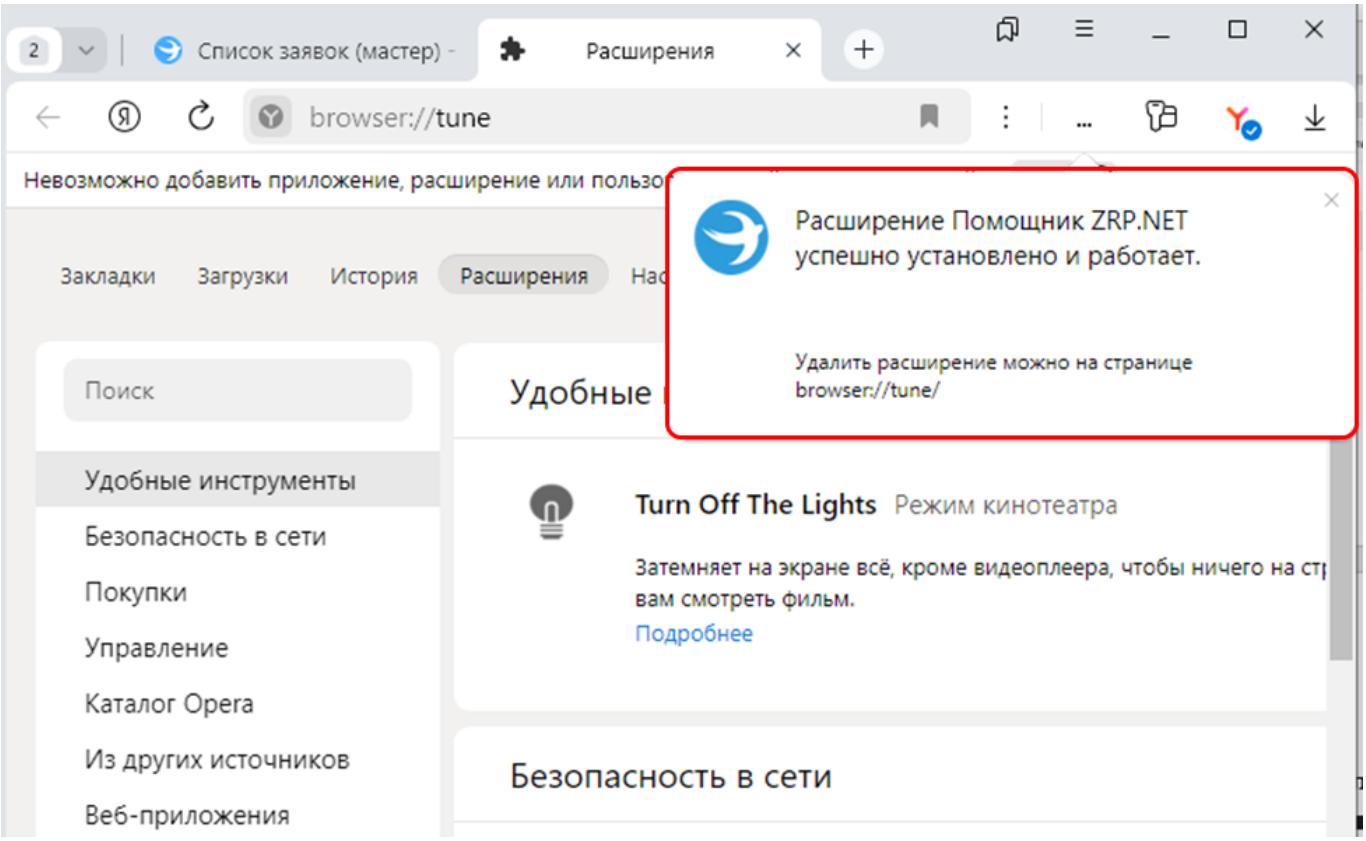

Рисунок 4.10 – Уведомление об успешности установки

Перейти в список расширений браузера по ссылке browser://tune/ и убедиться, что расширение включено (Рисунок 4.11).

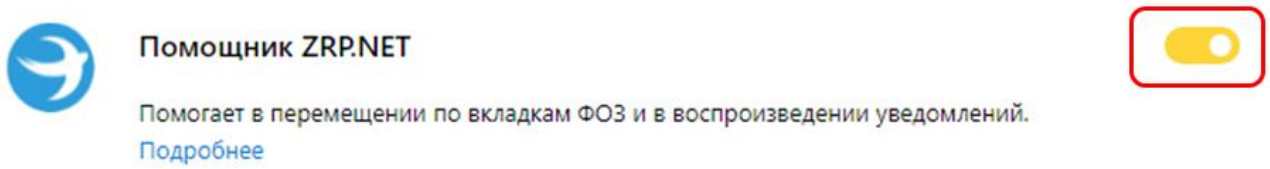

Рисунок 4.11 – Расширение включено

4.4.6 Особенности отображения уведомлений в ОС Linux

Некоторые особенности отображения уведомлений в различных браузерах в ОС Linux:

- В Firefox по умолчанию уведомления появляются во всплывающем окне в правом верхнем углу и остаются до тех пор, пока их не закроют (Рисунок 4.12).

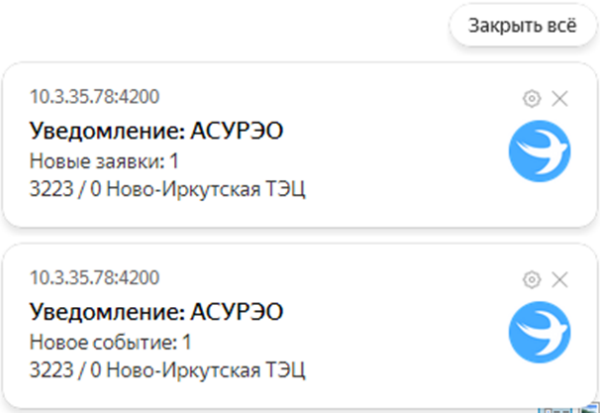

Рисунок 4.12 – Отображение уведомлений в Firefox

- В Chrome и Яндекс сначала отображаются уведомления как на рисунке 4.13, но в какой то момент начинают отображаться уведомления как на рисунке 4.12.

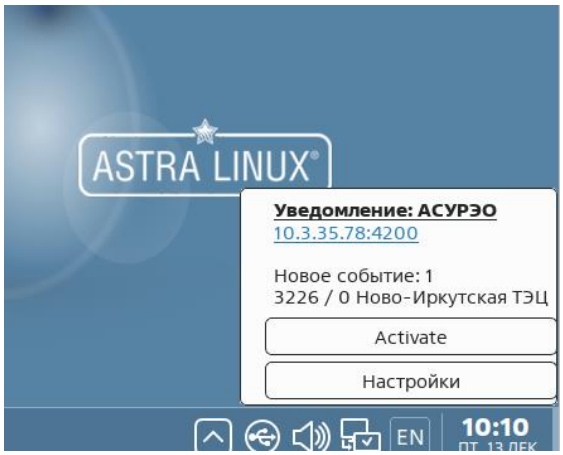

Рисунок 4.13 – Отображение уведомлений в Chrome и Яндекс

Также стоит отметить, что внешний вид push-уведомлений в разных браузерах на Linux может отличаться. Например, в Chrome на Linux не присылают логотип и иконку, а в Firefox уведомление ужимают, но оставляют маленькое лого.

5 Комплект поставки на ОС MS Windows

В комплект поставки программного комплекса на ОС MS Windows входят:

- Setup.exe – программа для запуска установщика;
- InstanceSetup.data – вспомогательный файл установщика, необходим для корректной работы установщика;
- папка «mssql» – содержит скрипты для обновления базы данных;
- папка «postgres» – содержит скрипты для обновления базы данных;
- PGAdmin – инструментарий СУБД;
- папка «Modules for IIS x64» – содержит модули URL Rewrite 2.0 и Application Request Routing 2.0, которые необходимы для настройки IIS в Windows 2008/2012 x64;
- папка «Modules for IIS x32» – содержит модули URL Rewrite 2.0 и Application Request Routing 2.0, которые необходимы для настройки IIS в Windows 2008/2012 x32;
- NetFx4.0_x86_x64 – MS FrameWork версии 4.0 для Windows 2008/2012 x32/x64;
- NetFx4.5_x86_x64 – MS FrameWork версии 4.5 для Windows 2008/2012 x32/x64;
- драйверы электронного ключа защиты (файлы папки driver);
- утилита диагностики электронного ключа защиты;
- электронный ключ защиты, подключаемый к USB-порту.

Примечание. Файлы «Modules for IIS x64», «Modules for IIS x32», «NetFx4.0_x86_x64», «NetFx4.5_x86_x64» необходимо устанавливать, в случае, если они отсутствуют в операционной системе (см. Список установленных компонентов Windows).

6 Комплект поставки на ОС семейства Linux

В комплект поставки программного комплекса на ОС семейства Linux входят:

- файлы docker-образа для создания контейнера ПК «АСУРЭО», включая мигратор базы данных – средство для обновления базы данных ПК «АСУРЭО», часть инсталлятора ПК «АСУРЭО» и web-сервера nginx;
- конфигурационные файлы: zvk.ini, docker-compose.yml, appsettings.json, authServer.settings.json, sms.ZRP.WebApi.settings.json;
- конфигурационный файл web-сервера nginx.

7 Последовательность установки ПК «АСУРЭО» на ОС MS Windows

Установку ПК «АСУРЭО» на ОС MS Windows необходимо производить в следующей последовательности:

1. Установить веб-сервер IIS.
2. Установить СУБД (MS SQL / PostgreSQL), создать базу данных и пользователя, осуществляющего доступ к базе.
3. Установить ПК «АСУРЭО».
4. Проверить работоспособность установленного ПО.

8 Последовательность установки ПК «АСУРЭО» на ОС семейства Linux

Установку ПК «АСУРЭО» на ОС семейства Linux необходимо выполнять в следующей последовательности:

Примечания:

- Для возможности установки системного ПО пользователь должен быть в группе sudo.
- Для установки системного ПО потребуются базовый и расширенный репозитории Astra Linux, необходимо их предварительно подключить. Адрес репозиториев уточнять у СПАК ИА.

1. Установка ОС Linux.
2. Установка docker Ce.
3. Установка docker-compose.
4. Добавление активного пользователя в группу docker.
5. Загрузка docker образа ПК «АСУРЭО».
6. Установка и настройка СУБД Postgres Pro.
7. Загрузка docker образа PGAdmin и запуск docker контейнера PGAdmin.
8. Восстановление из дампа БД ПК «АСУРЭО», создание пользователя, осуществляющего доступ к БД.
9. Настройка конфигурационных файлов zvk.ini, confighost.txt и config.json.
10. Загрузка docker контейнера web-сервера nginx и настройка конфигурационного файла.
11. Запуск контейнеров ПК «АСУРЭО» и web-сервера nginx.

После установки ПК «АСУРЭО» необходимо запустить браузер и перейти на заглавную страницу.

Для авторизации в системе необходимо использовать имя и пароль настроенной учётной записи в ПК «АСУРЭО».

Перед началом работ с Docker для разграничения прав и удобства необходимо добавить активного пользователя ОС Linux в группу Docker – это дает возможность запускать команды с docker без привилегий sudo.

Команда добавления пользователя в группу docker:

sudo usermod –aG docker username

После выполнения команды необходимо перелогиниться в системе, чтобы применились права.

9 Установка и настройка системного ПО

9.1 Установка ОС Linux

При установке ОС Linux необходимо обратить внимание на следующие пункты:

1. Разметка дисков. Рекомендуем выбрать метод разметки *«Авто – использовать весь диск и настроить LVM»*.

   Примечание: на текущий момент не требуется выполнять настройку LVM, но указанный метод разметки дает возможность расширения диска в будущем.

   Далее необходимо следовать шагам установки (Рисунок 9.1 – Рисунок 9.5).

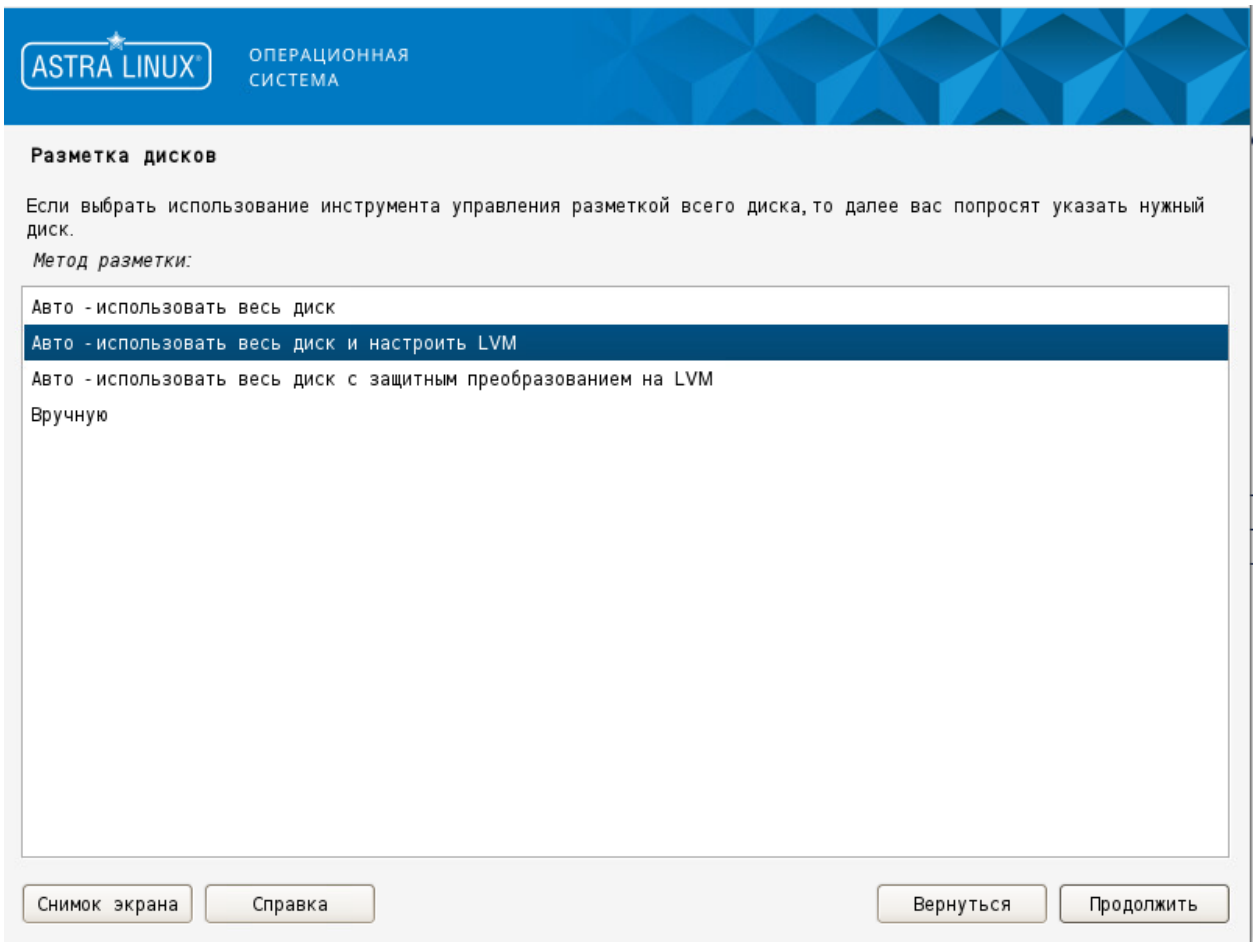

Рисунок 9.1 – Метод разметки дисков

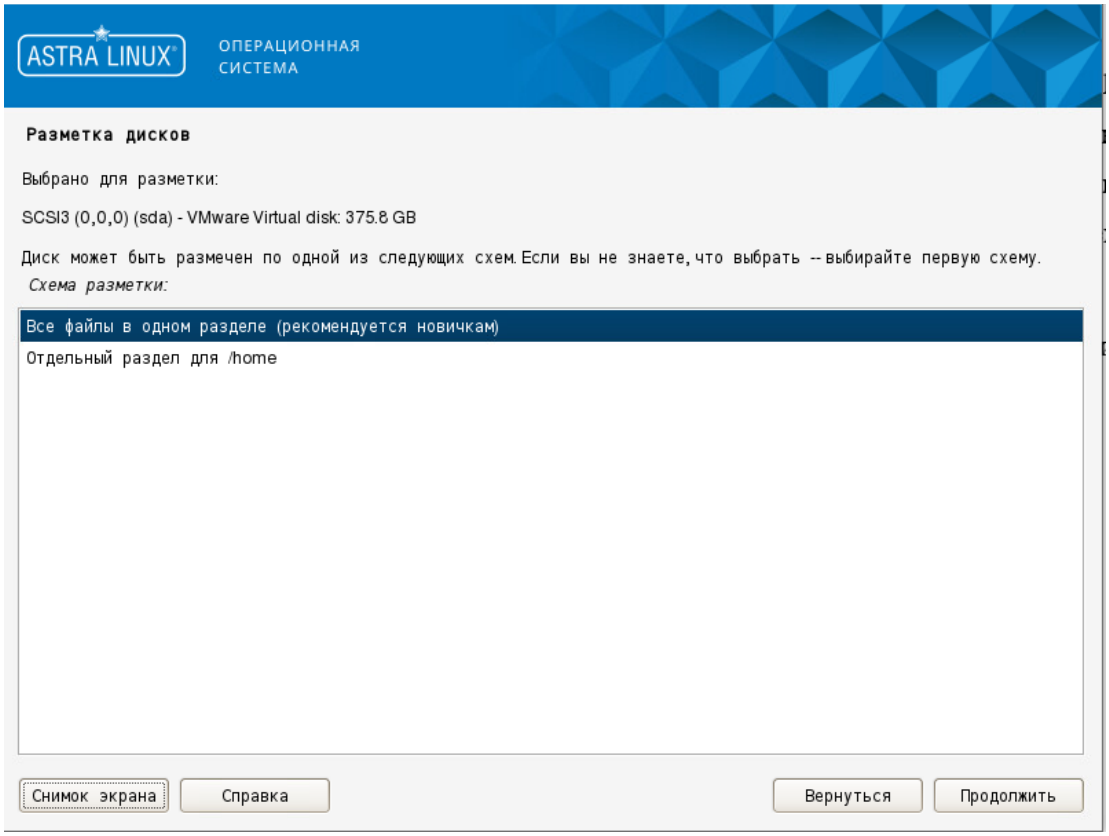

Рисунок 9.2 – Выбор схемы разметки

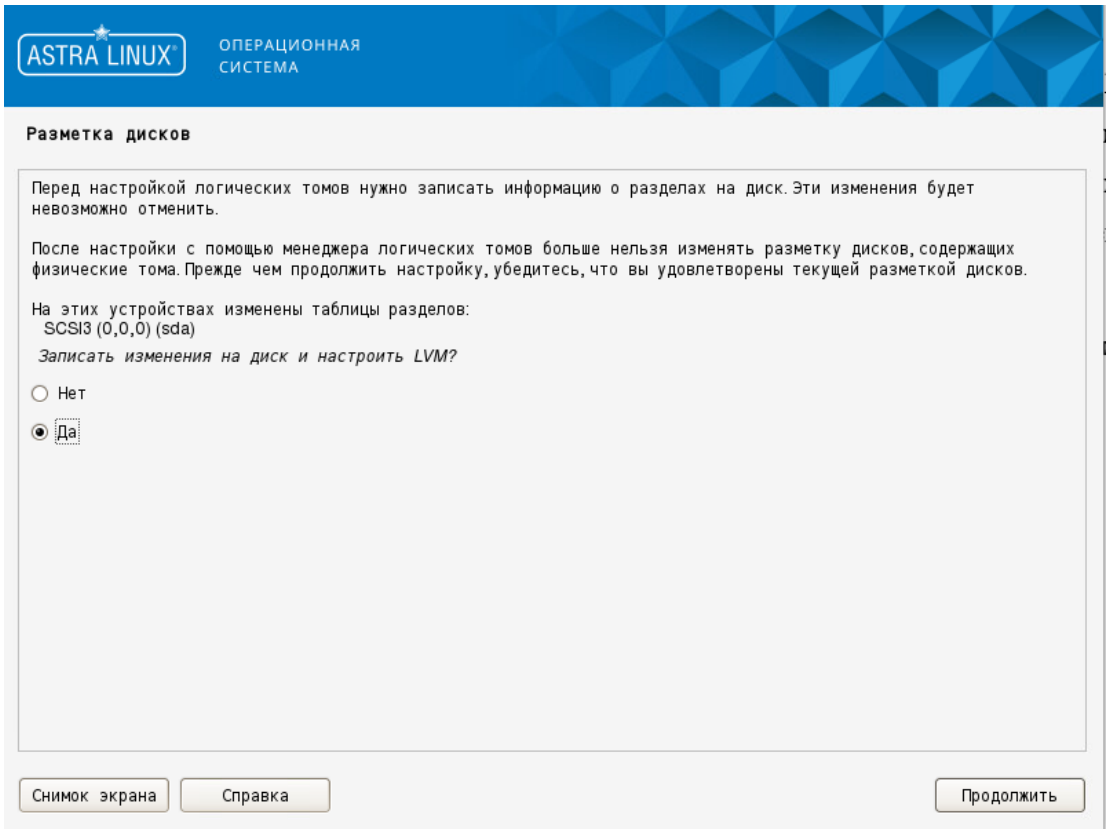

Рисунок 9.3 – Подтверждение выбранных параметров

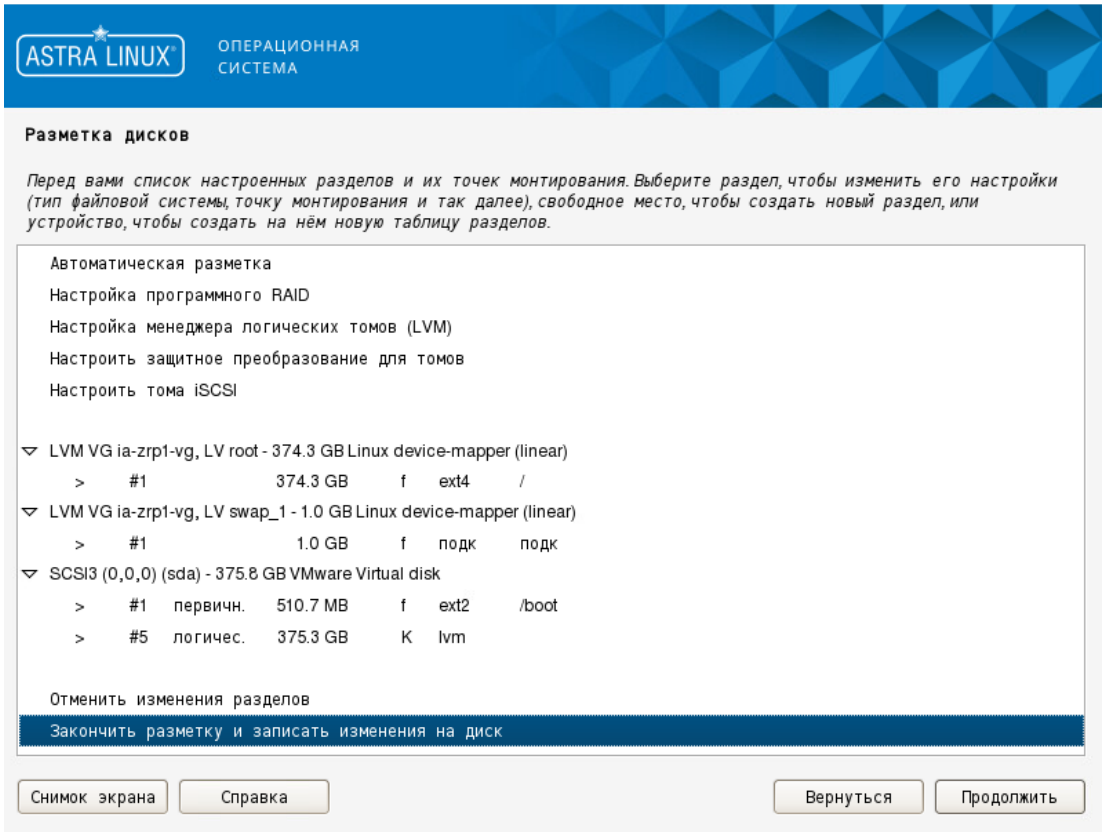

Рисунок 9.4 – Завершение разметки дисков

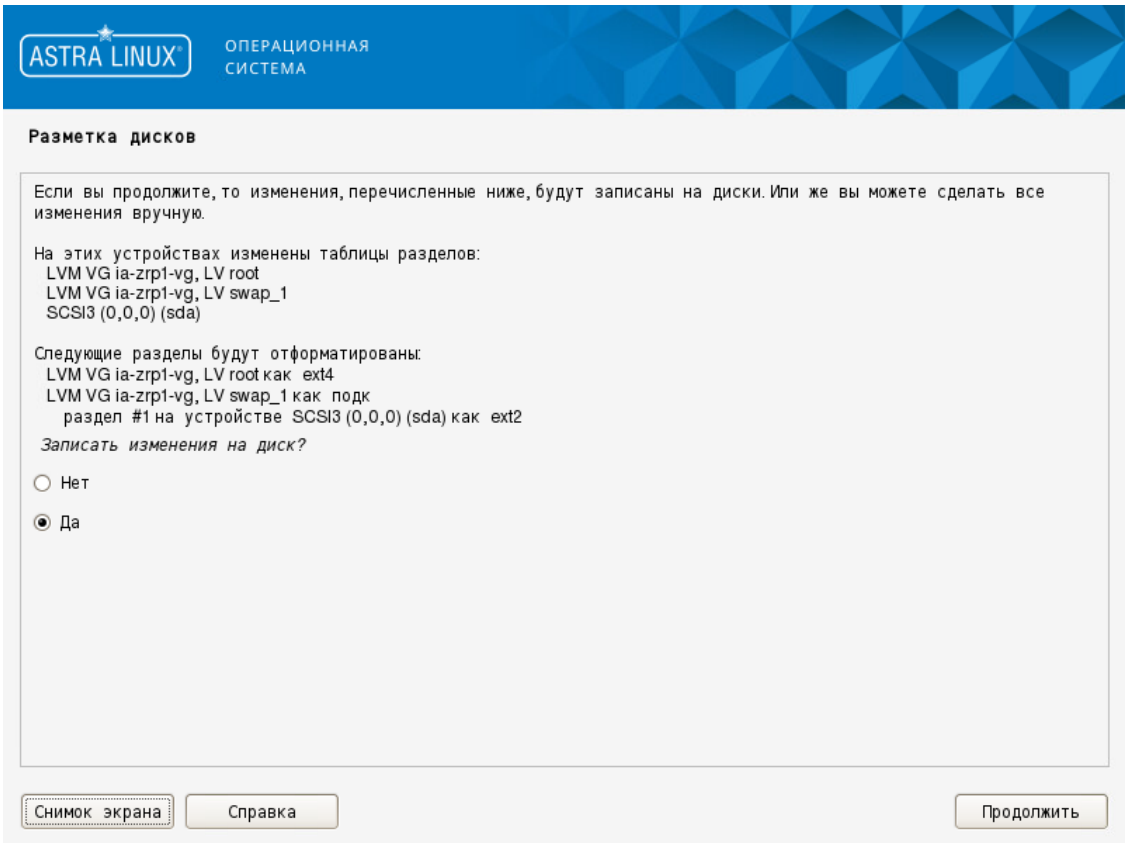

Рисунок 9.5 – Запись изменений по разметке дисков

2. Выбор ядра установки (Рисунок 9.6).

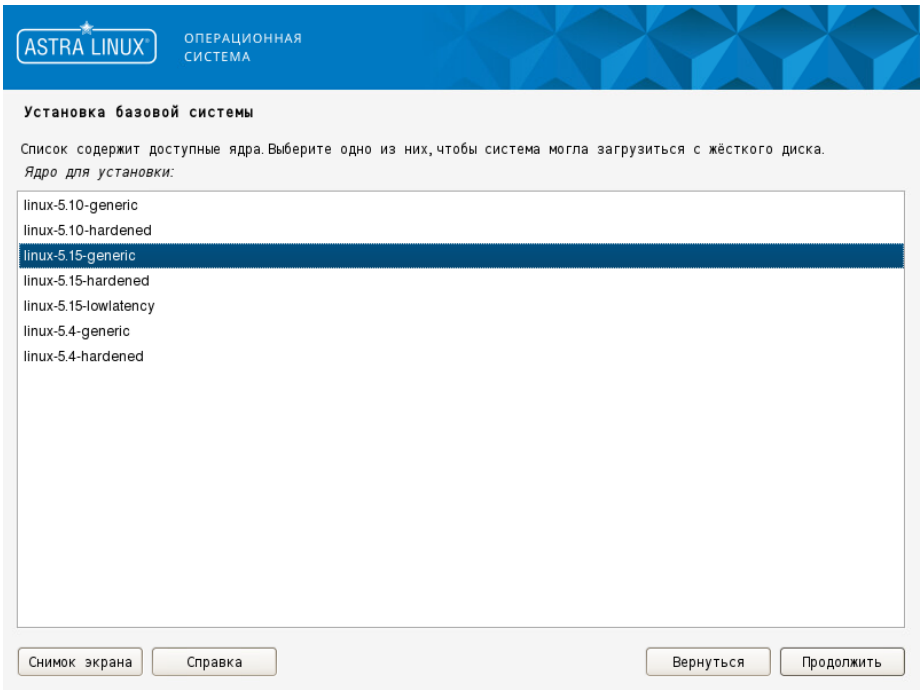

Рисунок 9.6 – Выбор ядра для установки

3. Выбор дополнительного ПО. Необходимо установить флаги *«Графический интерфейс Fly»*, *«Консольные утилиты»*, *«Средства удаленного подключения SSH»* (Рисунок 9.7).

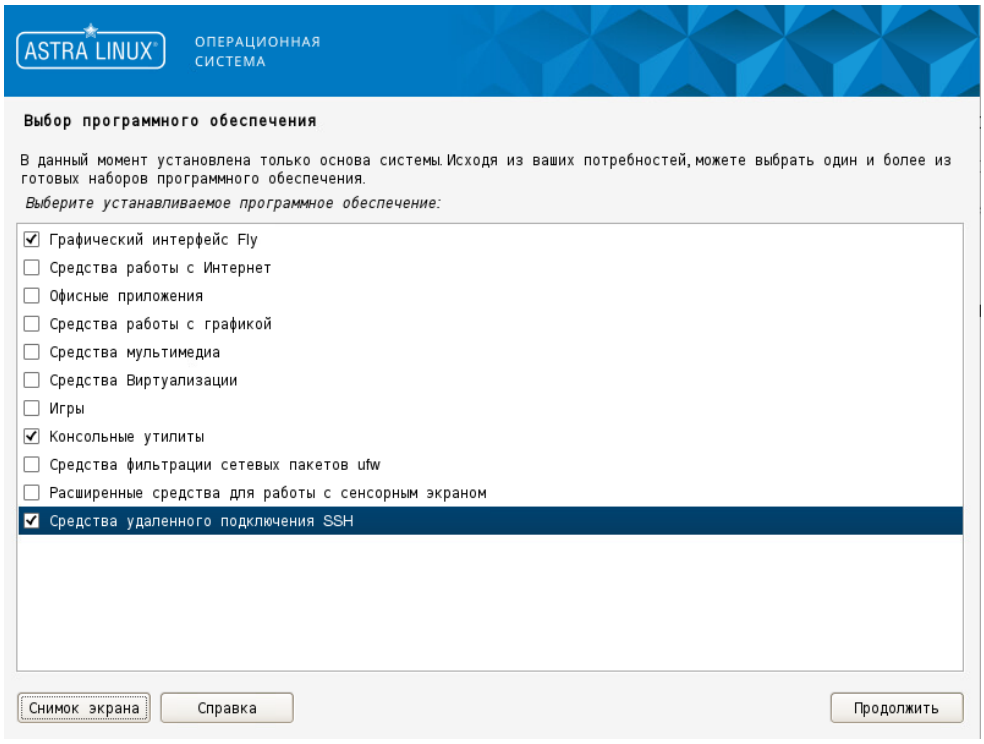

Рисунок 9.7 – Выбор дополнительного ПО

4. Дополнительные настройки ОС. Необходимо выбрать уровень защищенности, как минимум указать *«Базовый уровень защищенности «Орел»* (Рисунок 9.8).

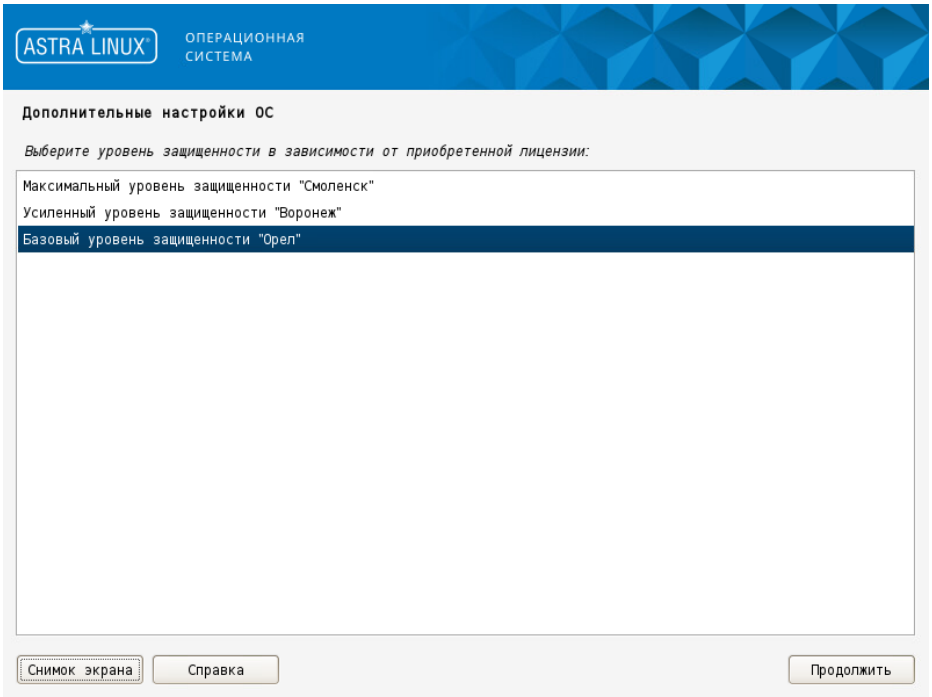

Рисунок 9.8 – Выбор уровня защищенности

На следующем шаге выбор дополнительных настроек не требуется (Рисунок 9.9).

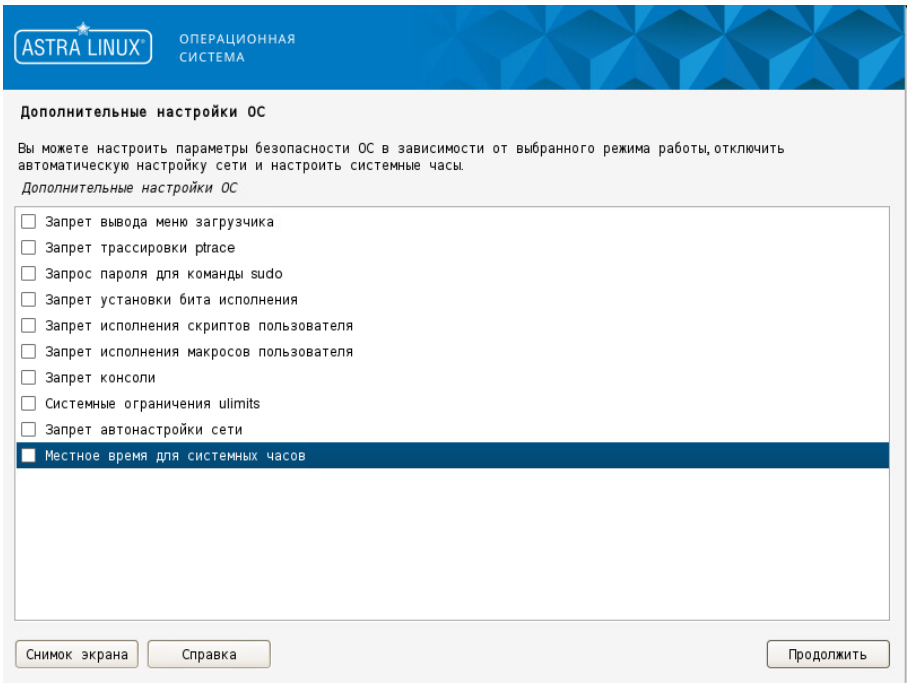

Рисунок 9.9 – Выбор дополнительных настроек

9.2 Установка docker и docker-compose

Установку необходимо производить в следующей последовательности:

1. Обновить список пакетов:
   sudo apt update
2. Установить docker-compose:
   sudo apt install docker-compose
3. Проверить работу docker:
   systemctl status docker

Его состояние должно быть «**Active».**

Примечание: Для установки docker-compose необходимо использовать внутренний репозиторий. Адрес репозитория уточнить у СПАК ИА.

9.3 Настройка прав и доступов для управления СП и docker

Перед началом работ с docker и управлением СП для разграничения от root прав необходимо создать группу для активных пользователей сервера и добавить на группу доступ на чтение/запись и исполнение в каталоге расположения СП, а также нужно добавить созданную группу в группу docker – это дает возможность запускать команды с docker без привилегий sudo.

Opt – это директория в UNIX-подобных операционных системах, которая обычно используется для установки программного обеспечения, которое не является частью стандартного дистрибутива операционной системы.

Для размещения прикладного ПО необходимо подготовить каталог приложения и предоставить права на запись в каталог для группы администраторов Системы.

1. Создать каталог /opt/zvk, выполнив команду: *mkdir /opt/zvk*
2. Рекурсивно назначить права, выполнив команду: *sudo chmod -R 755 /opt/zvk*

9.4 Настройка сети docker

Если ваша локальная подсеть находится в диапазоне адресов, начинающихся с 172.x.x.x, то рекомендуются изменить настройки сети docker по умолчанию во избежание сетевых конфликтов, т.к. стандартная сеть докера также начинается с 172.x.x.x.

Для этого в файле /etc/docker/daemon.json прописываем следующие настройки сети для docker:

1. *udo nano /etc/docker/daemon.json*

Скопировать настройки:

{

"live-restore": true,

"bip": "192.168.10.1/24",

"default-address-pools": [{

"base": "192.168.0.0/16",

"size": 24

}]

}

Если необходимо, то изменить подсеть на ту, с которой не будет сетевых конфликтов.

Сохранить и перезапустить службу docker.

2. *sudo systemctl restart docker*

Проверить изменение ip для сетевого адаптера docker.

3. *ip a | grep docker*

Если все сделано правильно, то должны увидеть изменённый ip (Рисунок 9.10).

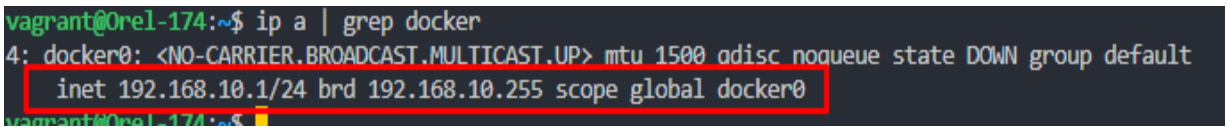

Рисунок 9.10 – Измененный ip

9.5 Установка и настройка веб-сервера IIS

9.5.1 Установка веб-сервера IIS

Для работы ПК используется веб-сервер IIS (Internet Information Services), входящий в комплект поставки MS Windows.

Для установки ПК на Windows Server 2012 с IIS необходимо выполнить следующие действия:

1. Включить роль IIS (Рисунок 9.11).

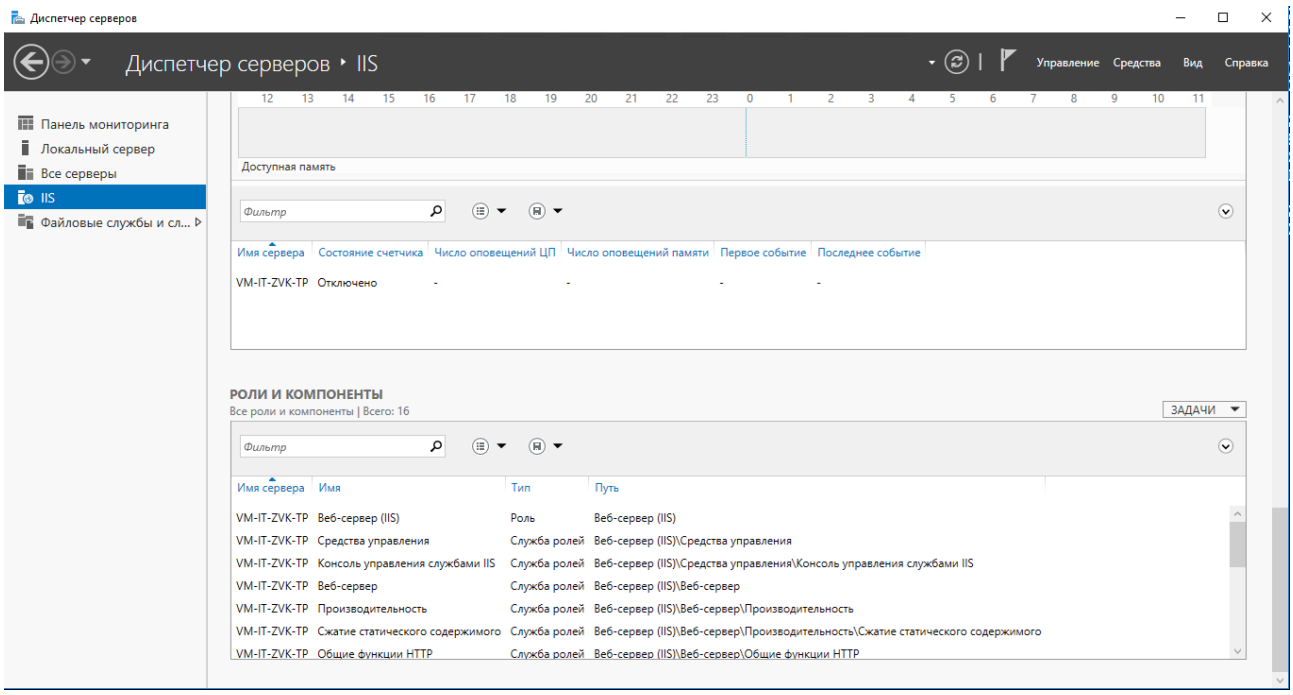

Рисунок 9.11 – Роль Веб-сервер (IIS)

2. Установить службы ролей совместимости с IIS 6 (Рисунок 9.12).

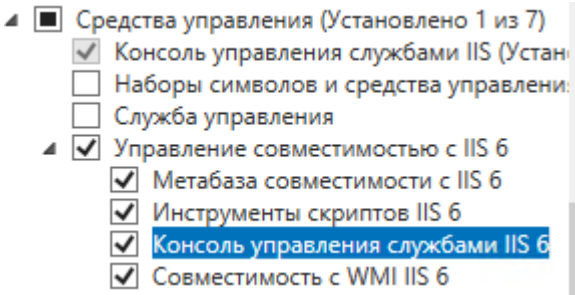

Рисунок 9.12 – Службы ролей совместимости с IIS 6

3. Также установить основные службы ролей (Рисунок 9.13).

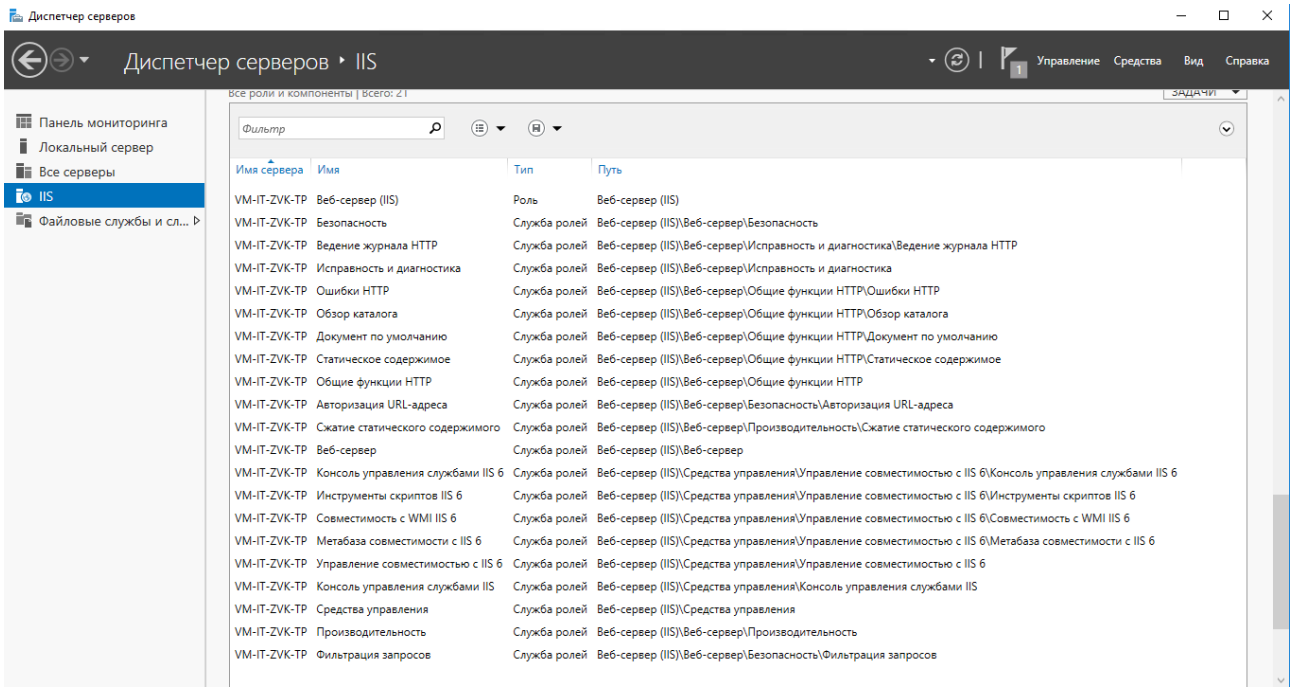

Рисунок 9.13 – Основные службы ролей

9.5.2 Дополнительные настройки web-сервера IIS

В случае использования веб-сервера IIS необходимо установить два дополнительных компонента, не входящих в стандартную поставку IIS:

– для IIS версий 8, 8.5:

- переадресация запросов URL Rewrite 2.0;
- прокси-переадресация Application Request Routing 3.0.

– для IIS версий 9, 10:

- переадресация запросов URL Rewrite 2.0 для ОС Win64 (ОС Windows 2016);
- прокси-переадресация Application Request Routing 3.0 для ОС Win64 (ОС Windows 2016).

Для установки компонент прокси-переадресации Application Request Routing 3.0 необходимо скачать дистрибутив с сайта Microsoft (https://www.microsoft.com/en-us/download/details.aspx?id=47333).

Для установки компонента URL Rewrite необходимо скачать дистрибутив с сайта модулей для IIS (https://www.iis.net/downloads/microsoft/url-rewrite). Так же он доступен в установщике веб-платформы IIS.

При переустановке на сервере АСУРЭО дополнительного компонента Application

Request Routing требуется вручную включить Proxy в Application Request Routing Cache -> Server Proxy Settings -> Enable Proxy (Рисунок 9.14).

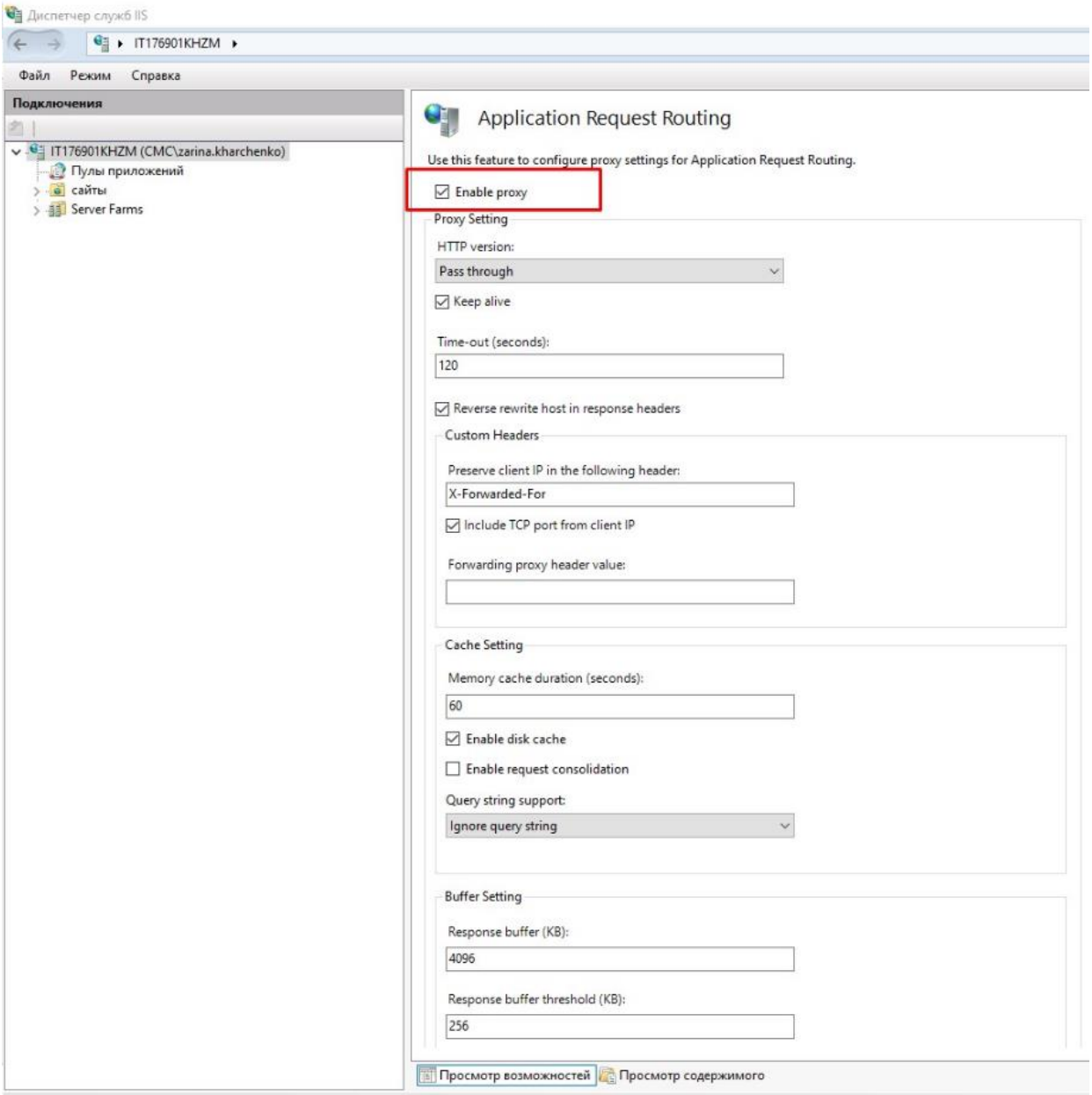

Рисунок 9.14 – Включение дополнительного компонента «Enable Proxy»

9.5.3 Рекомендации

В случае, если в результате отправки графика ремонтов с предприятия-инициатора на предприятие-приемник в Журнале сообщений подсистемы «Планы ремонтов» предприятия-инициатора отображается ошибка: «модуль SOAP. Ошибка Send: Request Entity Too Large (413)», то на предприятие-приемнике необходимо в веб-сервере IIS увеличить настройку «uploadReadAheadSize».

9.6 Настройка конфигурационного файла веб-сервер nginx

Для работы ПК «АСУРЭО» на ОС семейства Linux используется веб-сервер nginx.

Для автоматизированного запуска web-сервера nginx используя docker контейнеры и docker-compose необходимо выполнить следующие действия:

1. Скопировать папку «nginx-config», содержащую конфигурационный файл *«default.conf»* на сервер установки в папку /opt/nginx.

2. Открыть файл *«default.cong»* на редактирование и скорректировать внешний порт подключения и ip адрес сервера.

server {

 # Здесь необходимо задать порт для СП. По умолчанию 80, если он уже занят, то необходимо вписать другой.

listen 80;

listen [::]:80;

 # Здесь необходимо задать настройки для https.

listen 443 ssl;

listen [::]:443 ssl;

ssl_certificate /etc/nginx/certs/nginx.pem;

ssl_certificate_key /etc/nginx/certs/nginx.key;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_ciphers HIGH:!aNULL:!MD5;

ssl_session_cache shared:SSL:100m;

ssl_session_timeout 60m;

ssl_prefer_server_ciphers on;

root /etc/nginx/www;

```
index index.html index.htm;

server_name _;

server_name_in_redirect off;

## AppServer config
location = /appsrv/proxy.dll/help {
        rewrite ^/appsrv/proxy.dll/help$ /appservice/;
}

location ~ ^/appsrv/proxy.dll/help/(.*)$ {
        rewrite ^/appsrv/proxy.dll/help/(.*)$ /appservice/$1;
}

location ~ ^/appsrv/(proxy.dll/)?(.*)$ {
        if ( $http_user_agent ~* 'RemObjects' ) {
                rewrite ^/appsrv/(proxy.dll/)?(.*)$ /appservice/$2;
        }
                rewrite ^/appsrv/(proxy.dll/)?(.*)$ /appsite/$2;
}
location ~ \.application {
        types {
            application/x-ms-application    application;
            application/x-ms-manifest       manifest;
            application/octet-stream        deploy;
```

```
                }
                        }
```

 # В location /appsite и location /appservice в параметре proxy_pass необходимо вписать ip хоста вместо 10.3.29.187.

```
        location /appsite/ {
                proxy_pass http://10.3.29.187:9880/;
                proxy_redirect                  off;
                proxy_set_header        Host                    $http_host;
                proxy_set_header        X-Real-IP               $remote_addr;
                proxy_set_header        X-Forwarded-For
    $proxy_add_x_forwarded_for;
                proxy_set_header        X-Forwarded-Proto       $scheme;
        }

        location /appservice/ {
                proxy_pass http://10.3.29.187:8625/;
                proxy_redirect                  off;
                proxy_set_header        Host                    $http_host;
                proxy_set_header        X-Real-IP               $remote_addr;
                proxy_set_header        X-Forwarded-For
    $proxy_add_x_forwarded_for;
                proxy_set_header        X-Forwarded-Proto       $scheme;
        }
        # End of AppServer config

        location / {
                try_files $uri $uri/ =404;
```

```
        }

    }
```

3. При необходимости отредактировать mapping портов в docker-compose.yml. Ниже приведен пример для портов 80 и 443.

```
version: "3"
services:
  webserver:
    image: nginx:alpine
    restart: always
    container_name: webserver
    ports:
      - "80:80"
      - "443:443"
    volumes:
    - ./nginx-config/conf.d:/etc/nginx/conf.d
   - www:/etc/nginx/www
```

9.7 Настройка отображения шифров

Для корректного отображения шрифтов в установщике и в клиенте ПК «АСУРЭО» необходимо установить следующие настройки. На панели управления Control Panel необходимо выбрать *«Regional and Language Options»* (Рисунок 9.15).

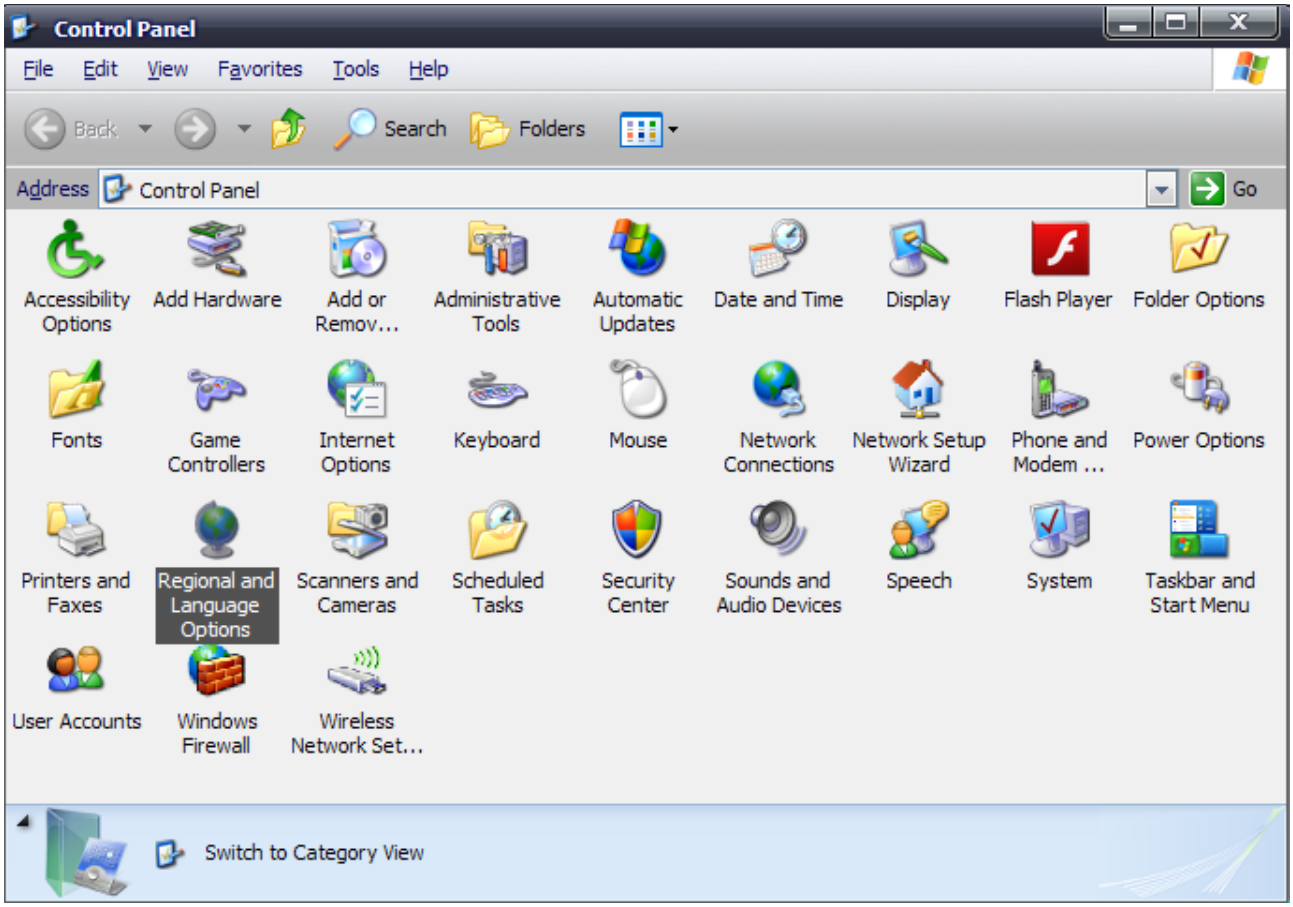

Рисунок 9.15 – Панель управления Control Panel

В окне Regional and Language Options на вкладке Advanced для настройки Language for non-unicode programs необходимо выбрать Russian (Рисунок 9.16).

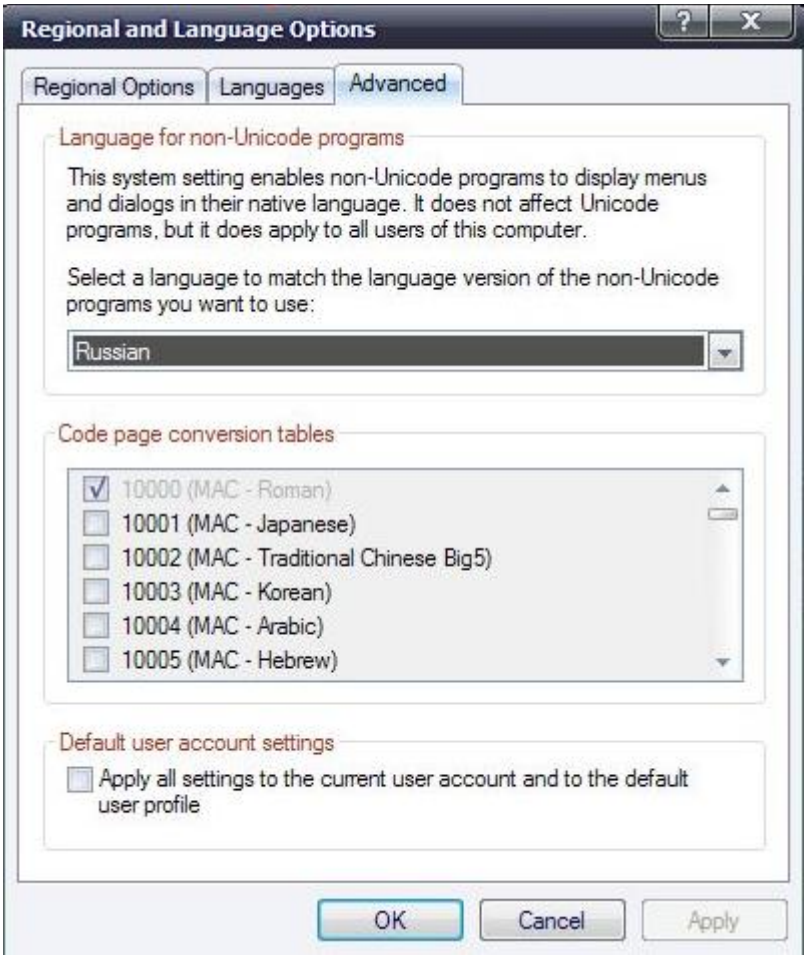

Рисунок 9.16 – Настройка Language for non-unicode programs

При нажатии кнопки «OK» открывается диалоговое окно Advanced, где предлагается использовать имеющиеся версии файлов для применения настройки или взять их из дистрибутива (Рисунок 9.17).

Рисунок 9.17 – Диалоговое окно Advanced

При нажатии кнопки «Yes» используются имеющиеся версии файлов для применения настройки. При нажатии кнопки «No» система запрашивает диск с дистрибутивом.

Для применения настроек необходимо перезагрузить систему. Для этого в диалоговом окне Change Regional Options необходимо нажать на кнопку «Yes» (Рисунок 9.18).

Рисунок 9.18 – Диалоговое окно Change Regional Options

Необходимо в настройке Windows «Регион и язык» в окне «Регион» на вкладке «Форматы» установить значения (Рисунок 9.19):

- Формат – Russian или Русский;
- Краткая дата – dd.MM.yyyy.

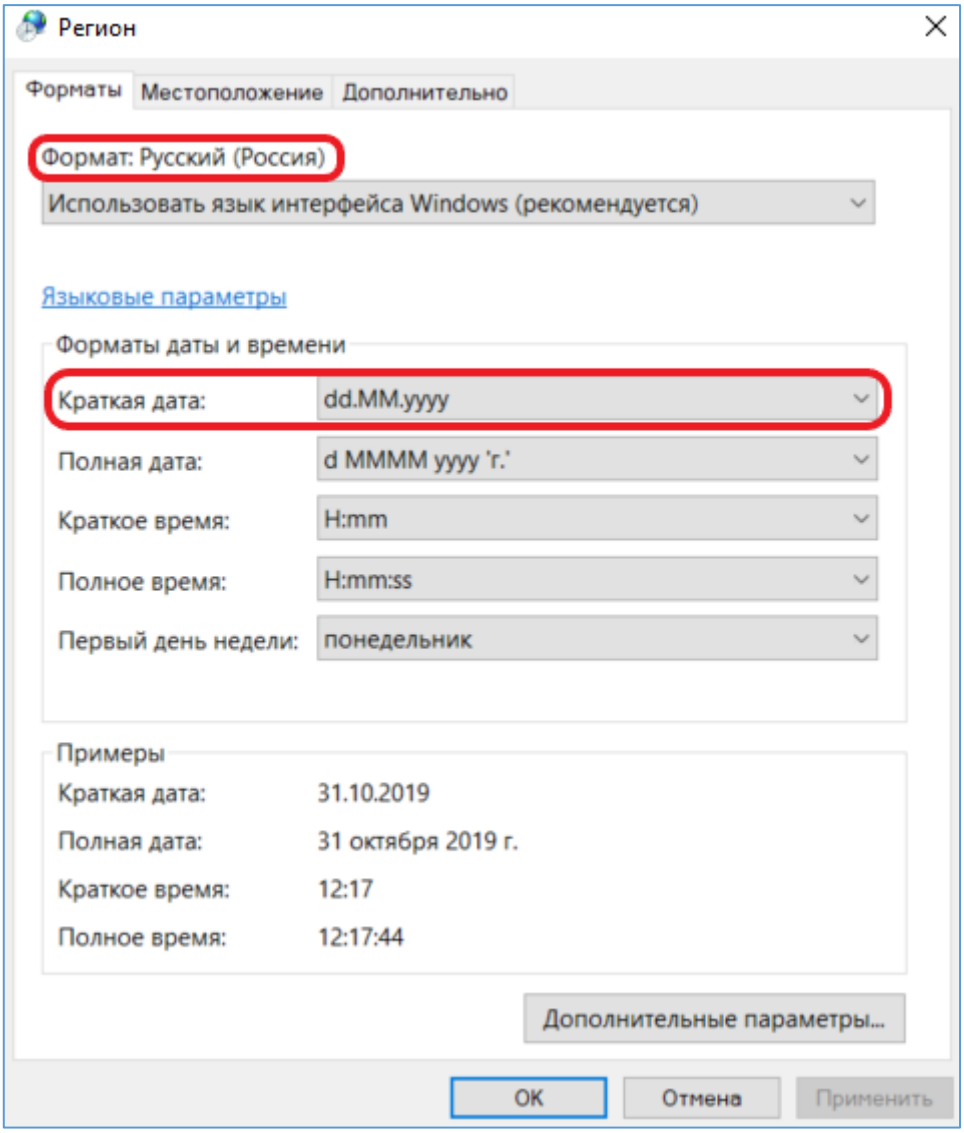

Рисунок 9.19 – Настройка языка и краткой даты

9.8 Установка и настройка СУБД на ОС MS Windows

Сервер СУБД должен быть установлен системным администратором до начала установки ПК.

9.8.1 Установка СУБД MS SQL на ОС MS Windows

Установка и настройка СУБД описана на примере СУБД MS SQL Server 2016.

Порядок установки MS SQL Server 2016:

– установка Windows-компонента *«Функции .Net Framework 3.5»* (добавление и установка компонента в диспетчере сервера) (Рисунок 9.20);

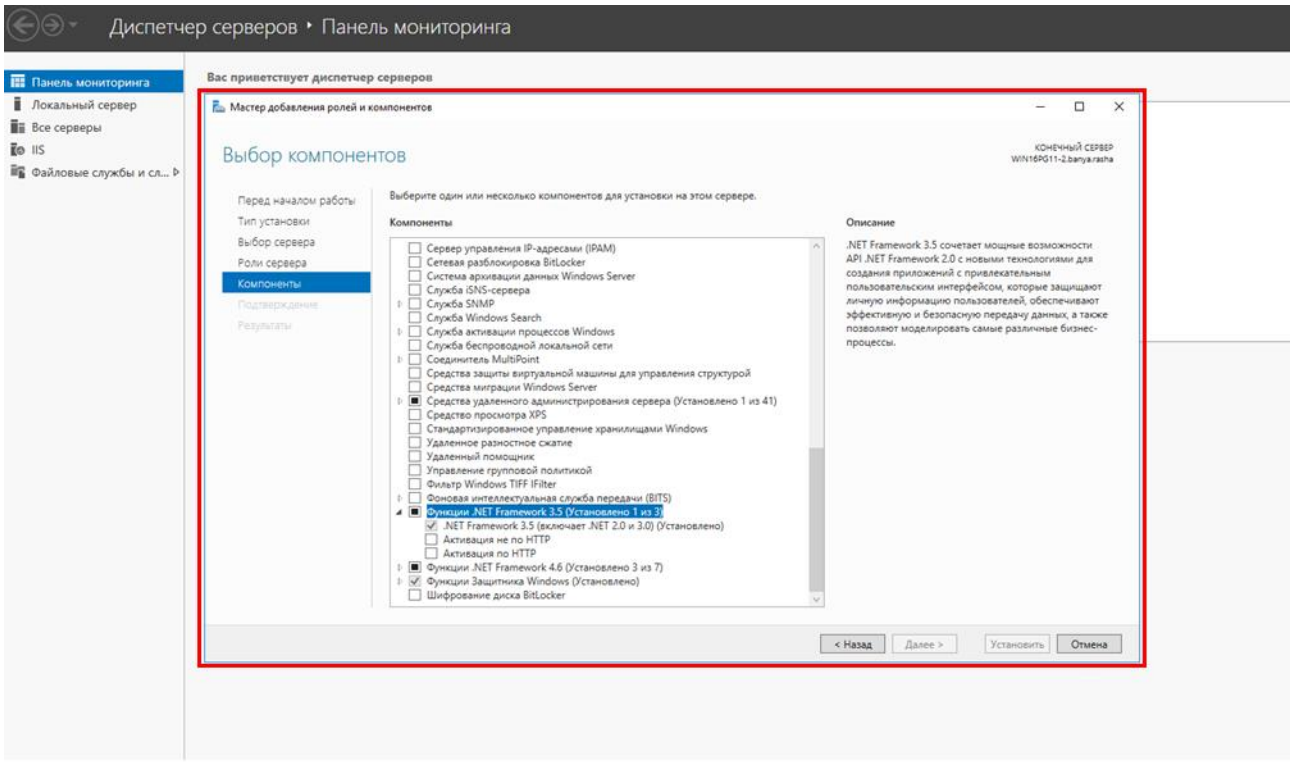

Рисунок 9.20 – Добавление компонента «Функции . Net Framework 3.5»

– установка СУБД MS SQL Server 2016;

– установка средства конфигурирования MS SQL Server Management Studio.

При установке сервера MS SQL Server необходимо указать для элемента *«Параметры сортировки» (Collation name)* значение «Cyrillic_General_CI_AS».

9.8.2 Настройка СУБД MS SQL на ОС MS Windows

После выполнения инсталляции СУБД необходимо выполнить дополнительные настройки на сервере.

Для изменения настроек необходимо:

1. Запустить утилиту *Диспетчер конфигурации SQL Server* из меню *«Пуск – Все программы – Microsoft SQL Server 2016 – Средства настройки – Диспетчер конфигурации»*.

2. Выбрать пункт «*Диспетчер конфигурации SQL Server*» и в появившемся окне настроить:

- для ветки Сетевая конфигурация SQL Server (SQL Server Network Configuration) – Протоколы для MSSQLSERVER (Protocols for MSSQLSERVER) разрешить использование протокола TCP/IP (Рисунок 9.21).

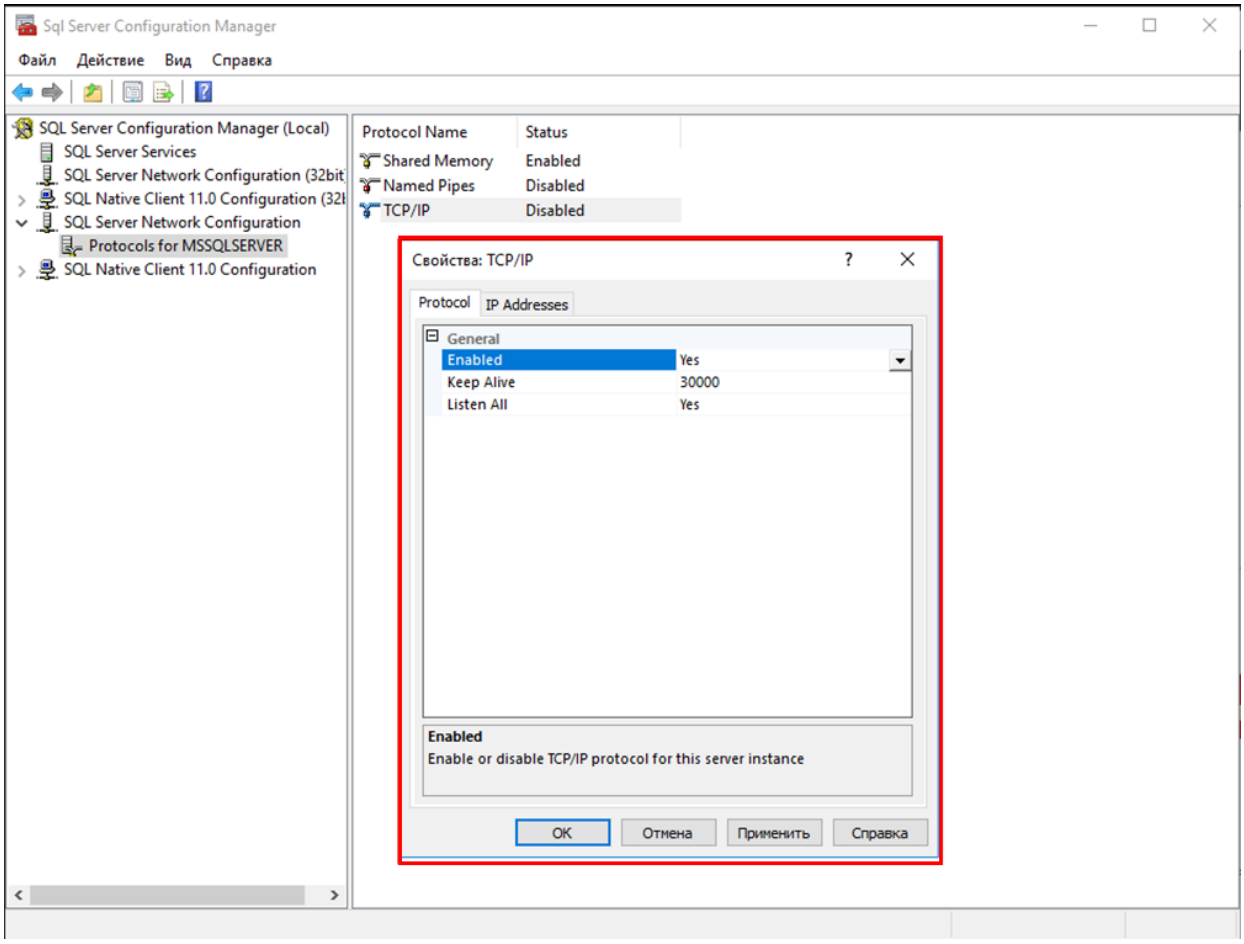

Рисунок 9.21 – Разрешение использования протокола TCP/IP

3. В случае если сервер приложения и СУБД MS SQL Server находятся на разных физических (виртуальных) серверах, то необходимо для ветки Службы SQL Server – SQL

Server Browser установить для параметра *«Режим запуска» (Start Mode)* значение *«Авто» (Automatic)* и нажать на кнопку *«Применить»* (Рисунок 9.22). Если сервер приложений и СУБД MS SQL Server установлены на одном физическом (виртуальном) сервере, то п.3 пропускается.

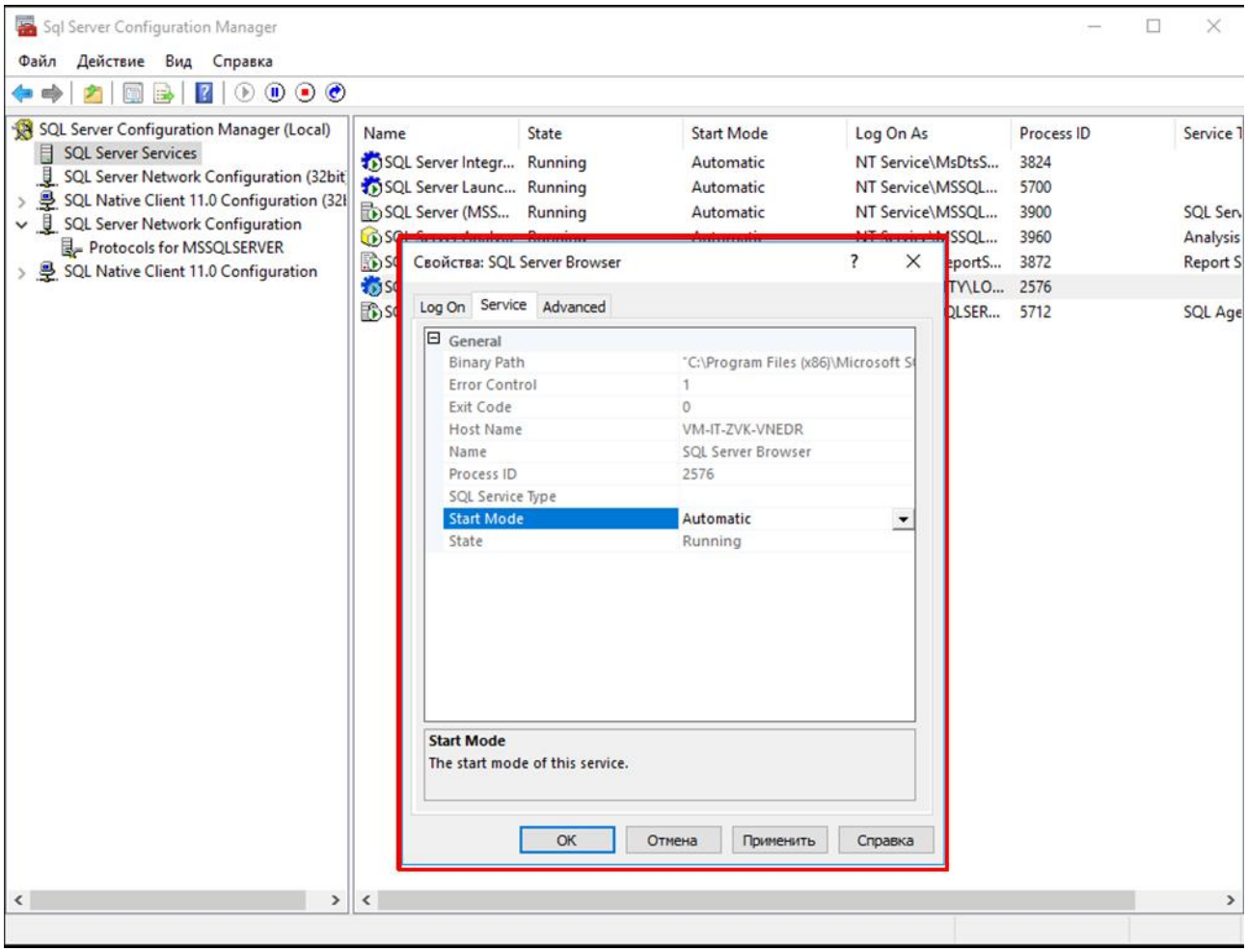

Рисунок 9.22 – Подключение службы «SQL Server Browser»

4. Для запуска службы «SQL Server Browser» перейти на вкладку *«Вход» (Log On)* и нажать на кнопку *«Пуск» (Start)*, затем кнопку *«ОК»* (Рисунок 9.23).

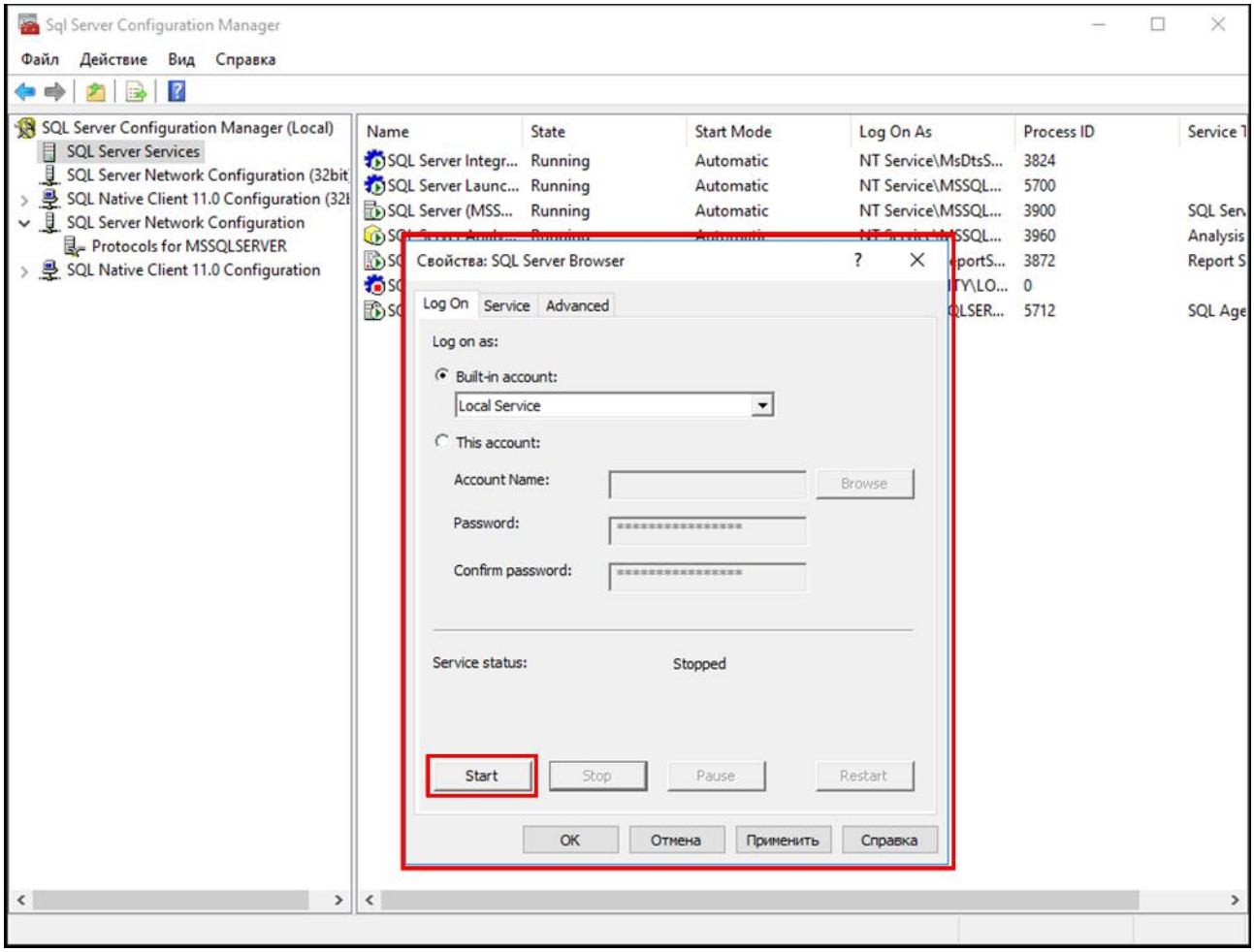

Рисунок 9.23 – Запуск службы «SQL Server Browser»

5. По умолчанию после инсталляции на SQL Server запрещено использование пользователей SQL. Для корректной работы ПК это ограничение необходимо убрать. Для этого нужно запустить среду SQL Server Management Studio. Подключиться к SQL Server и в окне свойств сервера (раздел *«Безопасность»*) выбрать пункт *«Проверка подлинности SQL Server и Windows»* (Рисунок 9.24).

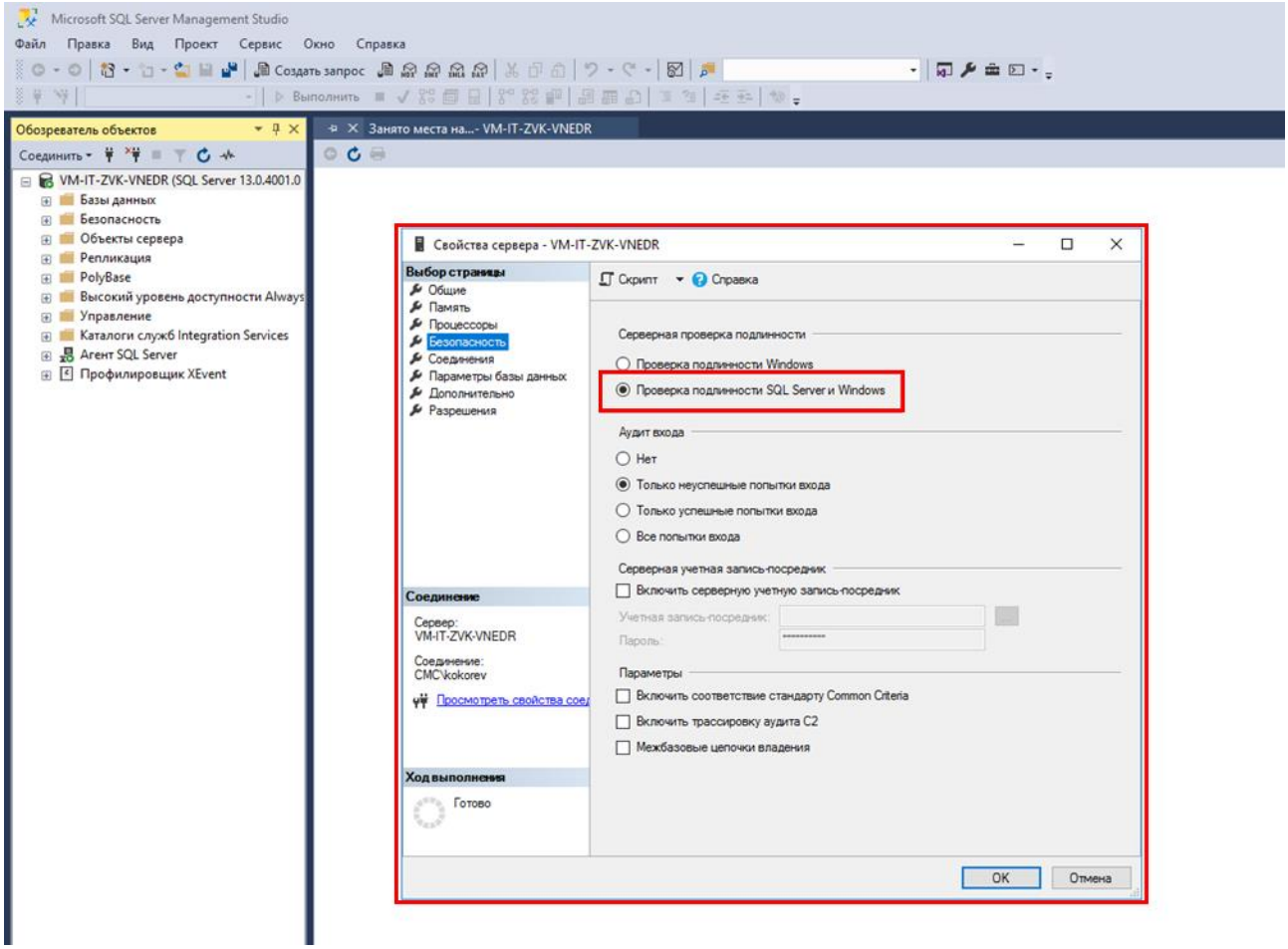

Рисунок 9.24 – Установка разрешения использования проверки подлинности SQL

6. Нажать на кнопку *«ОК»* и перезагрузить сервер.

Внимание! При использовании СУБД MS SQL 2016 / 2019 должен быть обязательно дополнительно установлен SQL Native Client 2016 (версия клиента 10.x).

Проверить наличие Native Client на рабочей станции можно, открыв список программ и компонентов (*«Пуск – Панель управления – Все элементы панели управления – Программы и компоненты»*) или введя в командной строке «appwiz.cpl» (Рисунок 9.25).

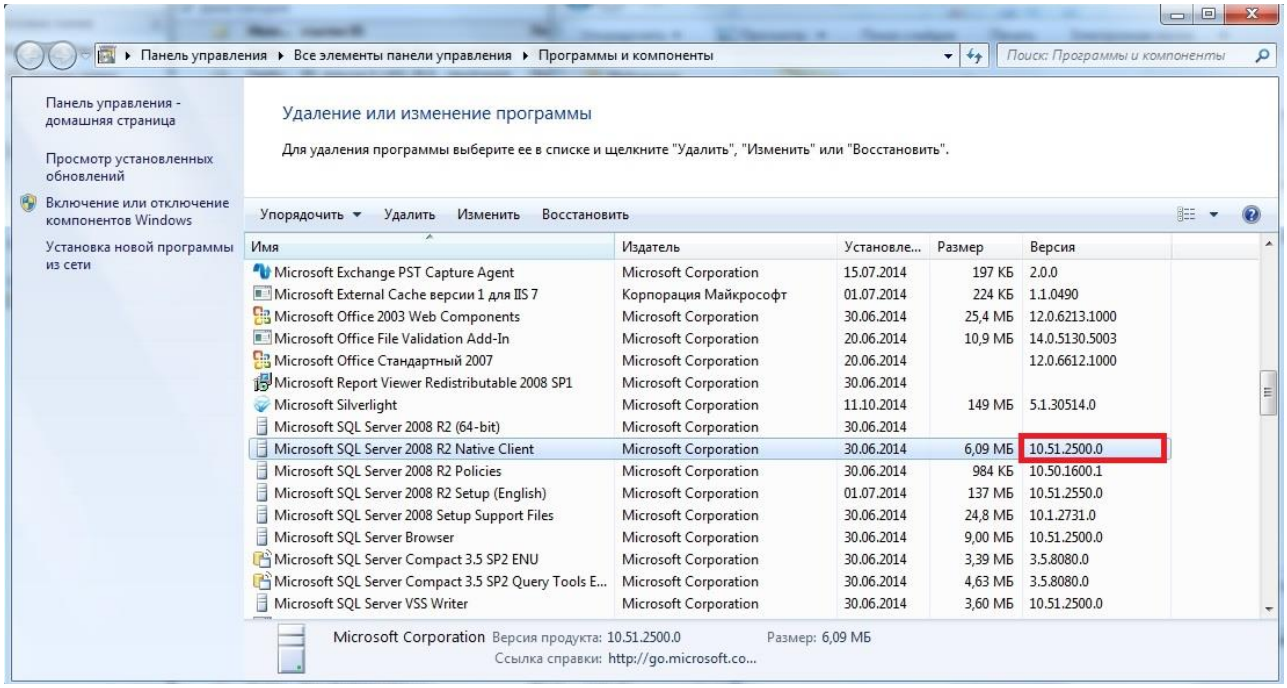

Рисунок 9.25 – Проверка наличия и версионности Native Client

Если установлен Native Client другой версии, необходимо установить ещё и версию 10. Скачать Native Client 10 можно на сайте производителя – компании Microsoft.

При установке Native Client Setup в окне выбора устанавливаемых функций выбрать Client Components (Рисунок 9.26).

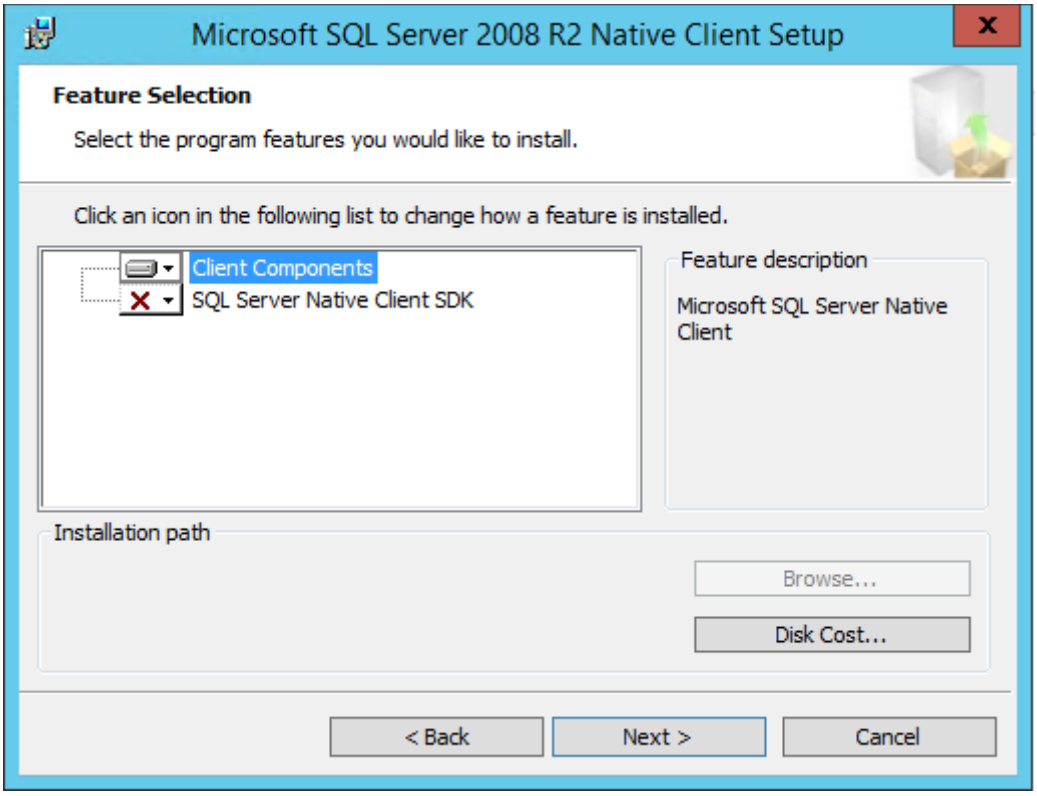

Рисунок 9.26 – Окно выбора устанавливаемых функций Native Client

9.8.3 Установка СУБД PostgreSQL на ОС MS Windows

Для создания учетной записи пользователя PostgreSQL, от имени которой ПК работает с БД, необходимо выполнить следующие действия:

1. Открыть файл *«postgresql-15.7-2-windows-x64.exe»* двойным нажатием правой кнопки мыши.

2. В окне Мастера установки нажать кнопку *«Next >»* (Рисунок 9.27).

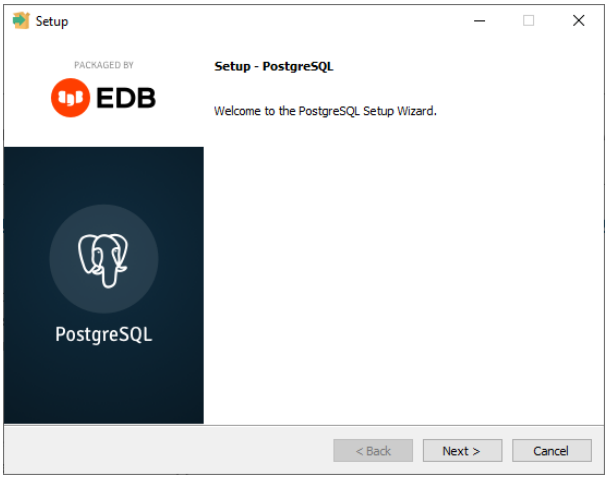

Рисунок 9.27 – Мастер установки

3. При установке PostgreSQL предоставляется возможность выбора директории установки (по умолчанию предлагается директория «C:\Program File\PostgreSQL\15») (Рисунок 9.28).

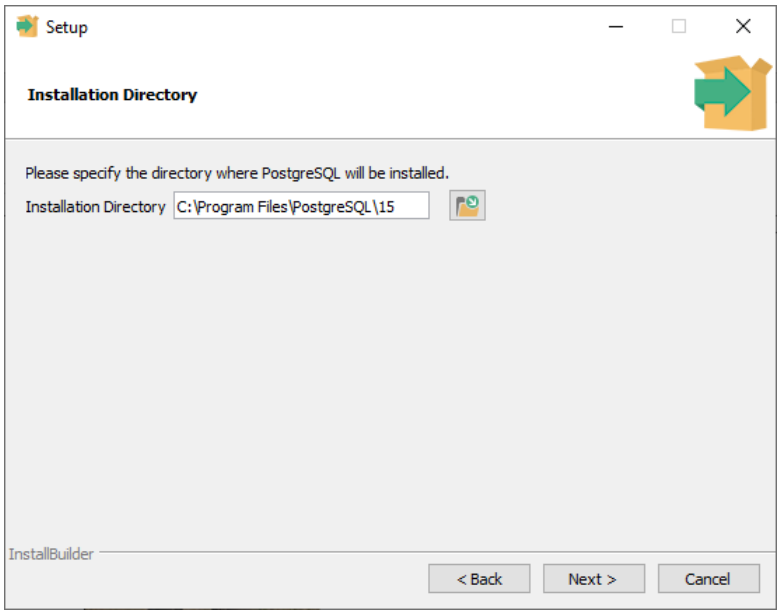

Рисунок 9.28 – Выбор папки установки

4. В окне «Select Components» выбрать необходимые компоненты для установки (Рисунок 9.29).

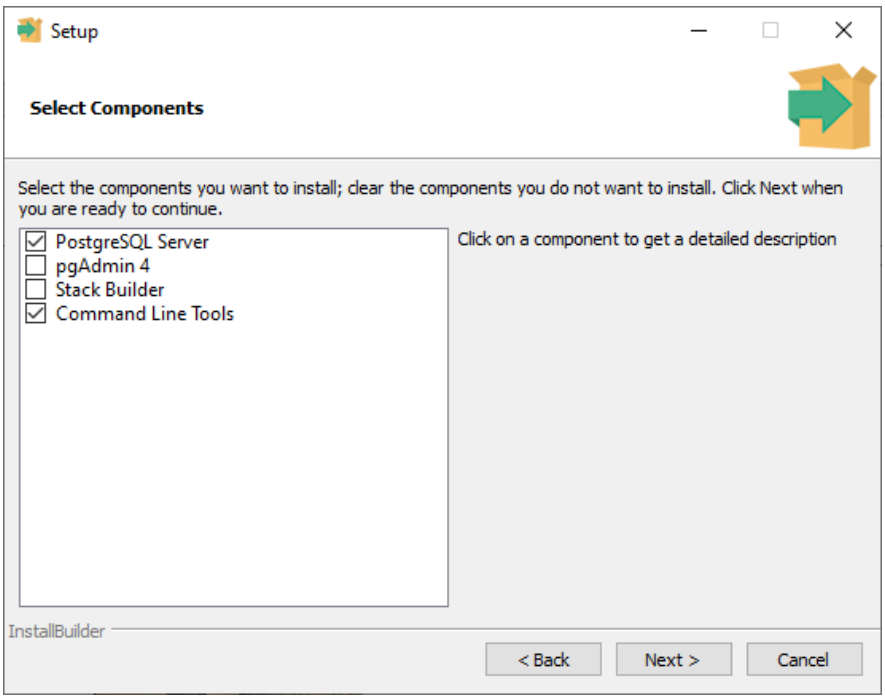

Рисунок 9.29 – Компоненты устанавливаемой программы

5. Выбор каталога данных (Рисунок 9.30).

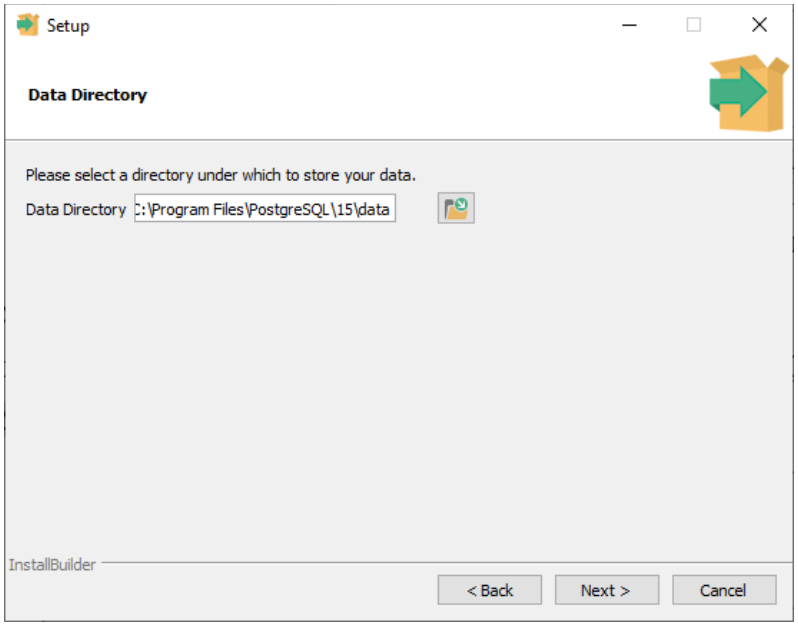

Рисунок 9.30 – Выбор каталога данных

6. На следующих шагах задаются параметры сервера (Рисунок 9.31, Рисунок 9.32, Рисунок 9.33).

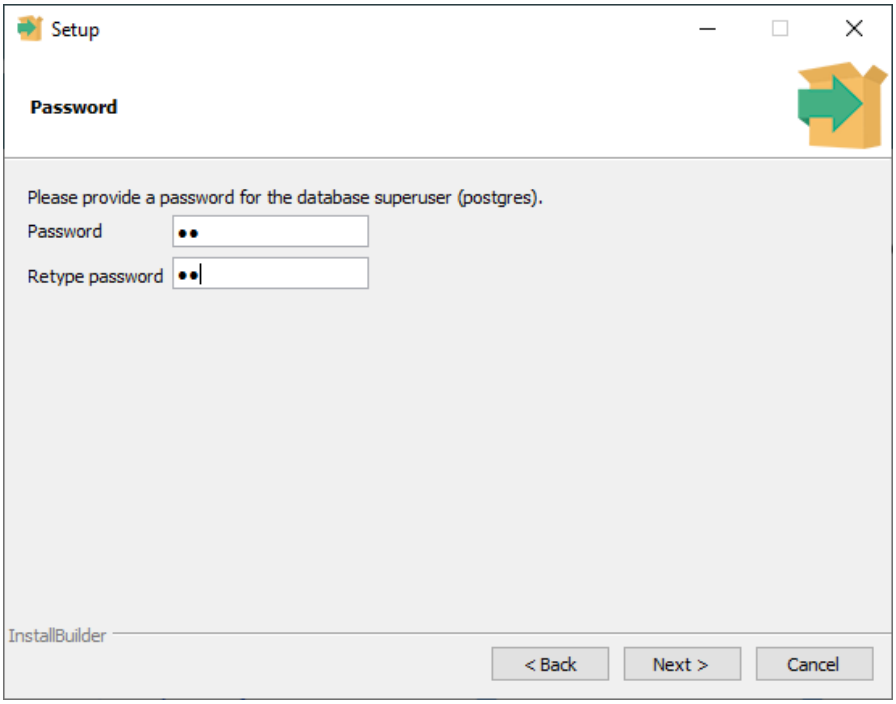

Рисунок 9.31 – Пароль суперпользователя базы данных

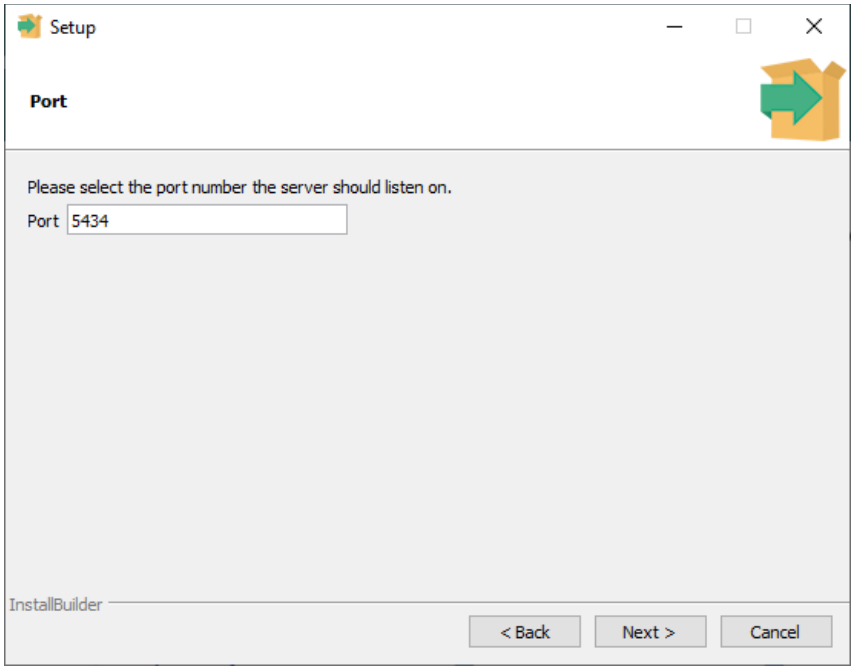

Рисунок 9.32 – Номер порта

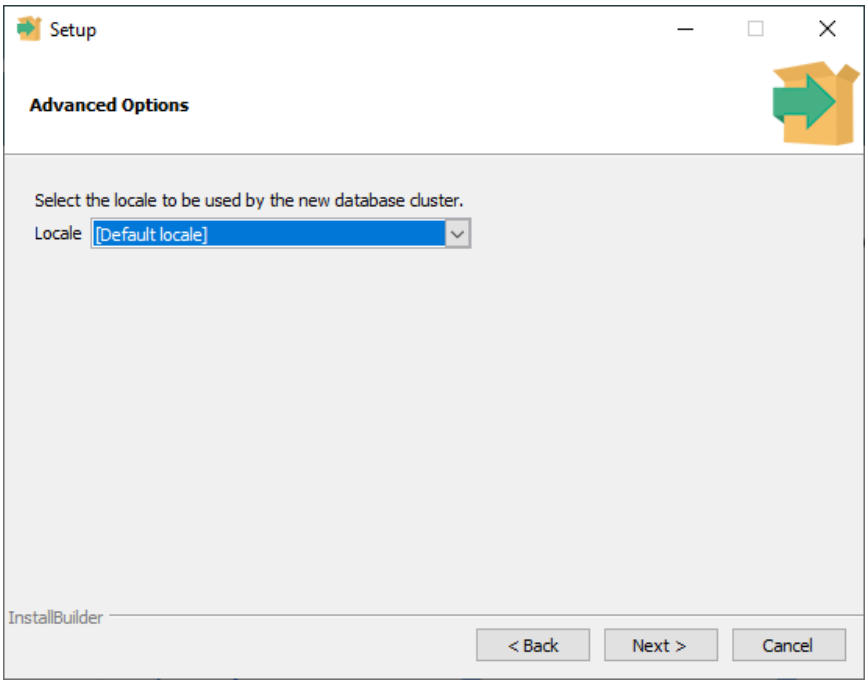

Рисунок 9.33 – Locale

7. На следующем шаге в окне мастера отображается вся информация, полученная программой установки (Рисунок 9.34).

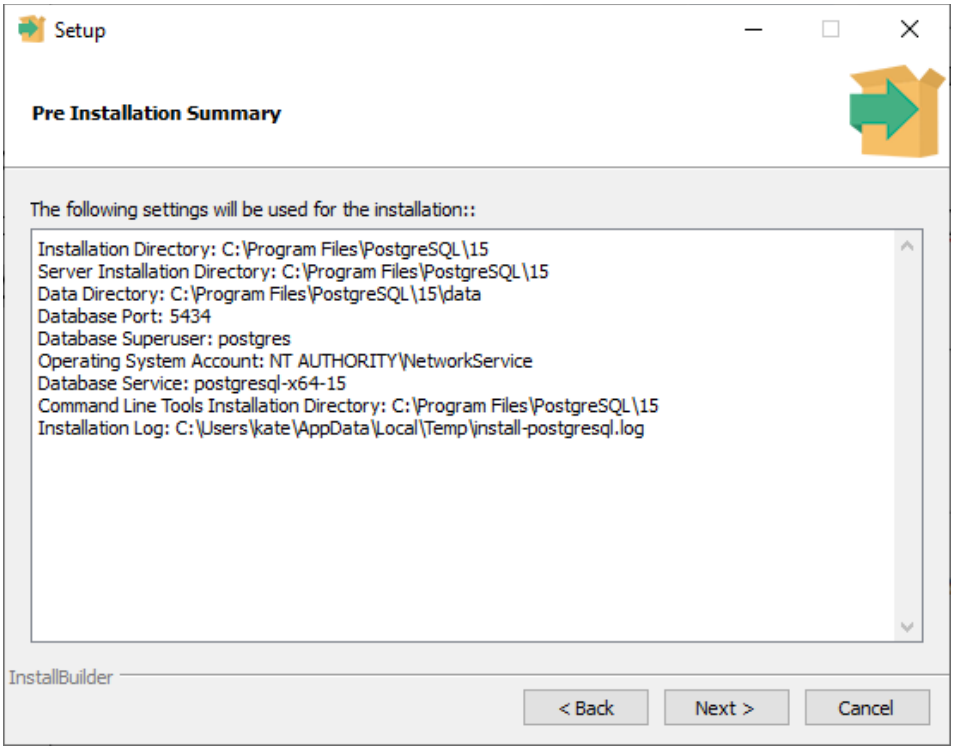

Рисунок 9.34 – Завершений сбора информации

8. На следующем шаге в окне мастера отображается информация о готовности к установке PostgreSQL (Рисунок 9.35).

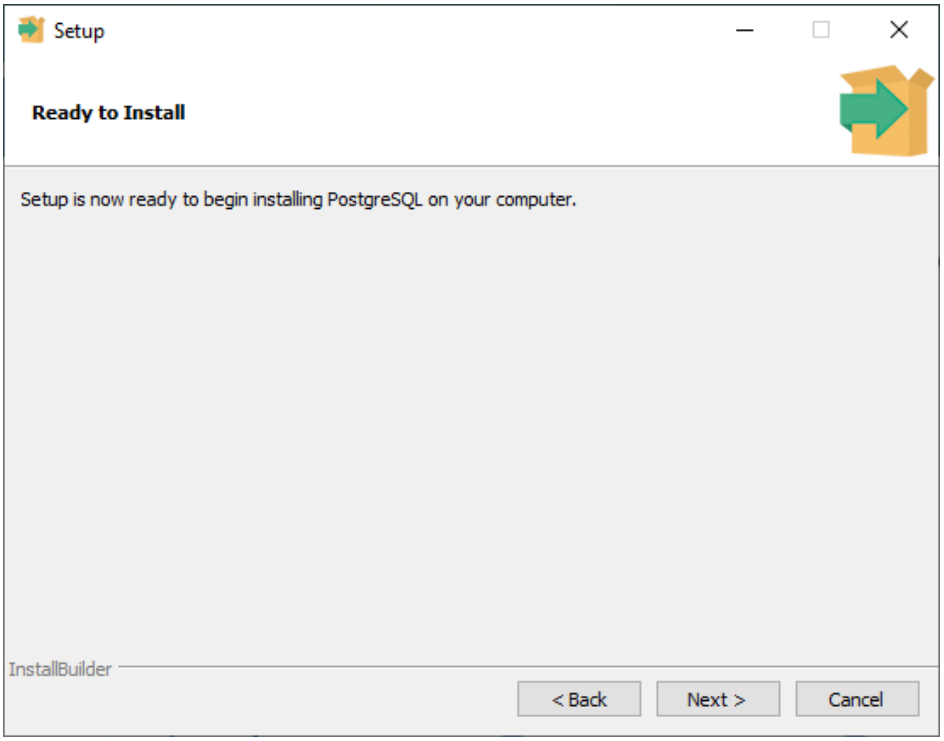

Рисунок 9.35 – Готовность к установке PostgreSQL

9. Последним этапом является процесс копирования файлов (Рисунок 9.36).

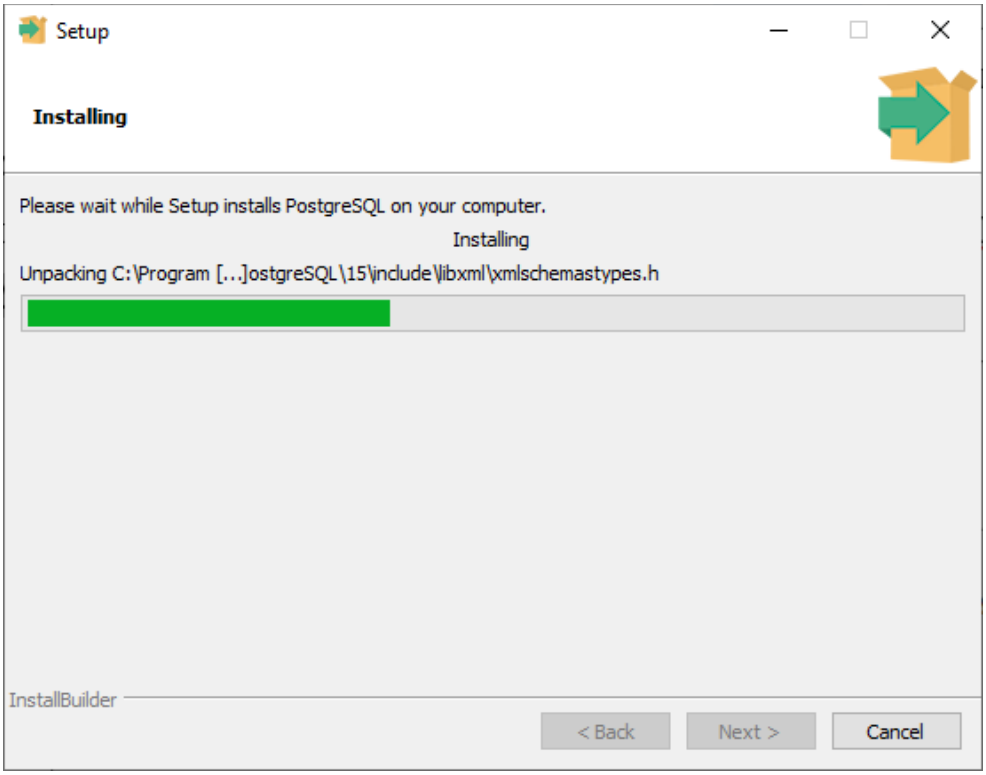

Рисунок 9.36 – Процесс копирования файлов

10. По окончанию процесса установки появляется окно завершения установки (Рисунок 9.37).

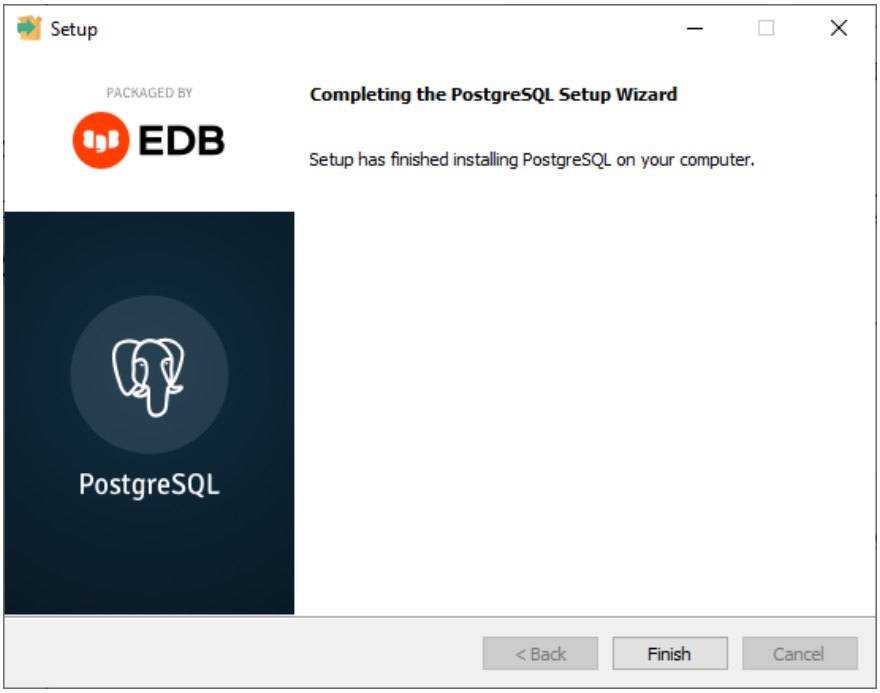

Рисунок 9.37 – Окно завершения установки

9.9 Установка и настройка СУБД на ОС семейства Linux

9.9.1 Установка СУБД PostgreSQL

Для создания учетной записи пользователя PostgreSQL, от имени которой ПК работает с БД, необходимо выполнить следующие действия:

1. Открыть файл *«postgresql-15.7-2-windows-x64.exe»* двойным нажатием правой кнопки мыши.

2. В окне Мастера установки нажать кнопку *«Next >»* (Рисунок 9.27).

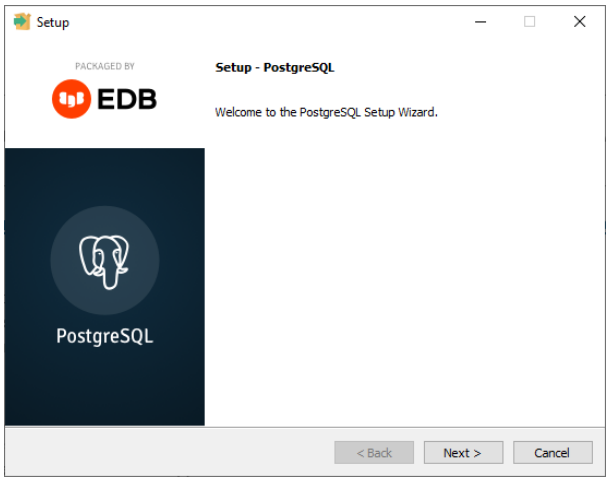

Рисунок 9.38 – Мастер установки

3. При установке PostgreSQL предоставляется возможность выбора директории установки (по умолчанию предлагается директория «C:\Program File\PostgreSQL\15») (Рисунок 9.28).

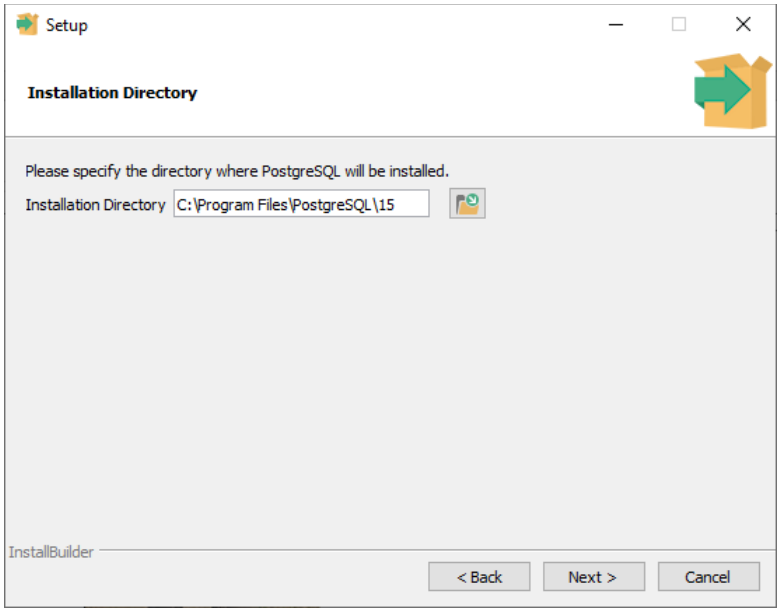

Рисунок 9.39 – Выбор папки установки

4. В окне «Select Components» выбрать необходимые компоненты для установки (Рисунок 9.29).

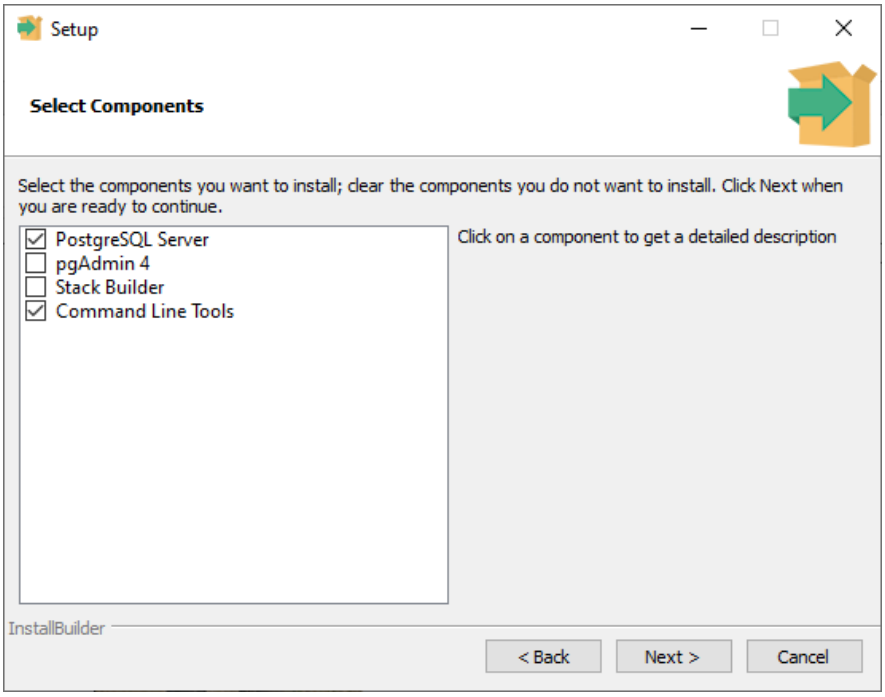

Рисунок 9.40 – Компоненты устанавливаемой программы

5. Выбор каталога данных (Рисунок 9.30).

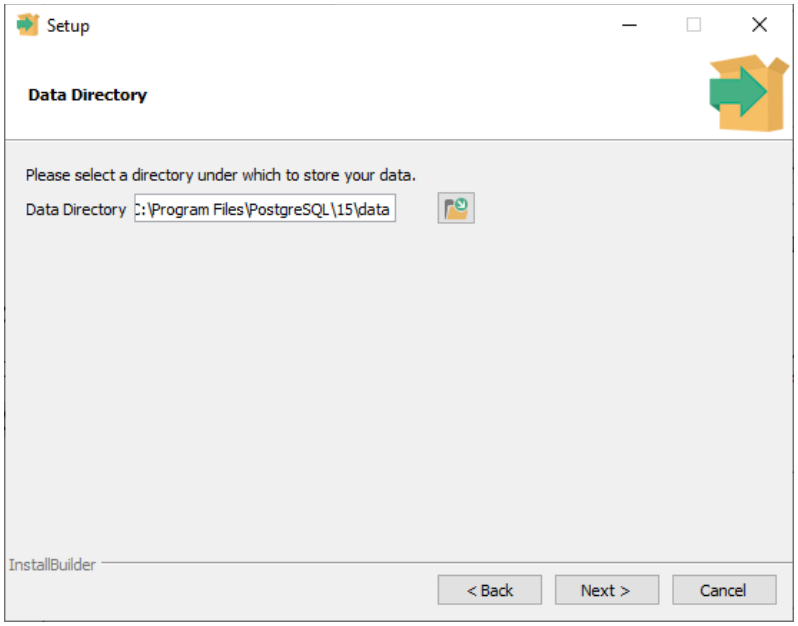

Рисунок 9.41 – Выбор каталога данных

6. На следующих шагах задаются параметры сервера (Рисунок 9.31, Рисунок 9.32, Рисунок 9.33).

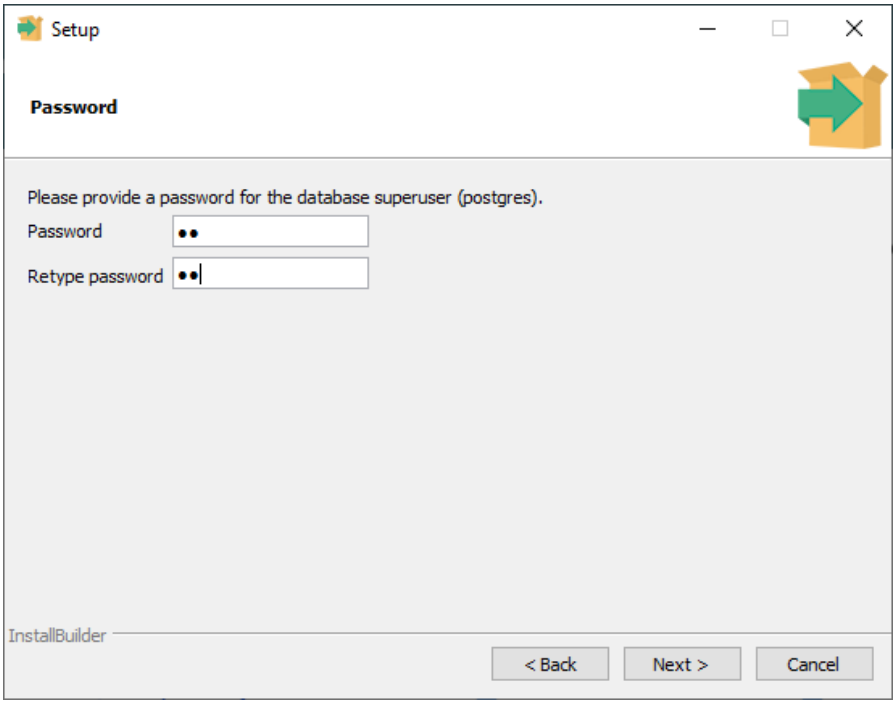

Рисунок 9.42 – Пароль суперпользователя базы данных

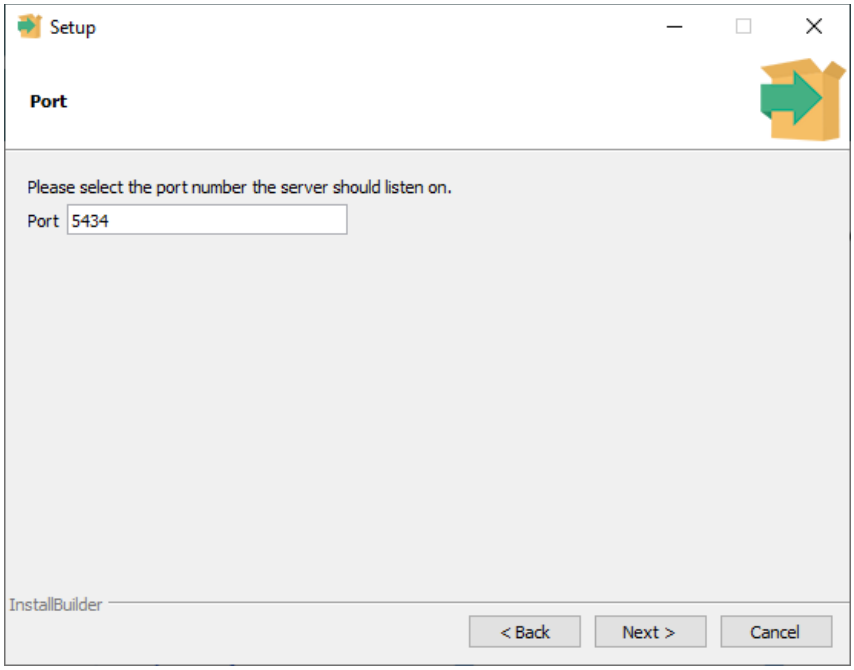

Рисунок 9.43 – Номер порта

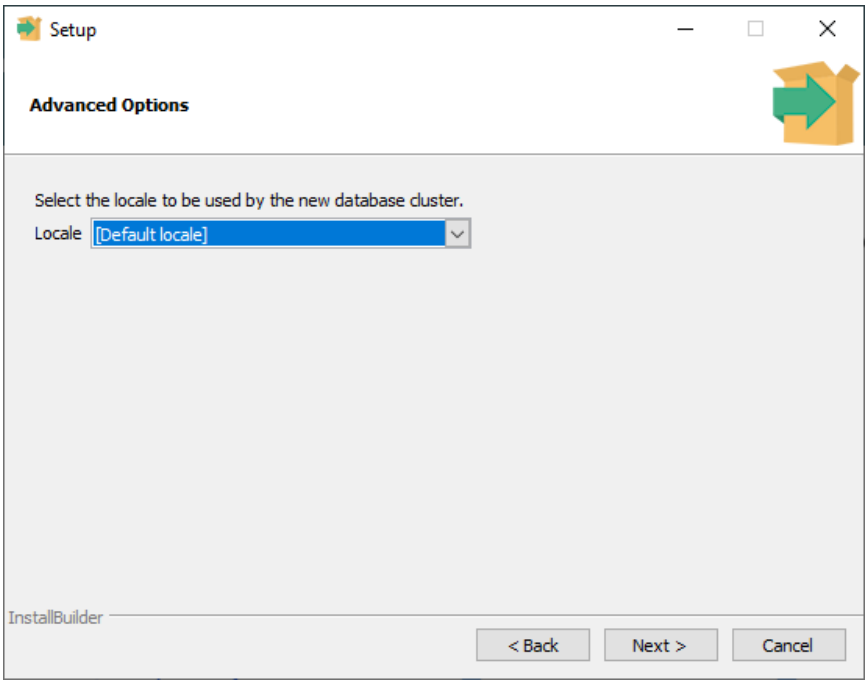

Рисунок 9.44 – Locale

7. На следующем шаге в окне мастера отображается вся информация, полученная программой установки (Рисунок 9.34).

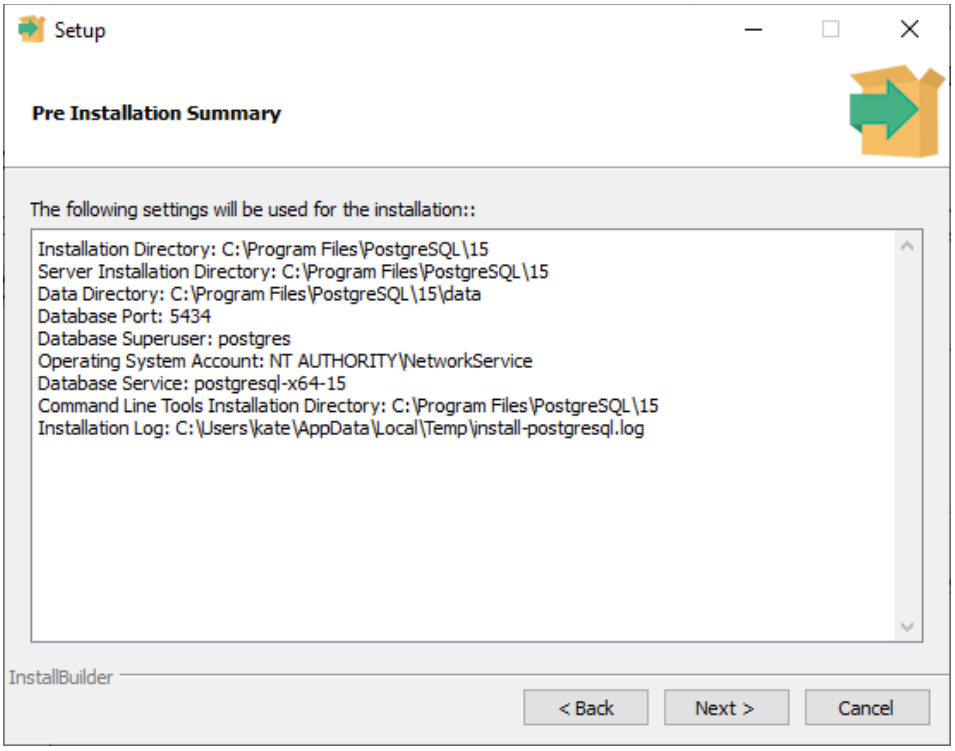

Рисунок 9.45 – Завершений сбора информации

8. На следующем шаге в окне мастера отображается информация о готовности к установке PostgreSQL (Рисунок 9.35).

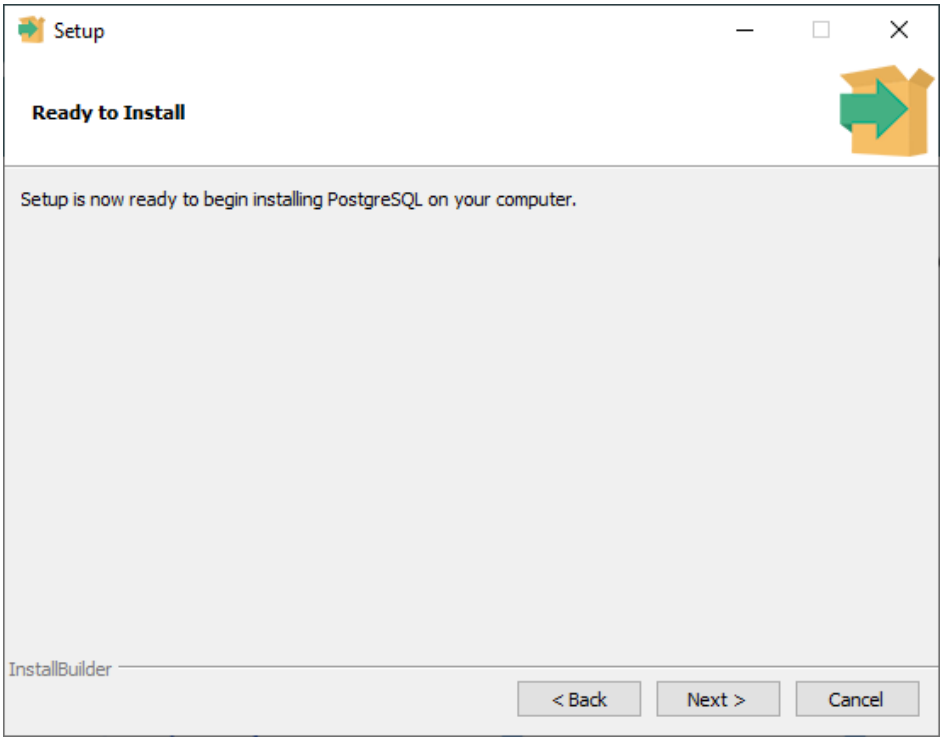

Рисунок 9.46 – Готовность к установке PostgreSQL

9. Последним этапом является процесс копирования файлов (Рисунок 9.36).

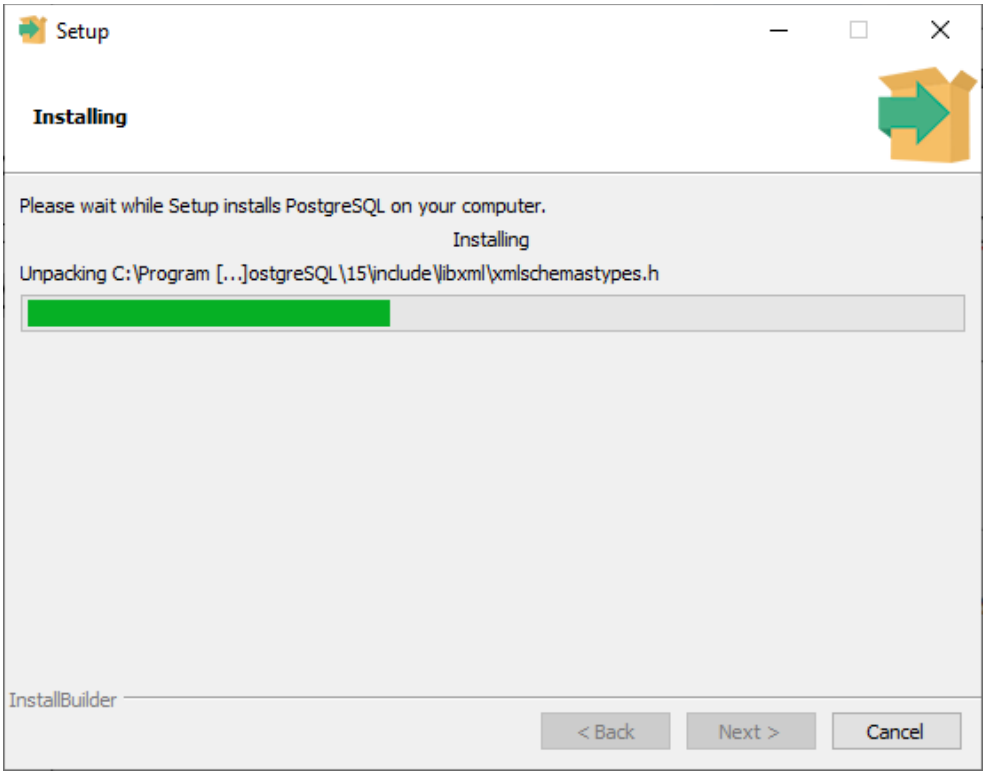

Рисунок 9.47 – Процесс копирования файлов

10. По окончанию процесса установки появляется окно завершения установки (Рисунок 9.37).

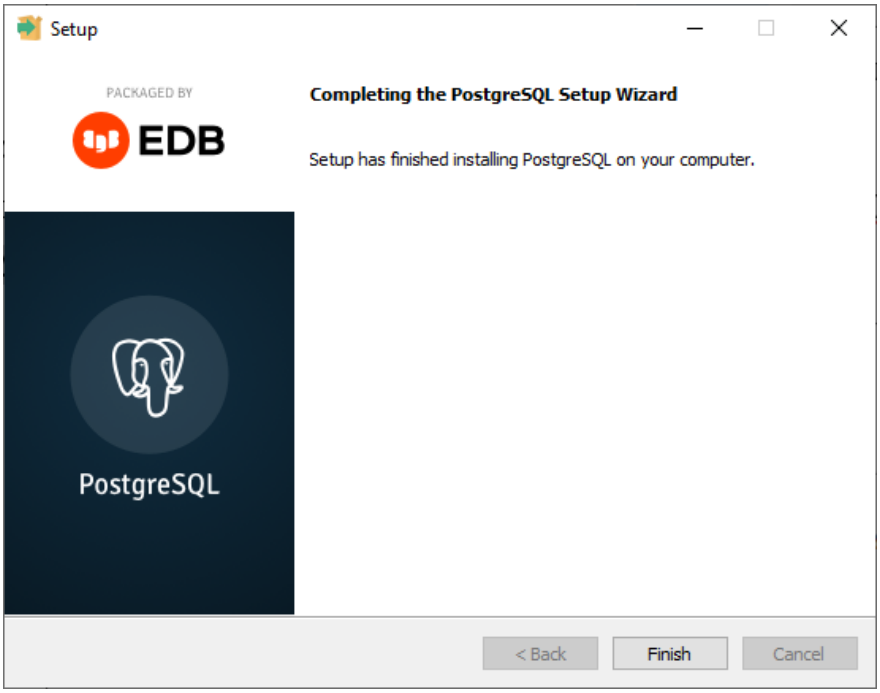

Рисунок 9.48 – Окно завершения установки

9.9.2 Установка СУБД на ОС семейства Linux

Для хранения данных в ПК «АСУРЭО» на ОС семейства Linux используется СУБД Postgres Pro. Для установки СУБД Postgres Pro необходимо выполнить следующие действия:

1. С помощью утилиты wget необходимо скачать скрипт sh добавления репозитория Postgres Pro в файл «sources.list».

   Выполнить команду: *wget - -http-user=user - -http-password=password* https://repoee.postgrespro.ru/pgproee-15/keys/pgpro-repo-add.sh (Рисунок 9.49).

```
root@astral:/opt/nginx# wget --http-user=user  --http-password=password  https:/
/repoee.postgrespro.ru/pgproee-15/keys/pgpro-repo-add.sh
--2022-10-03 15:43:18--  https://repoee.postgrespro.ru/pgproee-15/keys/pgpro-rep
o-add.sh
Распознаётся repoee.postgrespro.ru (repoee.postgrespro.ru)… 213.171.56.11
Подключение к repoee.postgrespro.ru (repoee.postgrespro.ru)|213.171.56.11|:443..
. соединение установлено.
HTTP-запрос отправлен. Ожидание ответа… 401 Unauthorized
Выбранная аутентификация: Basic realm="Restricted"
Повторное использование соединения с repoee.postgrespro.ru:443.
HTTP-запрос отправлен. Ожидание ответа… 200 OK
Длина: 16194 (16K) [application/octet-stream]
Сохранение в: «pgpro-repo-add.sh»

pgpro-repo-add.sh   100%[===================>]  15,81K  --.-KB/s    за 0,02s

2022-10-03 15:43:23 (883 KB/s) - «pgpro-repo-add.sh» сохранён [16194/16194]
```

Рисунок 9.49 – Выполнение команды wget - -http-user=user - -http-password=password https://repoee.postgrespro.ru/pgproee-15/keys/pgpro-repo-add.sh

   При этом в параметрах –http-user и –http-Password необходимо указать учётные данные полученные при приобретении лицензии Postgres Pro.

2. Запустить на выполнение скрипт добавления репозитория Postgres PRO.

   Выполнить команду: *sh pgpro-repo-add.sh* (Рисунок 9.50).

```
root@astral:/opt/nginx# sh pgpro-repo-add.sh
--2022-10-03 15:49:16--  https://repoee.postgrespro.ru/pgproee-15/astra-smolensk
/1.7/dists/1.7_x86-64/main/binary-amd64/Release
Распознаётся repoee.postgrespro.ru (repoee.postgrespro.ru)… 213.171.56.11
Подключение к repoee.postgrespro.ru (repoee.postgrespro.ru)|213.171.56.11|:443..
. соединение установлено.
HTTP-запрос отправлен. Ожидание ответа… 401 Unauthorized

Ошибка аутентификации пользователя/пароля.
Repository https://repoee.postgrespro.ru/pgproee-15 is password protected
Please enter your username: sms-a
Please enter your password (wouldn't be echoed):
--2022-10-03 15:49:36--  https://repoee.postgrespro.ru/pgproee-15/astra-smolensk
/1.7/dists/1.7_x86-64/main/binary-amd64/Release
Распознаётся repoee.postgrespro.ru (repoee.postgrespro.ru)… 213.171.56.11
Подключение к repoee.postgrespro.ru (repoee.postgrespro.ru)|213.171.56.11|:443..
. соединение установлено.
HTTP-запрос отправлен. Ожидание ответа… 401 Unauthorized
Выбранная аутентификация: Basic realm="Restricted"
Повторное использование соединения с repoee.postgrespro.ru:443.
HTTP-запрос отправлен. Ожидание ответа… 200 OK
Длина: 136 [application/octet-stream]
Сохранение в: «STDOUT»

-                   100%[===================>]     136  --.-KB/s    за 0s

/2022-10-03 15:49:37 (324 MB/s) - записан в stdout [136/136]

Your username/password are saved to /etc/apt/auth.conf.d/repoee.postgrespro.ru.c
onf
Игн:1 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 DVD  1.7_x86-64 InRelease
Ошб:2 cdrom://OS Astra Linux 1.7.0 1.7_x86-64 DVD  1.7_x86-64 Release
  Используйте apt-cdrom, чтобы APT смог распознать данный CD-ROM. apt-get update
 не используется для добавления новых CD-ROM
Пол:3 https://repoee.postgrespro.ru/pgproee-15/astra-smolensk/1.7 1.7_x86-64 InR
```

Рисунок 9.50 – Выполнение команды sh pgpro-repo-add.sh

При выполнении команды необходимо авторизоваться учётной записью полученной при приобретении лицензии Postgres PRO.

3. Открыть на изменение файл pgprooee-15.list расположенный по пути /etc/apt/sources.list.d и в явном виде указать учётные данные подключения к репозиторию (Рисунок 9.51).

```
  GNU nano 3.2              /etc/apt/sources.list.d/pgproee-15.list              Изменён

# Repositiory for 'PostgresPro Enterprise'
deb https://YOURLOGIN:YOURPASS@repoee.postgrespro.ru/pgproee-12/astra-smolensk/1.7 1.7_x8$
```

Рисунок 9.51 – Указание учетных данных подключения к репозиторию

4. Запустить установку СУБД postgrespro-ent-15.

   Выполнить команду: *apt-get install postgrespro-ent-15* (Рисунок 9.52).

```
root@astral:/opt/nginx# apt-get install postgrespro-ent-15
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  libbasicusageenvironment1 libfam0 libgroupsock8 libkdecorations2private7
  liblivemedia64 libusageenvironment3 tini
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  libzstd1 postgrespro-ent-15-client postgrespro-ent-15-contrib
  postgrespro-ent-15-libs postgrespro-ent-15-server
Предлагаемые пакеты:
  postgrespro-ent-15-docs postgrespro-ent-15-docs-ru libdbd-pg-perl oidentd
  | ident-server locales-all
Следующие НОВЫЕ пакеты будут установлены:
  postgrespro-ent-15 postgrespro-ent-15-client postgrespro-ent-15-contrib
  postgrespro-ent-15-libs postgrespro-ent-15-server
Следующие пакеты будут обновлены:
  libzstd1
Обновлено 1 пакетов, установлено 5 новых пакетов, для удаления отмечено 0 пакетс
в, и 634 пакетов не обновлено.
Необходимо скачать 10,6 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 45,9 MB
.
W: Цель Packages (main/binary-amd64/Packages) настроена несколько раз: в /etc/ap
t/sources.list:6 и в /etc/apt/sources.list:7
W: Цель Packages (main/binary-all/Packages) настроена несколько раз: в /etc/apt/
sources.list:6 и в /etc/apt/sources.list:7
```

Рисунок 9.52 – Выполнение команды apt-get install postgrespro-ent-15

При окончании установки также в автоматическом режиме будет произведена инициализация базы данных (Рисунок 9.53).

```
update-alternatives: используется /opt/pgpro/ent-15/man/ru/man1/vacuumdb.1.gz дл
я предоставления /usr/share/man/ru/man1/vacuumdb.1.gz (pgsql-vacuumdbmanru) в ав
томатическом режиме
update-alternatives: используется /opt/pgpro/ent-15/man/ru/man1/vacuumlo.1.gz дл
я предоставления /usr/share/man/ru/man1/vacuumlo.1.gz (pgsql-vacuumlomanru) в ав
томатическом режиме
Updating /etc/manpath.config
Initalizing database...
OK
Synchronizing state of postgrespro-ent-15.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgrespro-ent-15
Created symlink /etc/systemd/system/multi-user.target.wants/postgrespro-ent-15.s
ervice → /lib/systemd/system/postgrespro-ent-15.service.
Обрабатываются триггеры для systemd (241-7~deb10u8astra.se24) …
Обрабатываются триггеры для libc-bin (2.28-10+ci202012301235+astra1) …
```

Рисунок 9.53 – Инициализация базы данных

5. Проверить, что СУБД в активном режиме.

   Выполнить команду: *systemctl status postgrespro-ent-15.service* (Рисунок 9.54).

```
root@astral:/opt/nginx# systemctl status postgrespro-ent-15.service
● postgrespro-ent-15.service - Postgres Pro ent 15 database server
   Loaded: loaded (/lib/systemd/system/postgrespro-ent-15.service; enabled; vend
   Active: active (running) since Mon 2022-10-03 15:57:37 +04; 3min 9s ago
 Main PID: 15215 (postgres)
    Tasks: 9 (limit: 4527)
   Memory: 55.6M
   CGroup: /system.slice/postgrespro-ent-15.service
           ├─15215 /opt/pgpro/ent-15/bin/postgres -D /var/lib/pgpro/ent-15/data
           ├─15217 postgres: logger
           ├─15219 postgres: checkpointer
           ├─15220 postgres: background writer
           ├─15221 postgres: walwriter
           ├─15222 postgres: autovacuum launcher
           ├─15223 postgres: stats collector
           ├─15224 postgres: logical replication launcher
           └─15225 postgres: cfs-worker-0
```

Рисунок 9.54 – Выполнение команды systemctl status postgrespro-ent-15.service

6. Для установки пароля системной учётной записи «postgres» необходимо:

   6.1 Перейти на учётную запись postgres и войти в консоль psql.

   Выполнить команду: *su postgres* (Рисунок 9.55).

```
root@astral:/opt/nginx# su postgres
postgres@astral:/opt/nginx$ psql
psql (15.7 )
Введите "help", чтобы получить справку.

postgres=#
```

Рисунок 9.55 – Выполнение команды su postgres

6.2 Задать пароль.

Выполнить команду: *ALTER USER postgres WITH PASSWORD 'SecretPass'* (Рисунок 9.56).

```
postgres=# ALTER USER postgres WITH PASSWORD 'SecretPass';
ALTER ROLE
```

Рисунок 9.56 – Выполнение команды ALTER USER postgres WITH PASSWORD 'SecretPass'

9.9.3 Настройка СУБД на ОС семейства Linux

Если сервер приложений расположен не на той же самой машине, что и Postgres PRO, то требуется разрешить принимать подключения с другого сервера. По умолчанию, Postgres PRO в целях безопасности принимает только локальные подключения. Чтобы разрешить принимать подключения извне, необходимо:

1. В основном файле конфигурации «*postgresql.conf*», который расположен по пути /var/lib/pgpro/ent-15/data установить следующий параметр: *Listen_addresses = '*'* (Рисунок 9.57).

```
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for all
                                        # (change requires restart)
#port = 5432                            # (change requires restart)
max_connections = 100                   # (change requires restart)
#superuser_reserved_connections = 3     # (change requires restart)
#unix_socket_directories = '/tmp'       # comma-separated list of directories
                                        # (change requires restart)
```

Рисунок 9.57 – Установка параметра Listen_addresses = '*'

Обратите внимание, что необходимо в файле конфигурации «*postgresql.conf*» оставить параметр standard_conforming_strings закомментированным или выставить в значение on (standard_conforming_strings = on), как представлено на рисунке 9.58.

```
#------------------------------------------------------------------------------
# VERSION AND PLATFORM COMPATIBILITY
#------------------------------------------------------------------------------

# - Previous PostgreSQL Versions -

#array_nulls = on
#backslash_quote = safe_encoding        # on, off, or safe_encoding
#escape_string_warning = on
#lo_compat_privileges = off
#quote_all_identifiers = off
#standard_conforming_strings = on
#synchronize_seqscans = on

# - Other Platforms and Clients -

#transform_null_equals = off
```

Рисунок 9.58 – Установка параметра standard_conforming_strings = on

2. В файле настроек доступа *«pg_hba.conf»* указать IP, с которых можно принимать подключения, а именно адрес сервера приложений (Рисунок 9.59).

```
  GNU nano 3.2              /var/lib/pgpro/ent-15/data/pg_hba.conf              Изменён

# IPv4 local connections:
host    all             all             192.168.35.74/32          md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```

Рисунок 9.59 – Указание IP

3. Перезапустить сервис postgrespro-ent-15.service.

Выполнить команду: *systemctl restart postgrespro-ent-15.service* (Рисунок 9.60).

```
root@astral:/opt/nginx# systemctl restart postgrespro-ent-15.service
root@astral:/opt/nginx#
```

Рисунок 9.60 – Выполнение команды systemctl restart postgrespro-ent-15.service

9.10 Установка и настройка etcd на ОС MS Windows

Для установки etcd на ОС MS Windows можно воспользоваться следующим способом:

1. Скачать последнюю версию etcd для ОС MS Windows с сайта https://github.com/etcd-io/etcd, перейти в раздел с дистрибутивами для ОС MS Windows – https://github.com/etcd-io/etcd/releases/tag/v3.5.15. В разделе assets найти архив «etcd-v3.5.15-windows-amd64.zip».

2. Распаковать архив в директорию на диск, например, c:\etcd. Можно убедиться, что etcd работает, для этого нужно запустить Powershell, перейти в директорию установки, например, *cd c:\etcd* и выполнить команду: *\etcd*

   После успешного запуска etcd в консоли будет запись об этом. Лучшая проверка: настроить интеграцию в приложениях ЗРП.Delphi и ЗРП.Net и из интерфейса администратора ЗРП.Delphi отправить оповещения всем пользователям, убедиться, что они есть в веб-версии.

3. После успешного запуска etcd необходимо настроить etcd как службу в системе, для того чтобы при перезапуске не пришлось заново запускать службу.

   Для этого необходимо скачать приложение nssm.exe (https://nssm.cc/download):

   – Распаковать приложение, например, в папку C:\nssm

   – Открыть Powershell и перейти в папку с дистрибутивом:

     cd C:\nssm

   – Выполнить команду:

     .\nssm.exe install etcd

     Где etcd – имя устанавливаемой службы.

   – Далее запустится GUI nssm, с помощью него можно настроить службу, указать путь к исполнимому файлу, в текущем примере «c:\etcd\etcd.exe». Остальные параметры оставить без изменений.

   – Запустить службу, убедиться в её работоспособности.

9.11 Установка etcd на ОС Linux

Установка etcd на Astra Linux подразумевает выполнение нескольких основных шагов.

Etcd – это высоконадежное, распределенное хранилище ключ-значение, предназначенное для хранения данных конфигурации, которые могут быть автоматически обновлены и синхронизированы между несколькими серверами. Вот шаги, которые необходимо выполнить для установки etcd на Astra Linux:

1. Для установки etcd версии 3.3.25 требуется расширенный репозиторий (repository-extended) Astra Linux. Адрес репозитория уточнить у СПАК ИА.

2. Обновить пакеты и установить etcd: sudo apt update && sudo apt install -y etcd.

При использовании etcd-client версии ниже 3.4 для корректного выполнения команд, требуется включать API ETCD 3: *export ETCDCTL_API=3*

Для отключения API: *unset ETCDCTL_API*

ВАЖНО! Для работы в одномашинной конфигурации необходимо выполнить настройку etcd, для этого в файле /etc/systemd/system/etcd2.service в блок [Service] добавить строки:

Environment=ETCD_LISTEN_CLIENT_URLS="http://<ip-address>:2379"

Environment=ETCD_ADVERTISE_CLIENT_URLS="http://<ip-address>:2379"

, где <ip-address> – адрес сервера одномашинной конфигурации.

Сохранить изменения и выполнить перезапуск службы etcd командой:

sudo systemctl daemon-reload && sudo systemctl restart etcd

10 Установка и первоначальная настройка ПК «АСУРЭО»

10.1 Создание и настройка БД MS SQL

10.1.1 Создание базы данных

Перед установкой ПК на сервере баз данных MS SQL Server 2016 должна быть создана база данных, создана учетная запись пользователя (см. раздел «10.1.2 Создание учетной записи пользователя»), которая будет использована для подключения к БД, а также настроены права доступа этой учетной записи к созданной базе данных (см. раздел «10.1.3 Настройка прав учетной записи пользователя»).

Для создания базы данных необходимо выполнить следующие действия:

1. Открыть MS SQL Management Studio;
2. На вкладке *«Общие» (General)* в поле *«Имя базы данных» (Database name)* указать имя БД (Рисунок 10.1).

Внимание! Не допускается использование специальных символов в именах БД.

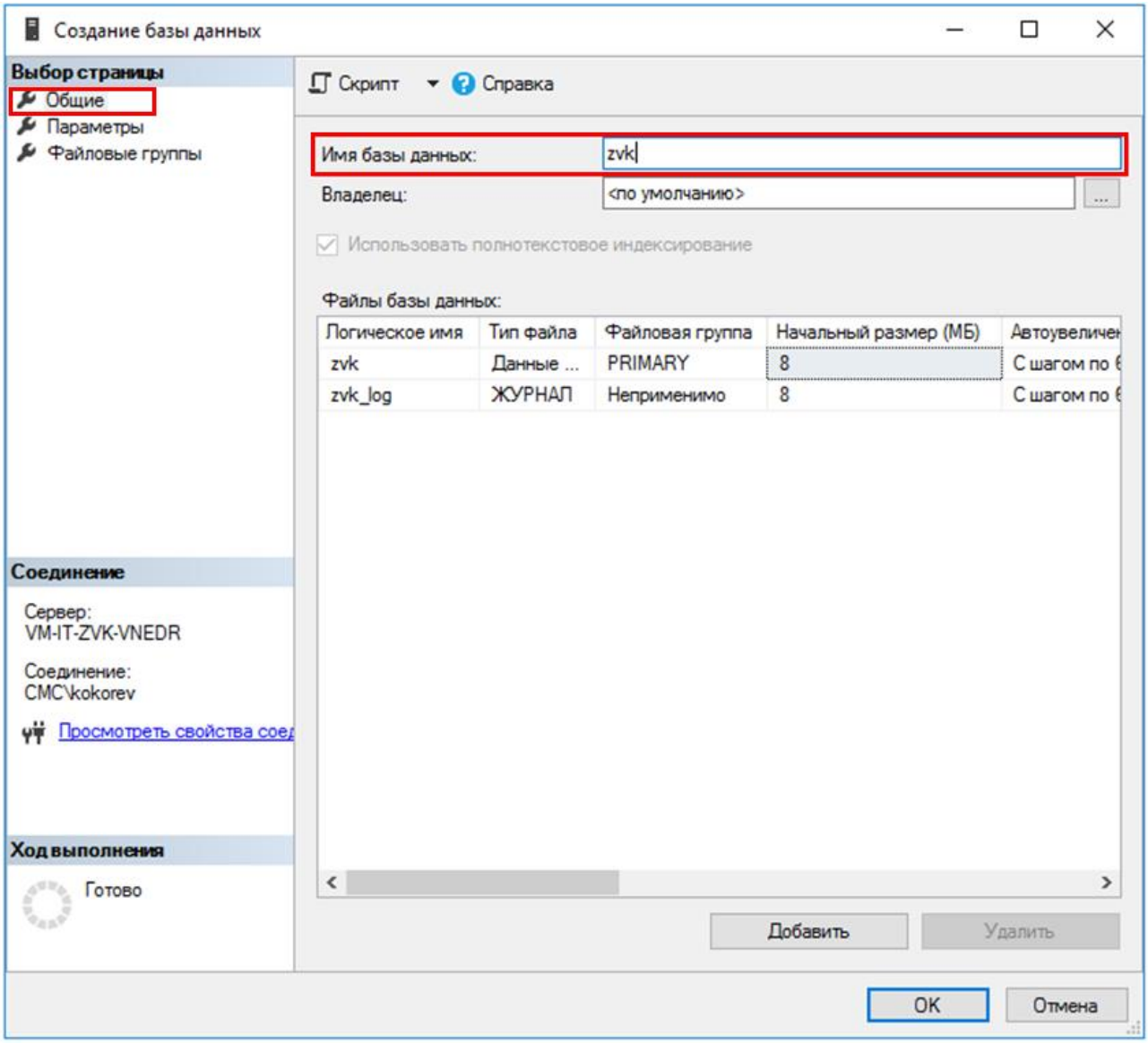

Рисунок 10.1 – Указание имя БД

3. На вкладке *«Параметры» (Options)* для элемента *«Параметры сортировки»* (Collation name) установить значение «Cyrillic_General_CI_AS» (Рисунок 10.2).

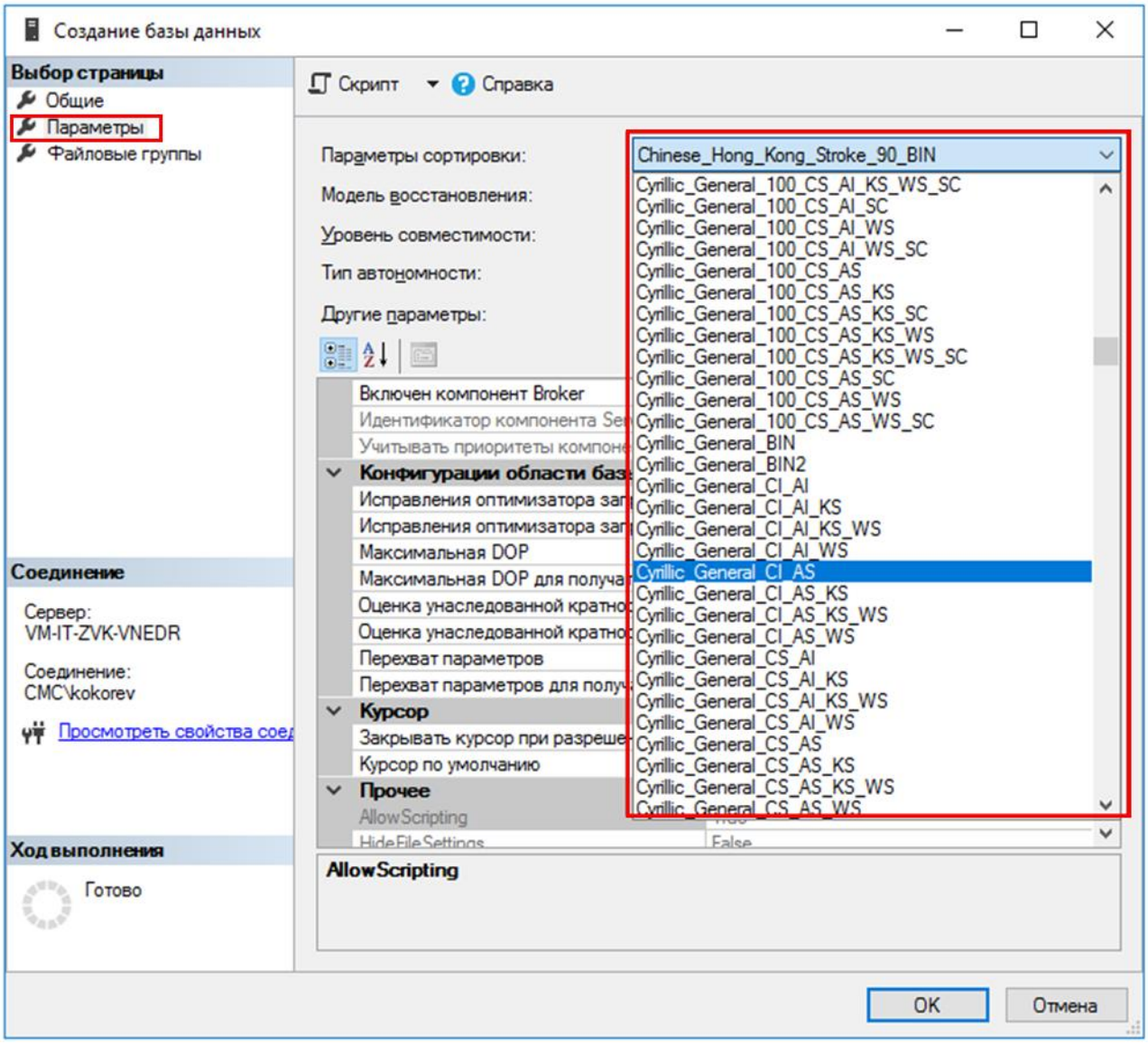

Рисунок 10.2 – Значение Cyrillic_General_CI_AS для элемента «Параметры сортировки» (Collation name)

4. На вкладке *«Параметры» (Options)* для элемента *«Модель восстановления» (Recovery Model)* установить значение *«Полная» (Full)* (Рисунок 10.3).

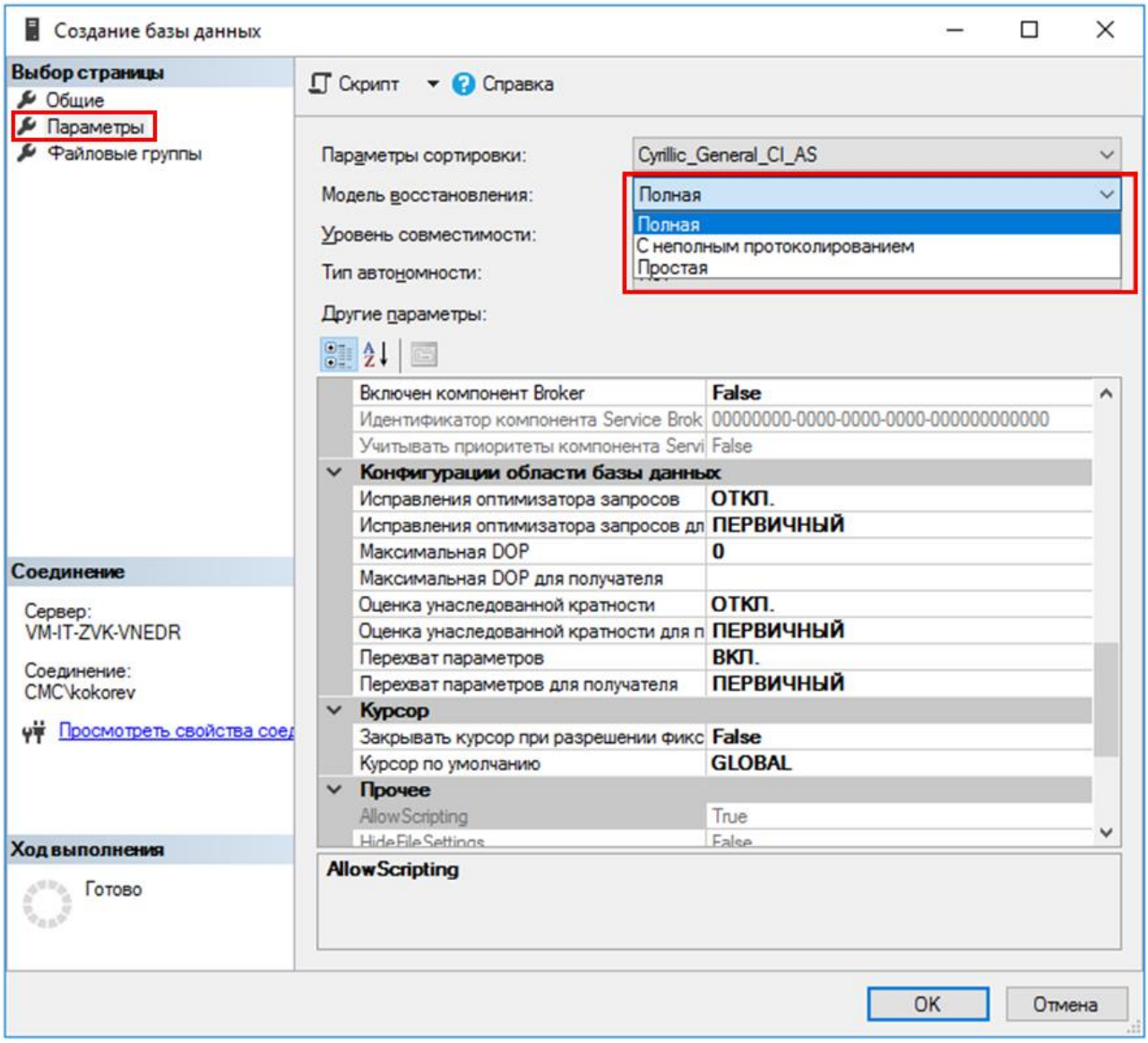

Рисунок 10.3 – Значение Cyrillic_General_CI_AS для элемента *«Модель восстановления» (Recovery Model)*

10.1.2 Создание учетной записи пользователя

При создании учетной записи пользователя, подключающегося к БД, в диалоговом окне создания следует указать имя пользователя, и обязательно необходимо выбрать пункт *«Система безопасности SQL»* (*SQL Server authentication*) и задать пароль для пользователя (Рисунок 10.4). Также следует указать созданную ранее базу данных в качестве базы данных по умолчанию для этого пользователя.

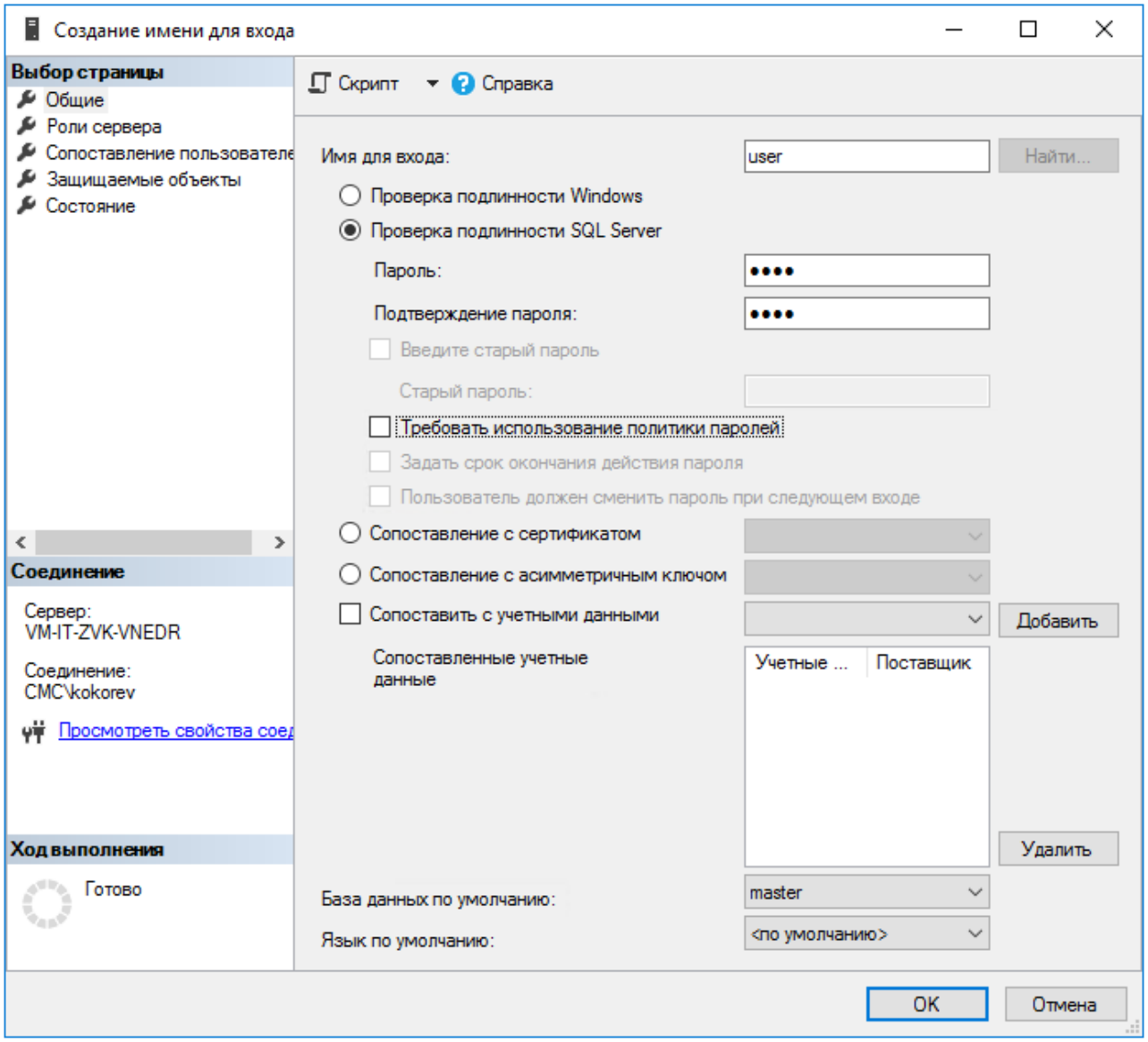

Рисунок 10.4 – Создание учетной записи пользователя

10.1.3 Настройка прав учетной записи пользователя

Для корректной работы программного комплекса учетной записи пользователя, с помощью которой осуществляется доступ к базе данных ПК, необходимо назначить роль базы данных db_owner (владелец БД) (Рисунок 10.5).

В разделе «Сопоставление пользователя» для созданной базы данных назначить членство в ролях: public, db_owner.

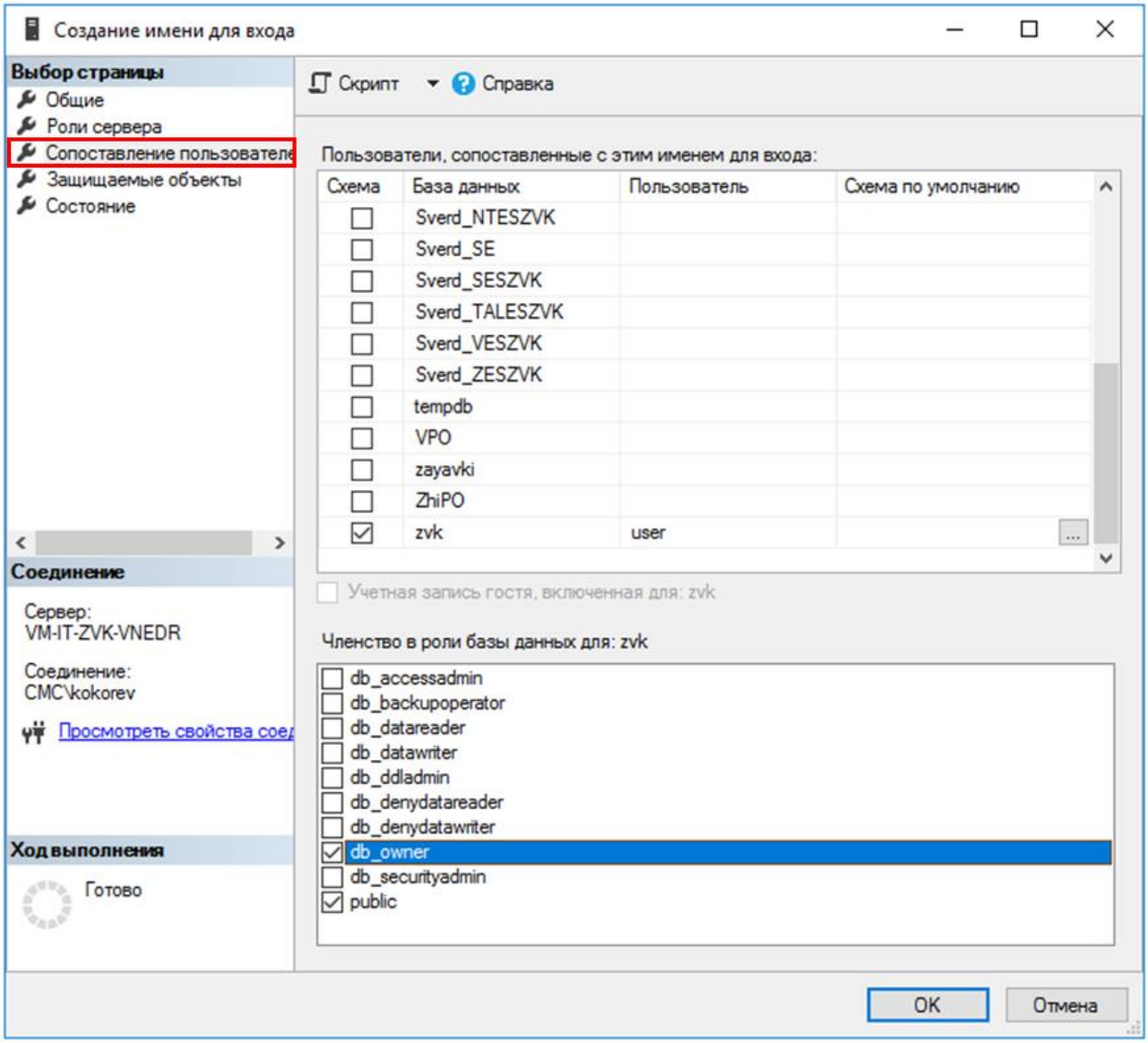

Рисунок 10.5 – Настройка прав учетной записи пользователя

При первоначальной установке и на время последующих обновлений программного комплекса учетной записи пользователя, с помощью которой осуществляется доступ к базе данных ПК, необходимо назначить роль sysadmin в разделе «Роли сервера» (Рисунок 10.6).

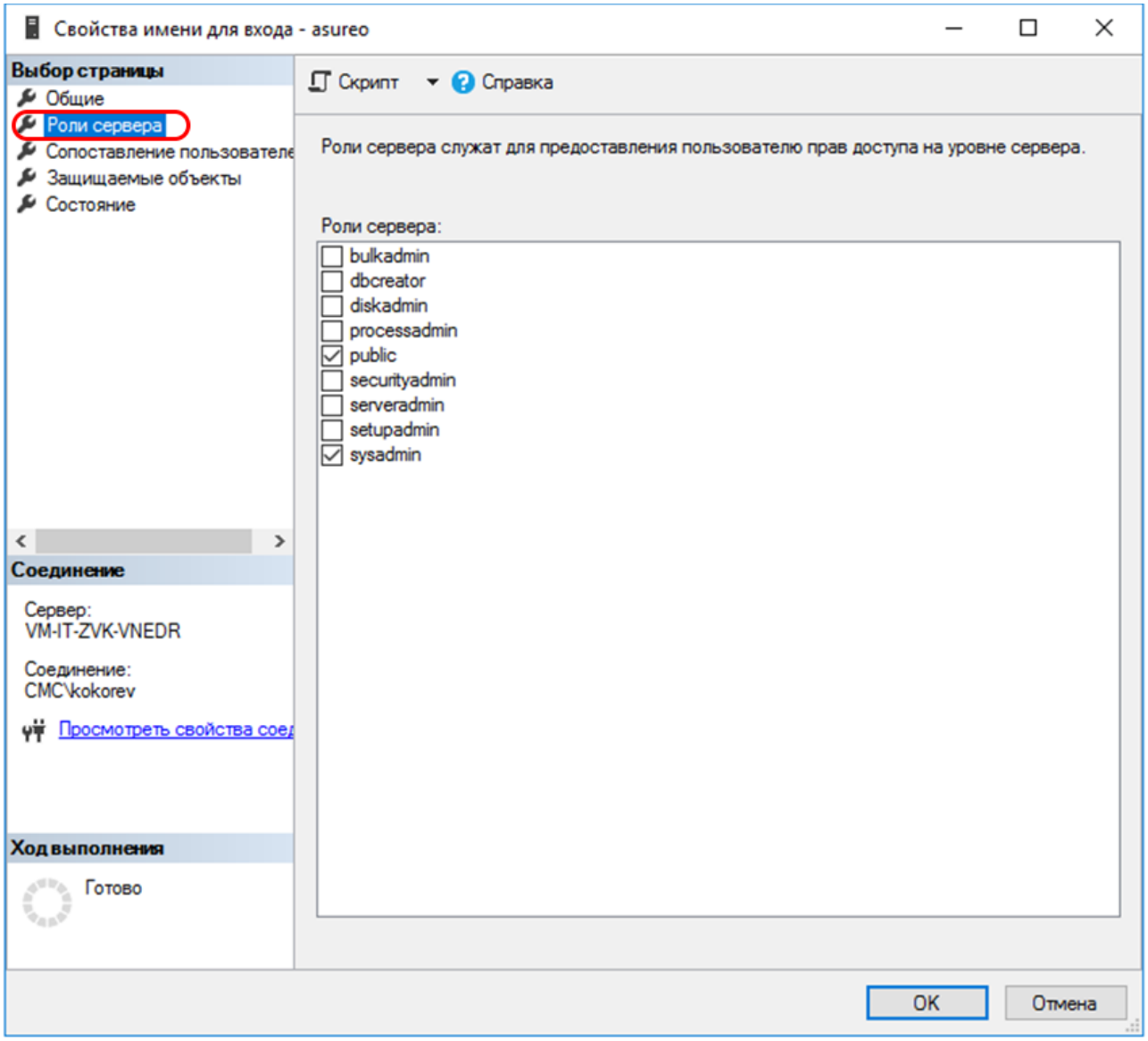

Рисунок 10.6 – Назначение роли sysadmin в разделе «Роли сервера»

10.2 Создание БД PostgreSQL

Перед установкой АСУРЭО на сервере баз данных PostgreSQL должна быть создана база данных.

Для управления СУБД PostgreSQL может использоваться «SQL Shell (psql)» или инструментарий PGAdmin (входит в комплект поставки).

10.2.1 Создание БД с использованием «SQL Shell (psql)»

Для создания базы данных в PostgreSQL на сервере БД, предназначенном для развертывания АСУРЭО с использованием «SQL Shell (psql)» необходимо выполнить следующие действия:

1) Открыть «PostgreSQL 15 (64 bit)»;

2) Кликнуть правой кнопкой мыши на пункте «SQL Shell (psql)». В открывшемся окне «SQL Shell (psql)» в строке postgres=# написать: «create database <имя БД>» (например, «create database asureotest») нажать «Enter». Далее в строке postgres=# ввести «\l» нажать «Enter» (Рисунок 10.7).

Внимание! Не допускается использование специальных символов в именах БД.

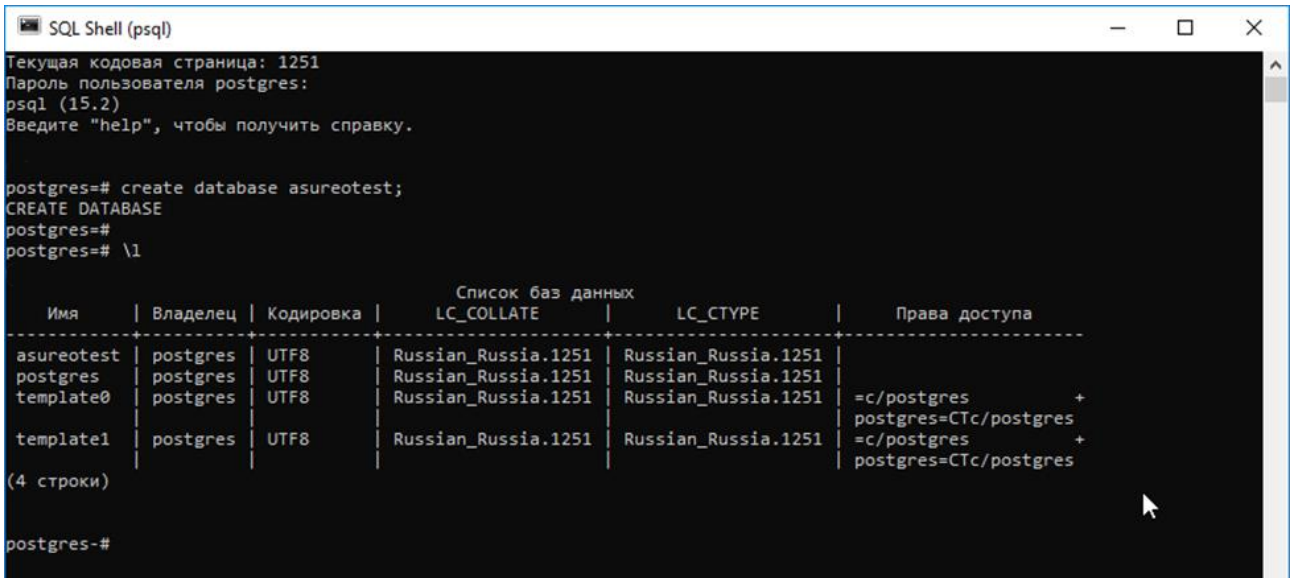

Рисунок 10.7 – Создание новой БД

10.2.2 Создание БД с использованием инструментария PGAdmin

Для создания базы данных в PostgreSQL на сервере БД, предназначенном для развертывания АСУРЭО с использованием инструментария PGAdmin необходимо выполнить следующие действия:

1. В меню «Пуск» выбрать пункт «PGAdmin 4» – «PGAdmin 4 v 4»;

2. Подключиться к серверу СУБД, указав пароль пользователя «postgres» (Рисунок 10.8), который был указан при установке СУБД (см. Рисунок 9.31).

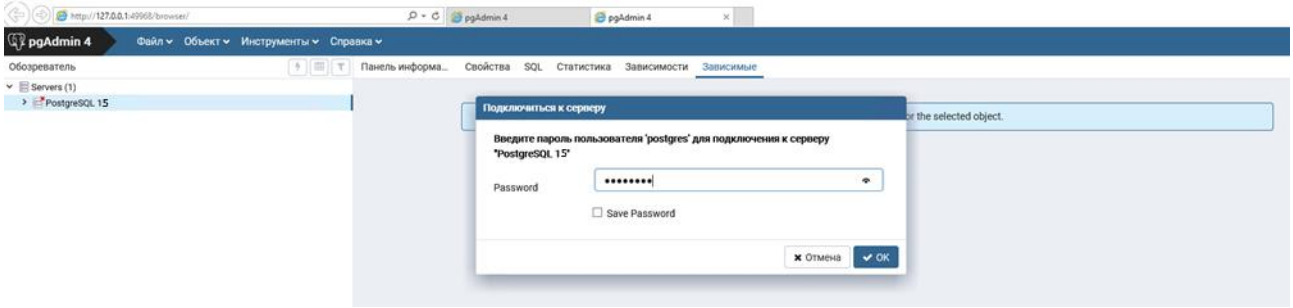

Рисунок 10.8 – Подключение к серверу

3. Из контекстного меню пункта «Базы Данных» выбрать «Создать – База Данных». В открывшейся форме «Создание Базы данных» указать имя базы данных, например, ASUREOTEST и нажать кнопку «Сохранить» (Рисунок 10.9).

Внимание! Не допускается использование специальных символов в именах БД.

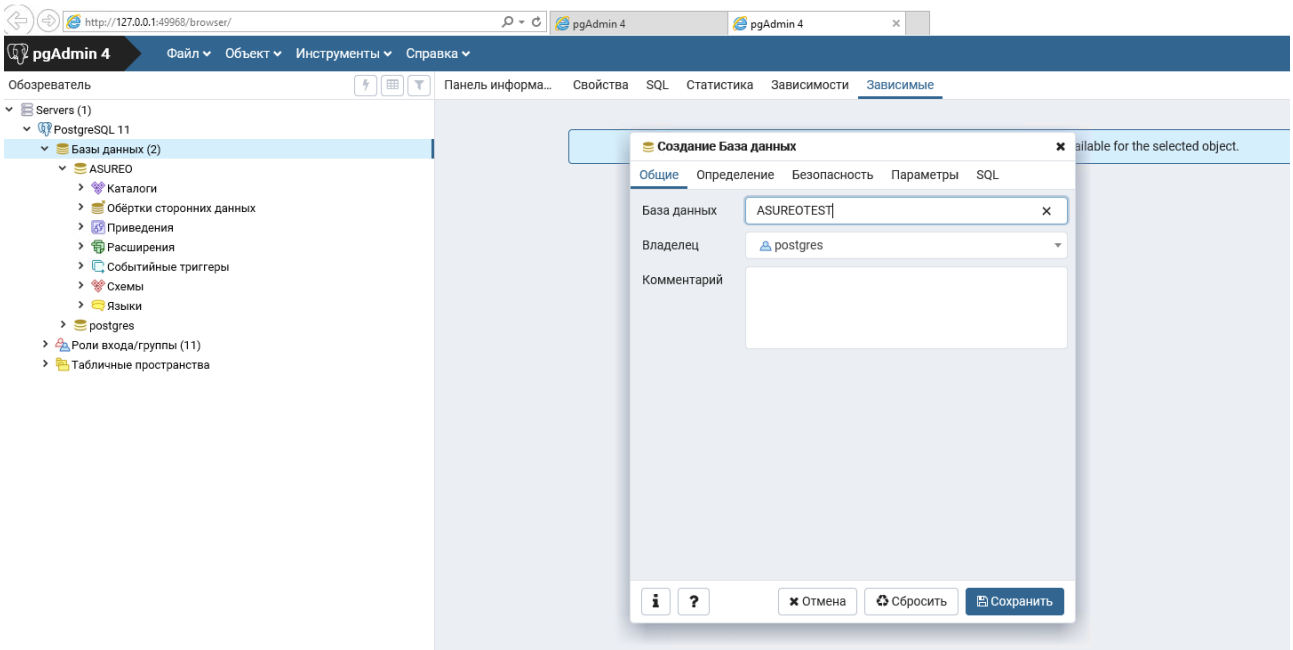

Рисунок 10.9 – Создание базы данных

10.2.3 Создание учетной записи пользователя в инструментарии PGAdmin

При создании учетной записи пользователя, подключающегося к БД, в диалоговом окне «Роль входа» на вкладке «Права» необходимо задать пользователя отличного от postgres без права «Superuser» (Рисунок 10.10).

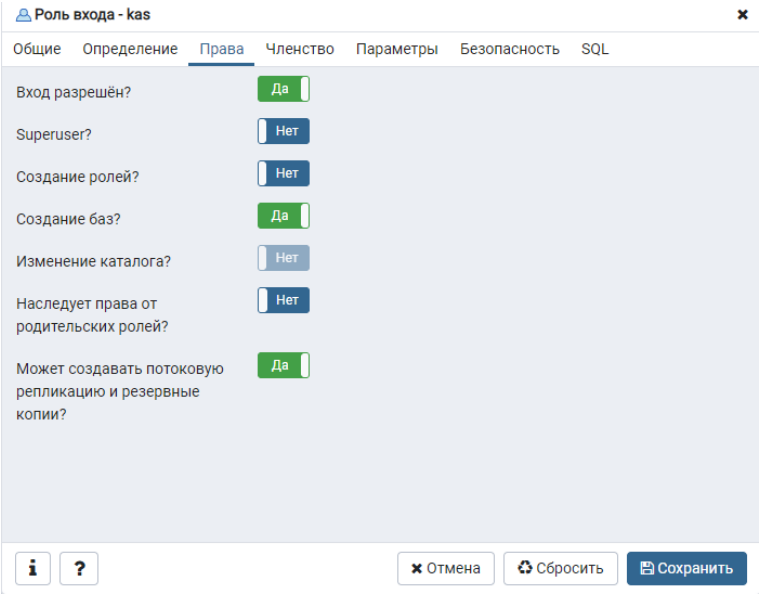

Рисунок 10.10 – Создание пользователя отличного от postgres без права «Superuser»

10.2.4 Настройка прав учетной записи пользователя

Для корректной работы учетной записи пользователя, с помощью которой осуществляется доступ к базе данных, необходимо в контекстном меню имени БД выбрать пункт «Мастер назначения прав». В открывшемся окне выбрать все объекты (Рисунок 10.11).

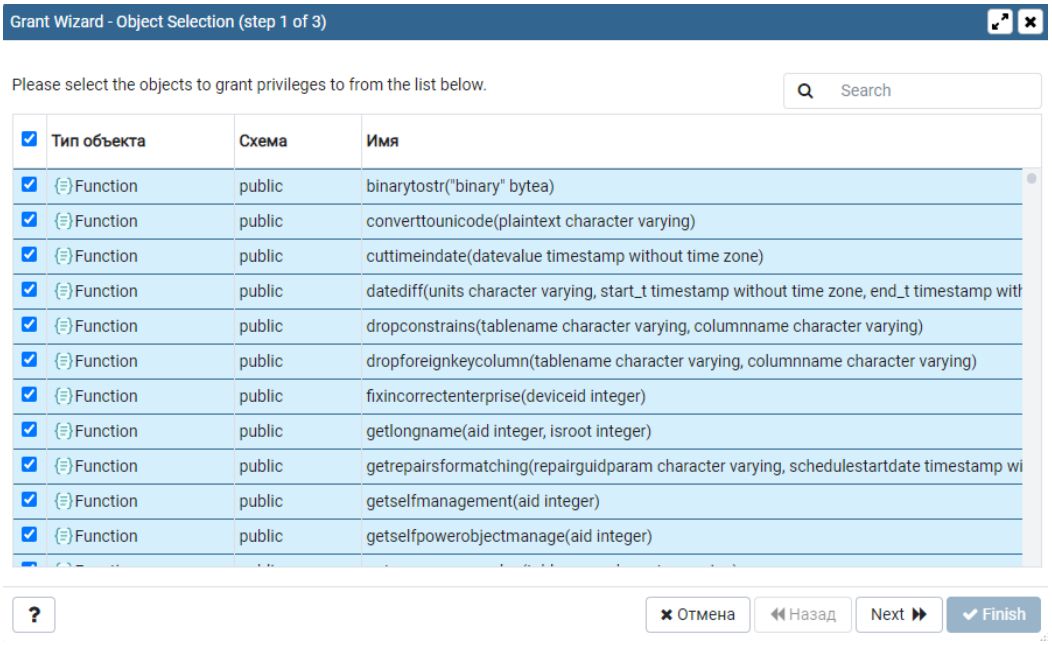

Рисунок 10.11 – Мастер назначения прав

Далее для пользователя, созданного в разделе «10.2.3 Создание учетной записи пользователя», необходимо добавить субъект и выбрать все права (Рисунок 10.12).

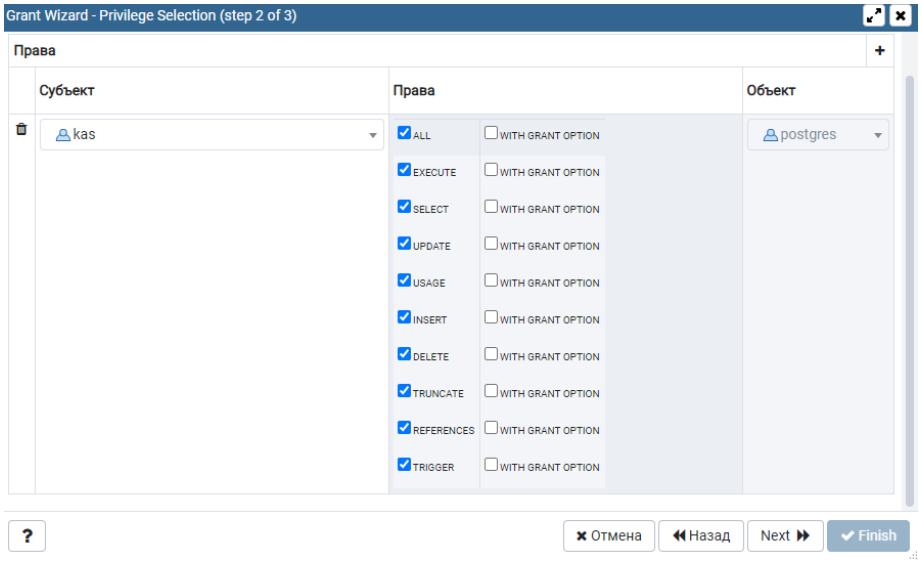

Рисунок 10.12 – Добавление субъекта

При нажатии кнопки «Finish» автоматически формируется скрипт, который необходимо запустить.

Внимание! При обновлении ПК необходимо включить для пользователя опцию «Superuser» (Рисунок 10.13). После завершения обновления опция должна быть выключена.

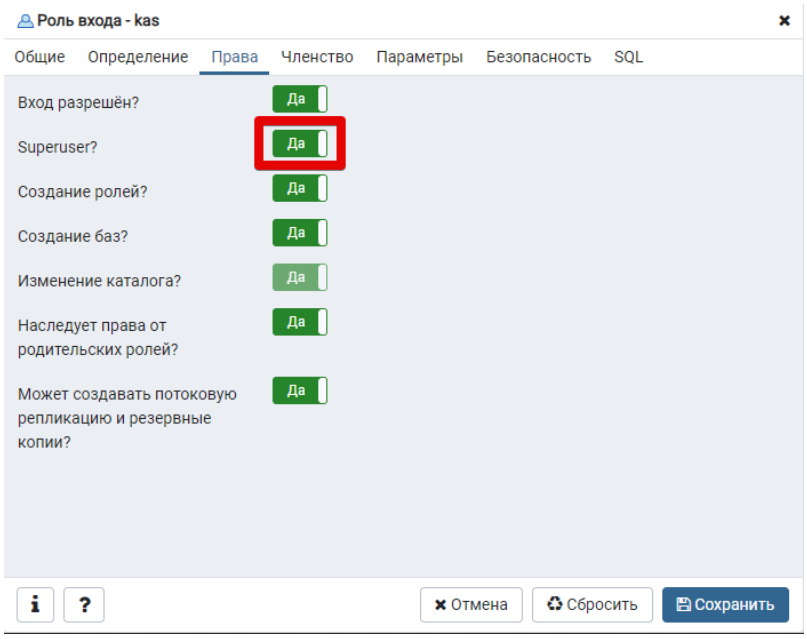

Рисунок 10.13 – Включение опции «superuser»

10.3 Настройка взаимодействия через DataPower

Подробная инструкция приведена в Руководстве Системного Оператора «Инструкция по настройке IBM DataPower Gateway».

10.4 Настройка HTTPS

10.4.1 Общая информация

Процесс настройки HTTPS:

1. На web-сервере назначается секретный ключ, с помощью которого генерируется запрос сертификата (открытого ключа);
2. Получение подписанного сертификата;
3. Установка подписанного сертификата на сервере;
4. Настройка самого сервера.

10.4.2 Установка и настройка сертификата для IIS 7.x

Перед настройкой необходимо убедиться, что в сертификатах сервера IIS присутствует SSL сертификат сервера.

Для настройки веб-сервера необходимо:

1. Запустить консоль управления IIS. Выбрать сайт, на который установлен комплекс АСУРЭО.
2. В разделе «Действия» выбрать привязки. В открывшемся окне необходимо нажать кнопку *«Добавить»*.
3. В окне «Добавление привязки узла» выбрать тип https, в сертификатах SSL выбрать созданный ранее сертификат (Рисунок 10.14).

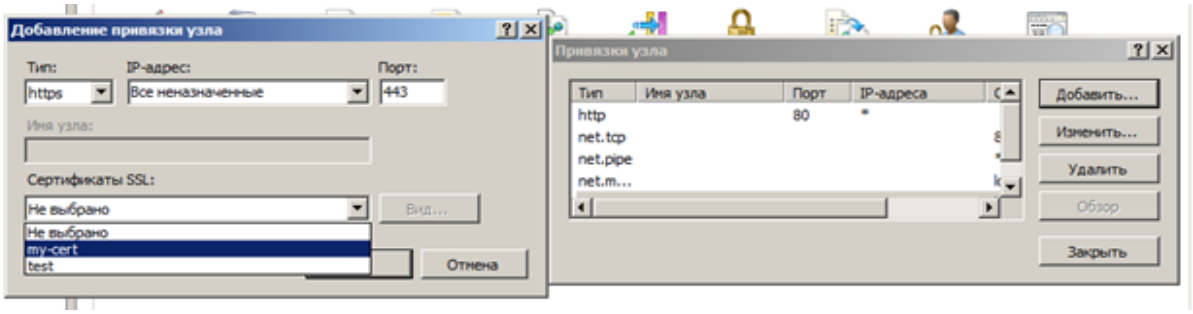

Рисунок 10.14 – Окно «Добавление привязки узла»

После совершенных действий необходимо провести настройки веб-сервера – включить поддержку SSL. Поддержку можно включить на весь веб-узел, либо только на один каталог, куда установлен АСУРЭО.

Если сертификат отсутствует, то необходимо обратиться в Центр сертификации.

10.4.3 Настройка сайта на веб-сервере IIS для работы с SSL

Для перенастройки сайта надо включить поддержку SSL на виртуальном каталоге, в который установлен программный комплекс. Для этого надо выбрать каталог и выбрать «Параметры SSL» (Рисунок 10.15).

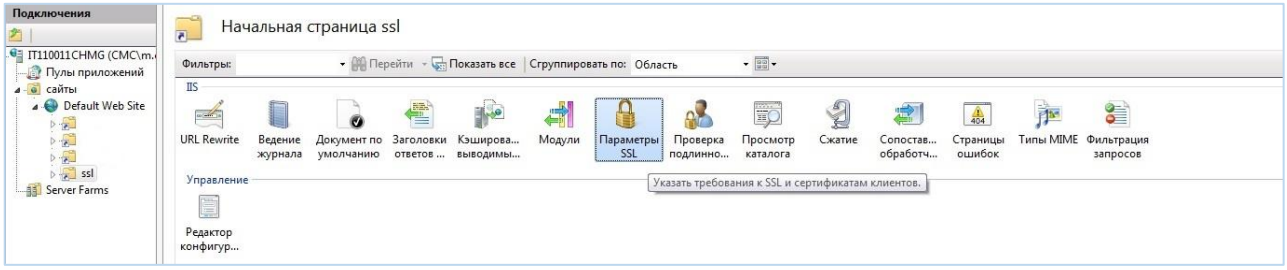

Рисунок 10.15 – Начальная страница SSL

В параметрах SSL в «Сертификатах клиента» выбрать *«Игнорировать»* и далее в действиях выбрать *«Применить»*. После этого необходимо перезагрузить сайт, на котором проводилась настройка (Рисунок 10.16). Если необходимо, чтобы внутренние клиенты продолжали работать по http, а внешние клиенты и обмен по SOAP работал по https, устанавливать флаг «Требовать SSL» в параметрах SSL не нужно.

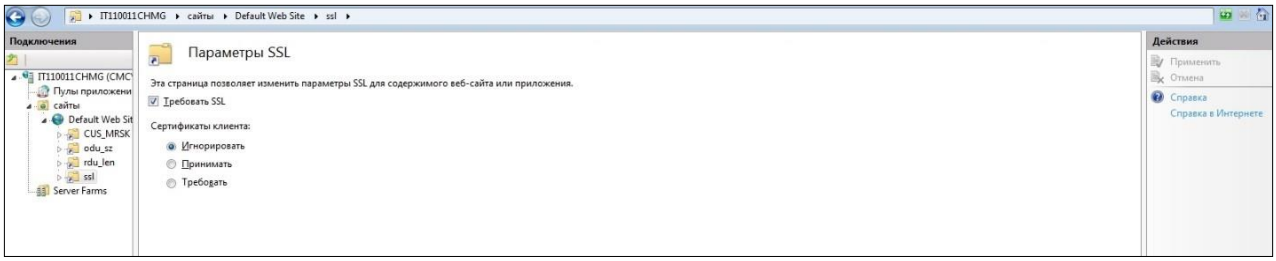

Рисунок 10.16 – Параметры SSL

В результате сайт заработает через защищенное соединение (Рисунок 10.17).

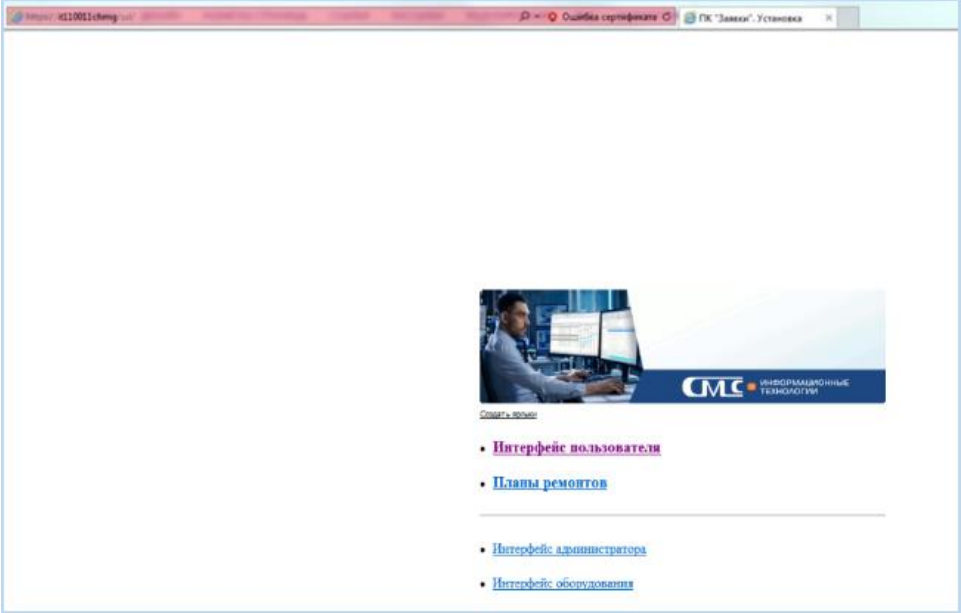

Рисунок 10.17 – Работа сайта через защищенное соединение

Внимание!

В случае настройки взаимодействия с ПК через HTTPS меняется ссылка для доступа к веб-сервисам, что необходимо учесть в настройках интеграции со смежными, системами.

Ссылка для доступа к веб-сервисам (используется протокол HTTPS) должна иметь вид:

https://<Имя_сервера>:<SSLPort>/<имя_экземпляра>/appsrv/Proxy.dll/soap

где SSLPort – номер порта IIS, через который устанавливается безопасное соединение, обычно 443.

В случае необходимости использования протокола HTTP, ссылка для доступа к веб-сервисам имеет вид:

http://<Имя_сервера>/<имя_экземпляра>/appsrv/Proxy.dll/soap

или

http://<Имя_сервера>:<NativePort>/soap

где NativePort – номер порта экземпляра, указанный в конфигурационном файле zvk.ini.

10.5 Настройка basic-авторизации

10.5.1 Общие сведения

Обмен сообщениями с использованием транспорта SOAP позволяет быстро и гарантировано доставлять сообщения между экземплярами ПК. Чтобы обмен производился напрямую, необходимо, чтобы между серверами были установлены доверительные отношения, что допустимо, для серверов оной сети или находящихся в доменах с доверительными отношениями. Но в случаях, если это недопустимо и для обмена используются незащищённые сети, например, через Internet, то на сервере-приёмнике должны быть сделаны определённые настройки, например, открыт определённый порт для всех входящих неавторизованных запросов, что может быть небезопасно. Средствами IIS возможна настройка авторизации для всех входящих запросов, но это неудобно с практической точки зрения: авторизация потребуется для всех и для пользователей собственной сети и для обмена сообщениями между доверенными серверами.

Для повышения защищенности процесса обмена сообщениями с внешними предприятиями может быть использована следующая схема.

Для обмена сообщениями с внешними предприятиями, на сайте где установлен ПК создаётся дополнительный каталог для работы с приложением. Для указанного каталога включаются настройки с требованием авторизации, соответственно все запросы от внешних предприятий должны быть перенаправлены на адрес нового каталога, что повысит безопасность при обмене сообщениями. В ПК реализована возможность отправки сообщений с заданным логином и паролем.

Для использования basic-авторизации на текущем предприятии необходимо указать настройки доступа (логин и пароль).

При отправке сообщения на предприятие с basic-авторизацией на стороне отправителя в состав пересылаемого веб-запроса включаются логин и пароль предприятия-адресата, которые будут использованы при проверке.

Если на предприятии-адресате не используется basic-авторизация, то при приеме сообщения логин и пароль учитываться не будут (Рисунок 10.18).

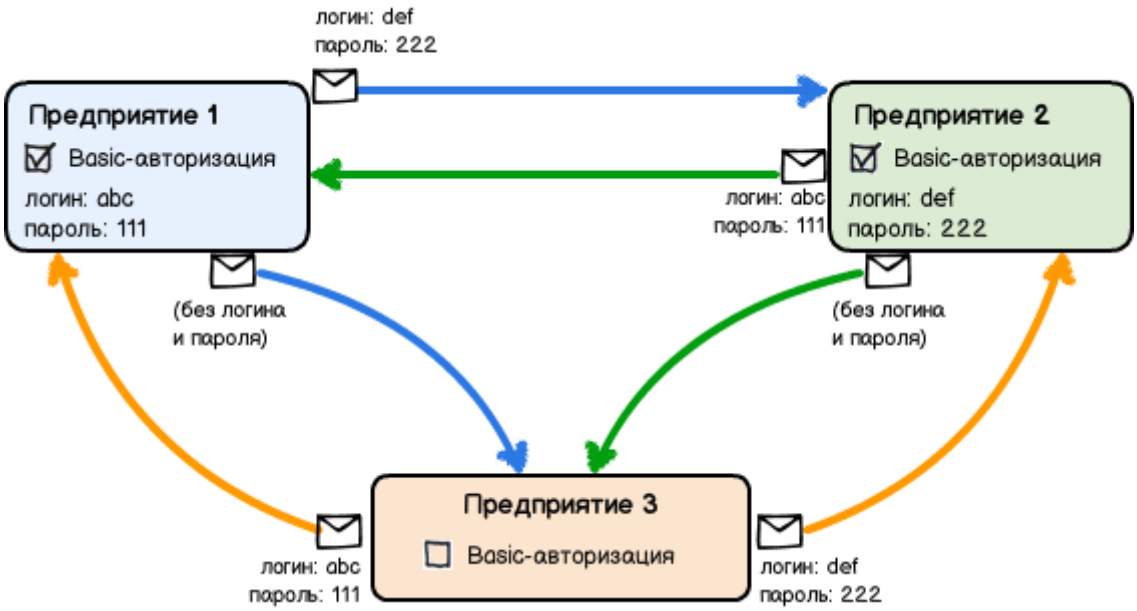

Рисунок 10.18 – Схема отправки сообщений по протоколу SOAP

Для использования basic-авторизации необходимо произвести настройки:

– на web-сервере IIS;
– в интерфейсе оборудования ПК.

10.5.2 Настройка web-сервера IIS на Windows Server 2008

В первую очередь необходимо разделить получение сообщений по SOAP каналу, приходящие с других предприятий и проходящих basic-авторизацию и подключение клиентов внутри сети предприятия без использования авторизации. Для этого необходимо выполнить следующие действия:

1) Перейти в Диспетчер Служб IIS и найти сайт, на который установлен ПК (Рисунок 10.19).

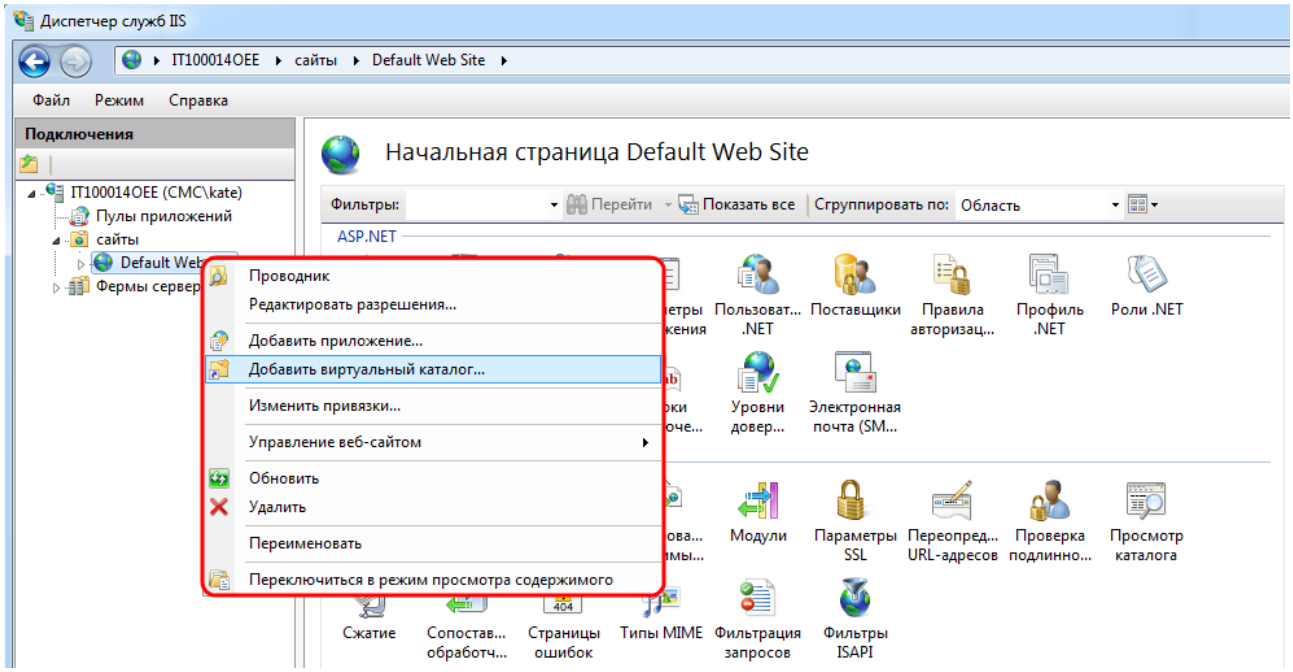

Рисунок 10.19 – Сайт на который установлен ПК

2) Создать под этим сайтом виртуальный каталог с понятным произвольным именем (это имя в последствии будет использоваться в качестве URL адреса обмена сообщениями). В качестве физического пути указать действующий физический каталог, в котором расположен ПК (Например, IIS_n) (Рисунок 10.20).

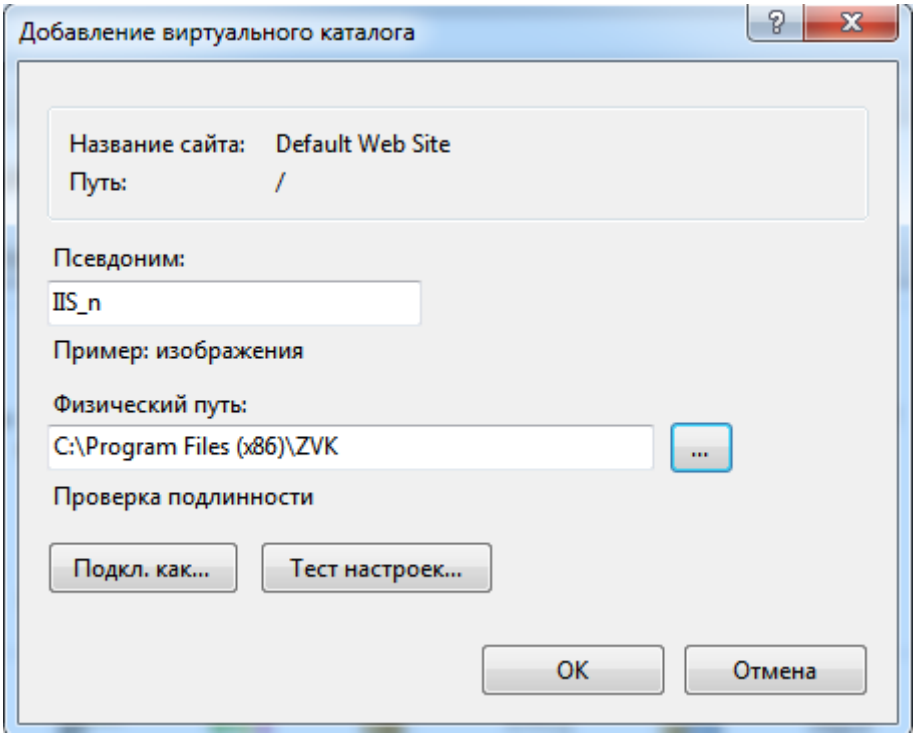

Рисунок 10.20 – Добавление виртуального каталога

Для использования basic-авторизации на стороне предприятия-получателя необходимо:

1) Завести локальную учётную запись без прав, где установлен web-сервер и соответственно ПК (например, test1).

2) Перейти в Диспетчер Служб IIS и найти сайт, на котором установлен ПК. Перейти к виртуальному каталогу, созданному ранее (Рисунок 10.21).

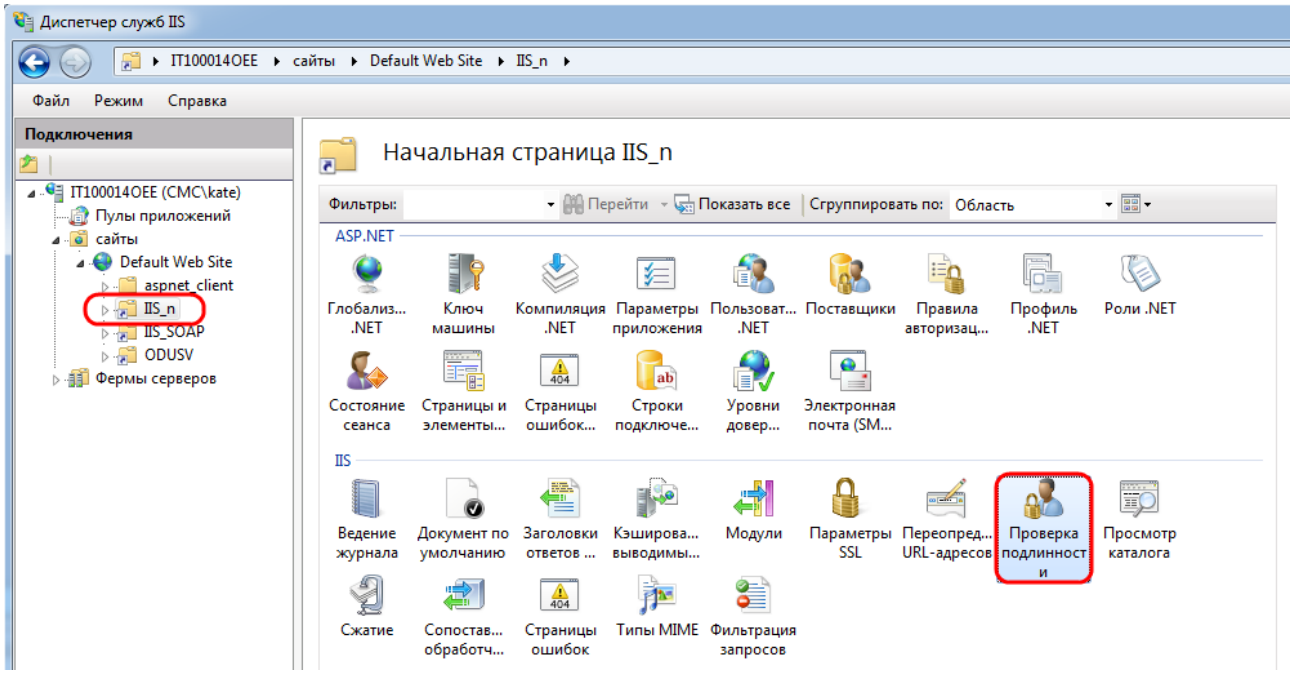

Рисунок 10.21 – Переход к виртуальному каталогу

3) Перейти на вкладку «Проверка подлинности» (Рисунок 10.22).

4) Отключить «Анонимную проверку подлинности» (Рисунок 10.22).

5) Включить «Обычная проверка подлинности» (Рисунок 10.22).

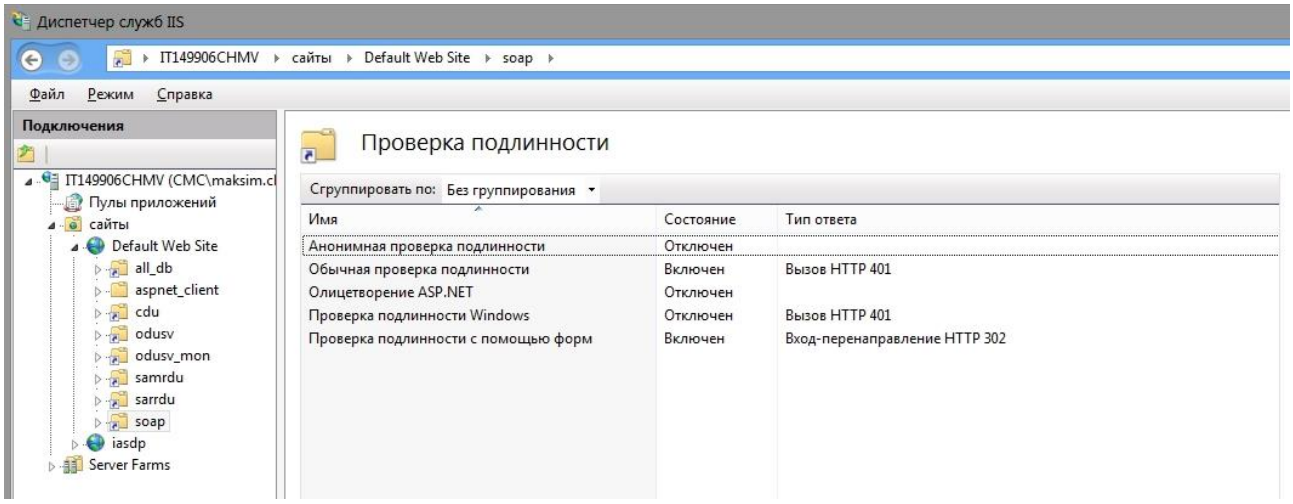

Рисунок 10.22 – Вкладка «Проверка подлинности»

10.5.3 Настройка ПК в части basic-авторизации

Для настройки отправки сообщения на экземпляр с basic-авторизацией необходимо указать логин и пароль для URL адреса на предприятии-отправителе.

Для этого необходимо выполнить следующие действия:

В *Интерфейсе оборудования* на вкладке *«Предприятия»* необходимо выбрать предприятие, на котором используется basic-авторизация.

В область параметров транспорта SOAP указать в качестве URL адреса виртуальный каталог, созданный ранее, логин и пароль, которые были переданы с принимающего предприятия (Рисунок 10.23).

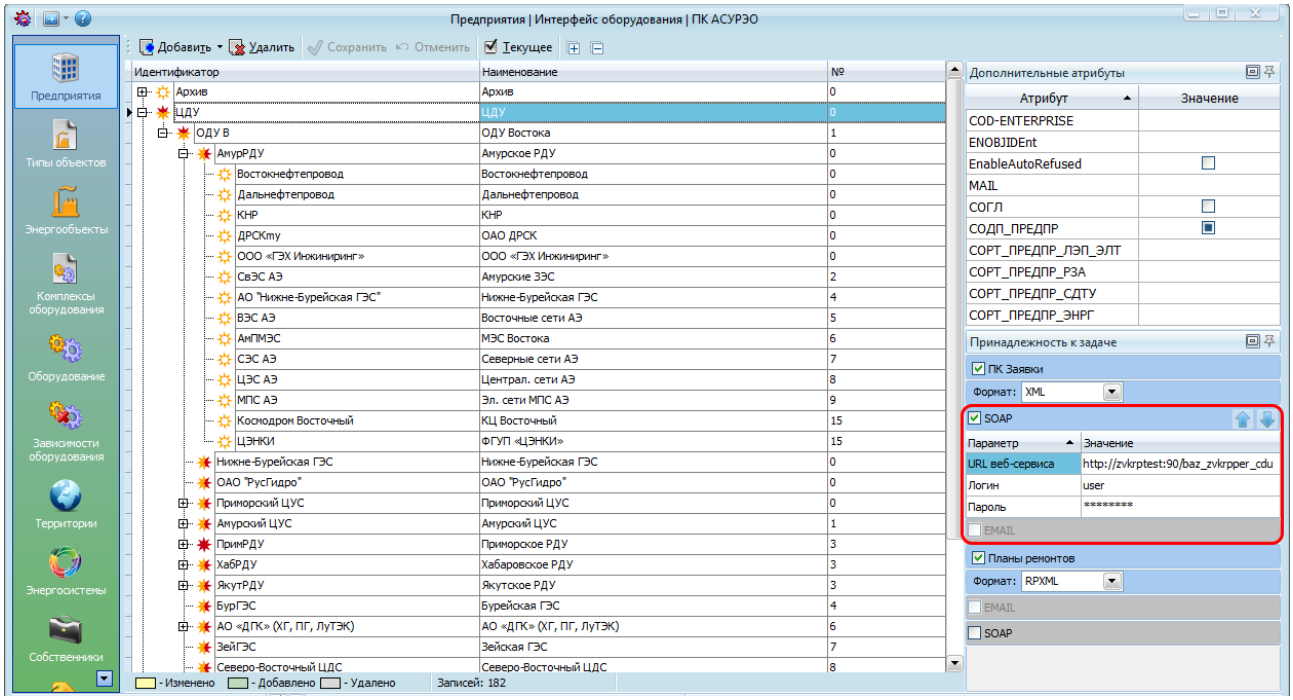

Рисунок 10.23 – Настройка транспорта SOAP

После осуществления всех настроек клиенты внутри предприятия будут подключаться без авторизации, при этом приём сообщений от других предприятий будет осуществляться с использованием basic-авторизации по новому адресу (адрес виртуального каталога).

Рекомендуем произвести тестовую отправку сообщения (например, переслать тестовую заявку и убедиться, что сообщение получено принимающим предприятием) и подключение клиента ПК (Запустить клиент и убедиться в отсутствии авторизации).

10.6 Установка АСУРЭО на СУБД MSSQL/PostgreSQL на ОС Windows

Внимание! При установке АСУРЭО на СУБД PostgreSQL на ОС Windows необходимо включить для пользователя опцию «Superuser». После завершения установки опция должна быть выключена.

Установка АСУРЭО осуществляется с помощью установщика дистрибутива ПК «АСУРЭО» / ПК «Планы ремонтов», что позволяет вводить необходимую информацию пошагово (Рисунок 10.24). Для открытия установщика необходимо запустить под правами администратора файл «*Setup.exe*» из каталога «*install*» установочного диска ПК.

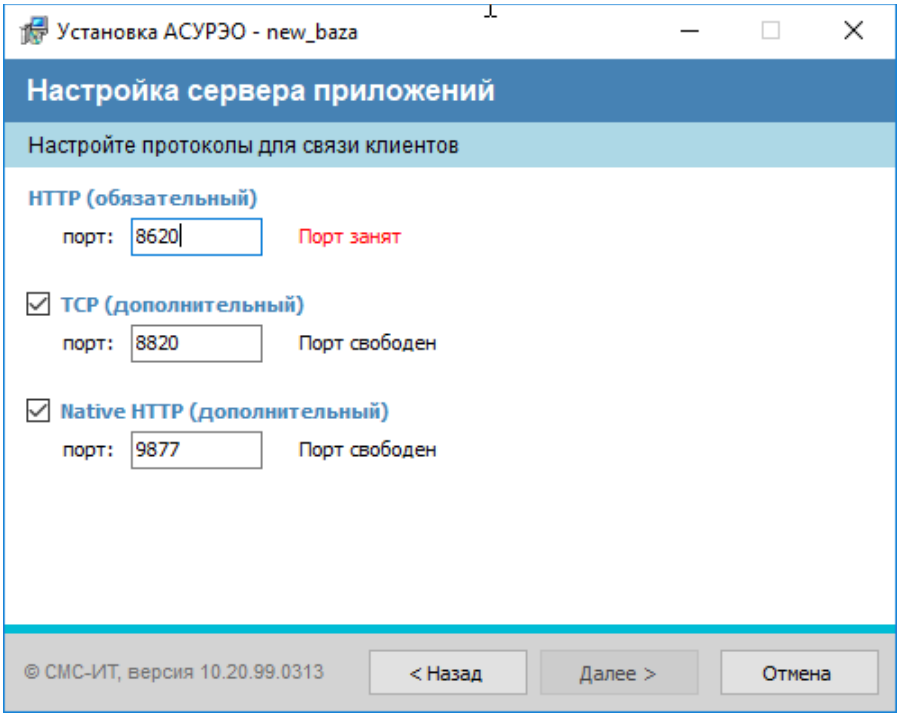

Рисунок 10.24 – Мастер установки

В верхней части окна установщика отображается информация о текущем шаге установки ПК. Управление установщиком осуществляется посредством кнопок:

– *Кнопка «Далее >»* предназначена для перехода к следующему шагу установки. Кнопка становится активной при заполнении обязательных полей и отсутствии ошибок, в указанных данных;
– *Кнопка «< Назад»* предназначена для перехода к предыдущему шагу установки. Кнопка становится активной при прохождении первого шага установки;
– *Кнопка «Отмена» предназначена для выхода из установщика. В появившемся диалоговом* окне *«Выход из программы установки»* для подтверждения отмены установки необходимо нажать на кнопку «*Да*», в противном случае нажать на кнопку «*Нет*» (Рисунок 10.25).

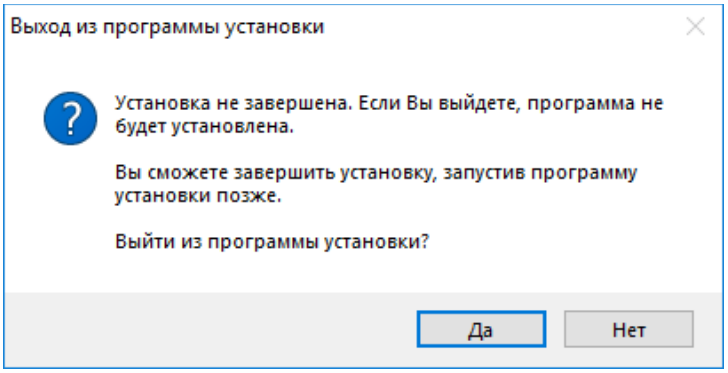

Рисунок 10.25 – Подтверждение отмены установки

В стартовом окне установщика *«Выбор производимых действий»* необходимо выбрать одно из действий (Рисунок 10.26):

– ***«Новый экземпляр»***. Для установки нового экземпляра.
– ***«Обновить экземпляры».*** Для обновления экземпляров, уже существующих на сервере (см. раздел «10.15 Обновление ПК»).
– ***«Удалить экземпляры».*** Для удаления установленных экземпляров.

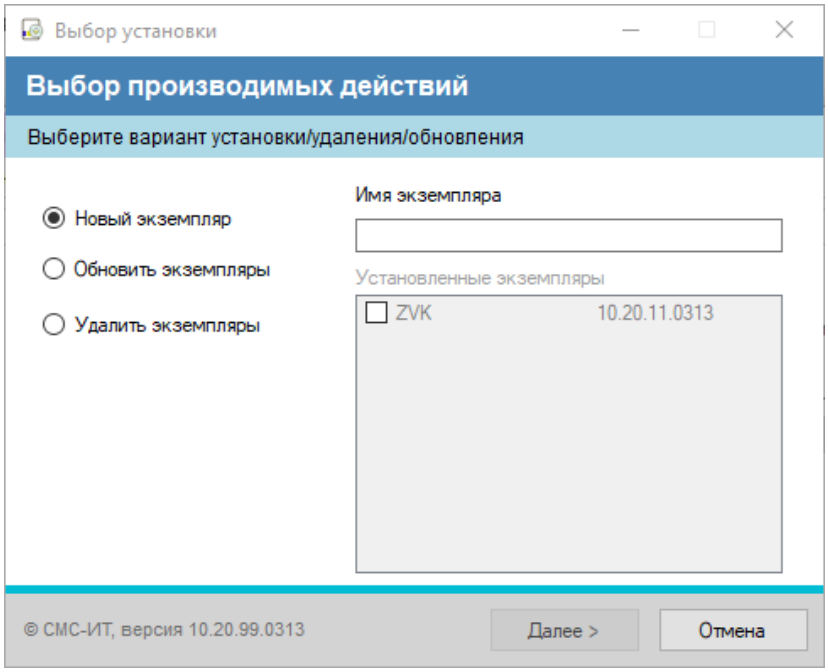

Рисунок 10.26 – Стартовое окно мастера установки

10.6.1 Выбор производимых действий

Для установки нового экземпляра ПК в стартовом окне мастера установки *«Выбор производимых действий»* необходимо выбрать пункт *«Новый экземпляр»*. В поле *«Имя*

экземпляра» необходимо ввести имя экземпляра латинскими буквами и нажать на кнопку *«Далее»* (Рисунок 10.27).

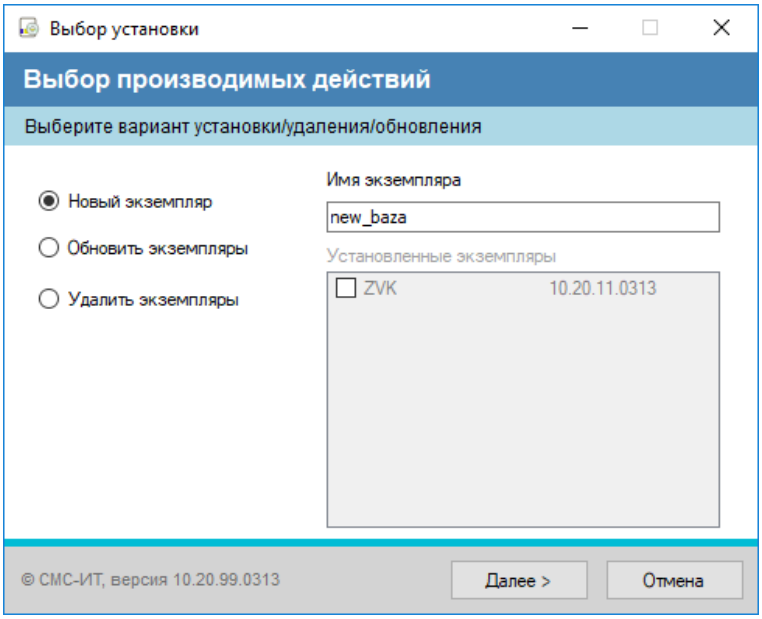

Рисунок 10.27 – Ввод имени экземпляра

При нажатии на кнопку *«Далее >»* открывается шаг *«Проверки системных требований»* (Рисунок 10.28).

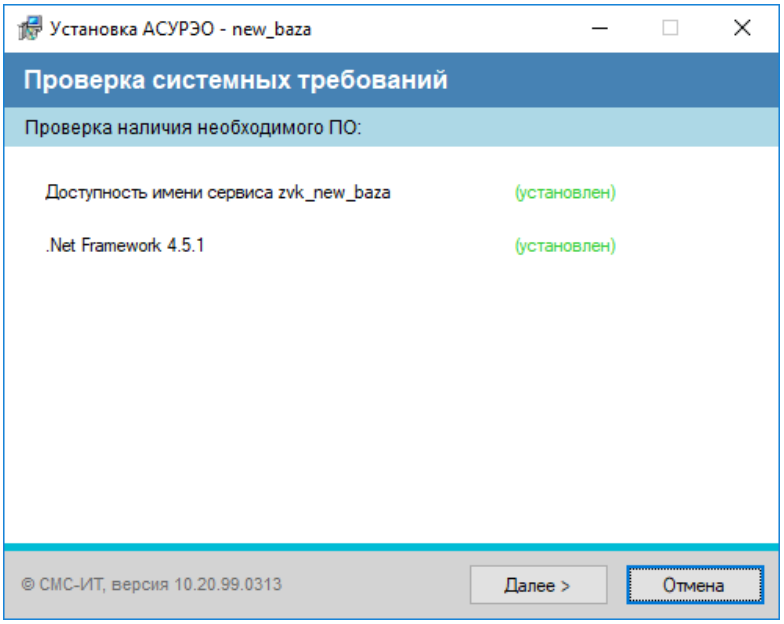

Рисунок 10.28 – Проверка системных требований

При установке первого экземпляра ПК в окне мастера *«Выбор папки установки»* (Рисунок 10.29) предоставляется возможность выбора директории установки, единой для всех

экземпляров комплекса (по умолчанию предлагается директория «C:\Program Files (x86)\ZVK»).

Внимание! ПК не следует устанавливать в директорию, содержащую в названии папок специальные символы (например, «;», «)», «%»). Сервер приложений работать не будет.

Внимание! Начиная с версии 10.20.115.0313 установка экземпляра (32-битное приложение) возможна только в директорию C:\Program Files (x86)\ZVK или в директорию на другом диске (например, диск D, F и др.).

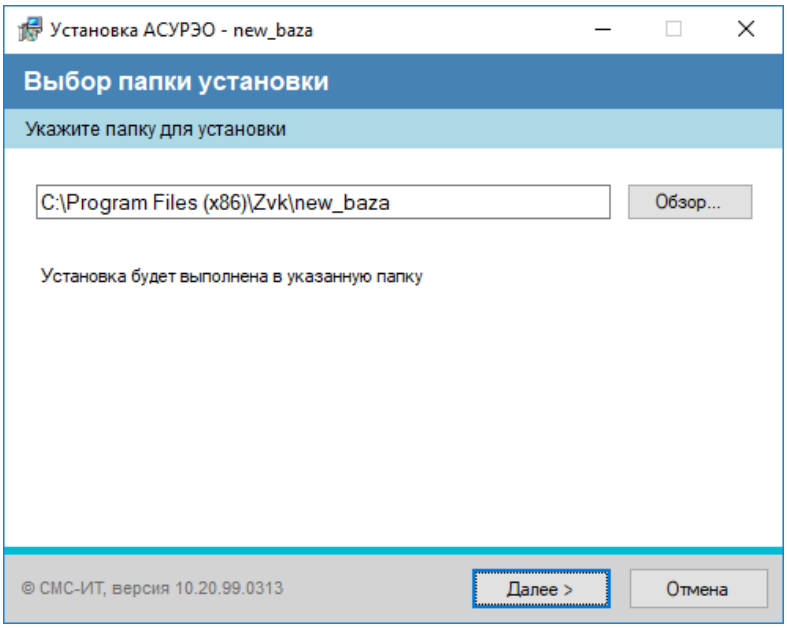

Рисунок 10.29 – Выбор папки установки

Поскольку в стартовом окне мастера *«Выбор производимых действий»* имя экземпляра уже было указано, то переход осуществляется сразу к выбору дополнительных компонентов ПК.

10.6.2 Выбор дополнительных компонентов

Если в поставку ПК входят дополнительные компоненты, то следующим шагом установки будет шаг «Выбор компонентов». В окне *«Выбор компонентов»* необходимо установить флаги напротив нужных компонентов (Рисунок 10.30).

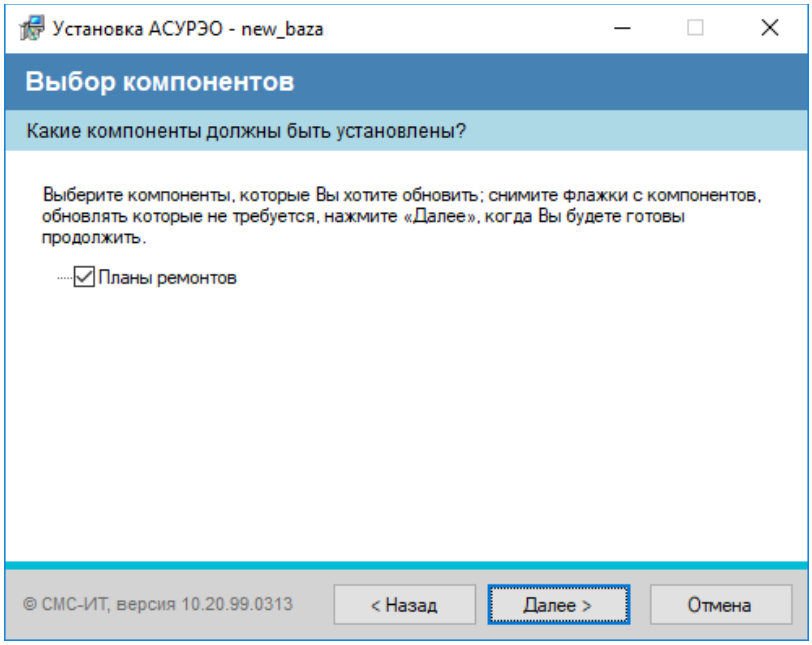

Рисунок 10.30 – Выбор компонентов

10.6.3 Выбор версии веб-сервера

В окне *«Выбор веб-сервера»* из раскрывающегося списка *«Найденные веб-серверы и сайты»* необходимо выбрать используемый веб-сервер IIS и в поле *«Адрес веб-сервера»* указать ip-адрес веб-сервера (Рисунок 10.31).

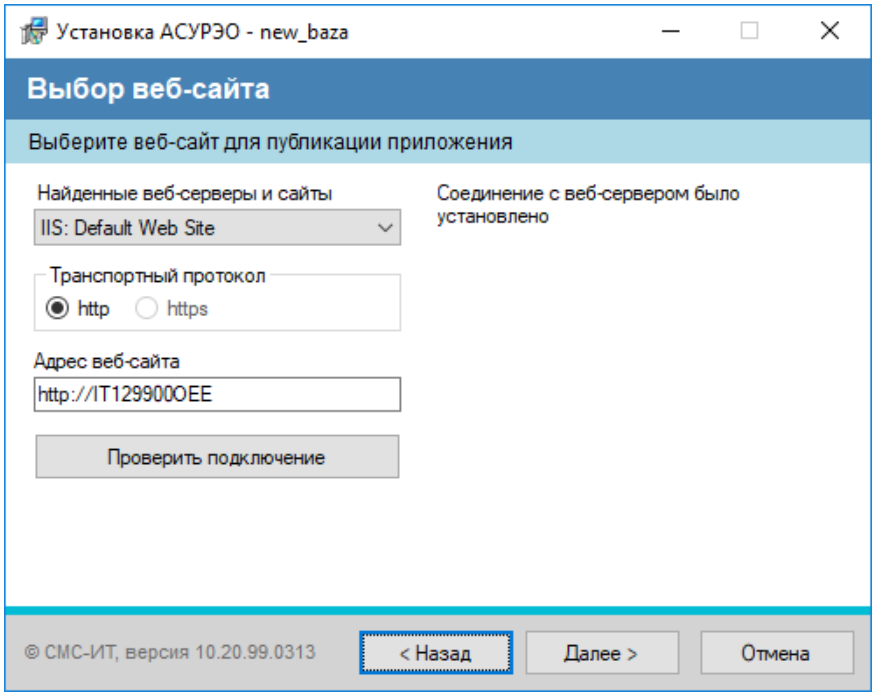

Рисунок 10.31 – Выбор версии веб-сервера

Внимание! При установке ПК на Windows Server 2008 с IIS 7 и выше необходимо установить два дополнительных компонента, не входящих в стандартную поставку IIS:

- переадресация запросов URL Rewrite 2.0;
- прокси-переадресация Application Request Routing 2.0.

В данном случае на шаге выбора версии веб-сервера появится сообщение об ошибке со ссылками на дистрибутивы (Рисунок 10.32).

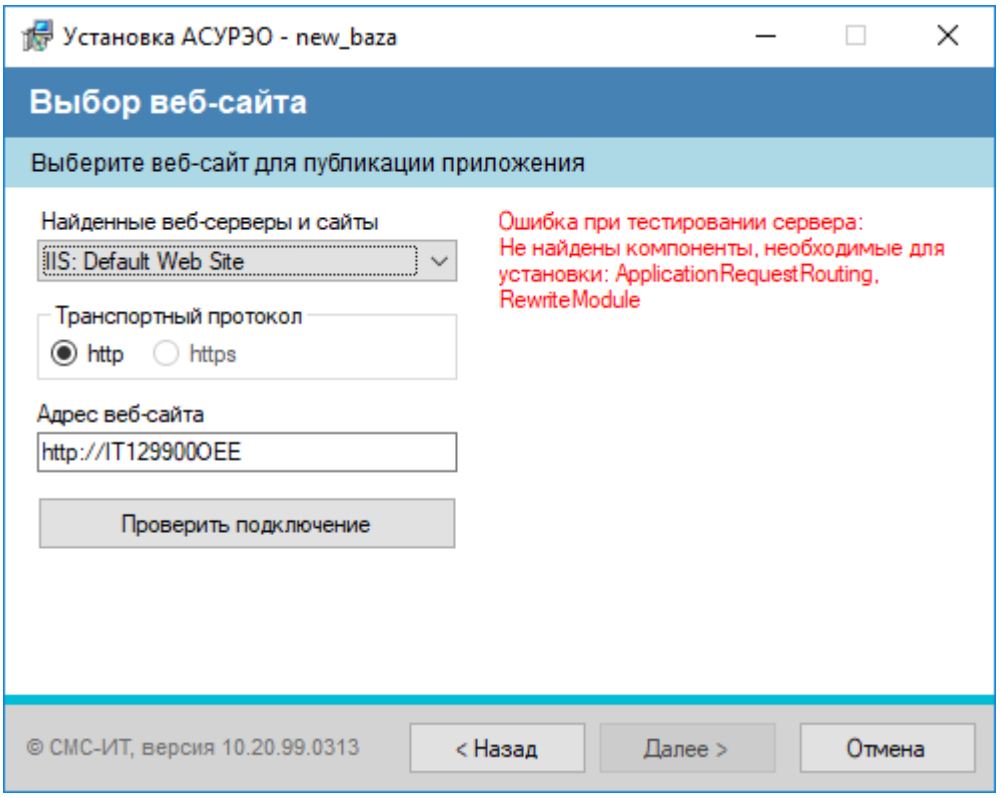

Рисунок 10.32 – Установка дополнительных компонентов IIS

Для установки компонента переадресации запросов URL Rewrite 2.0 необходимо скачать дистрибутив с сайта Microsoft.

Для 32-х и 64-х разрядных ОС выпущены отдельные дистрибутивы:

для x86: http://download.microsoft.com/download/6/9/C/69C1195A-123E-4BE8-8EDF-371CDCA4EC6C/rewrite_2.0_rtw_x86.msi;

для x64: http://download.microsoft.com/download/6/7/D/67D80164-7DD0-48AF-86E3-DE7A182D6815/rewrite_2.0_rtw_x64.msi.

Для установки компонента прокси-переадресации Application Request Routing 2.0 необходимо скачать дистрибутив с сайта Microsoft.

Для 32-х и 64-х разрядных ОС выпущены отдельные дистрибутивы:

для x86: http://download.microsoft.com/download/4/D/F/4DFDA851-515F-474E-BA7A-5802B3C95101/ARRv2_setup_x86.EXE;

для x64: http://download.microsoft.com/download/3/4/1/3415F3F9-5698-44FE-A072-D4AF09728390/ARRv2_setup_x64.EXE.

Для установки компонента прокси-переадресации Application Request Routing 3.0 необходимо скачать дистрибутив с сайта Microsoft.

Для 32-х и 64-х разрядных ОС выпущены отдельные дистрибутивы:

для x86: https://www.microsoft.com/en-us/download/details.aspx?id=47334

для x64: https://www.microsoft.com/en-us/download/details.aspx?id=47333

При необходимости, можно протестировать соединение с указанным сервером с помощью кнопки *«Проверить подключение»*.

10.6.4 Настройка сервера приложений

На данном шаге производится настройка протоколов для связи с клиентами (Рисунок 10.33). Для этого необходимо указать обязательный порт «HTTP» для связи web-сервера с сервером приложений. Также можно указать дополнительные порты TCP и / или Native HTTP, установив флаг напротив нужного порта.

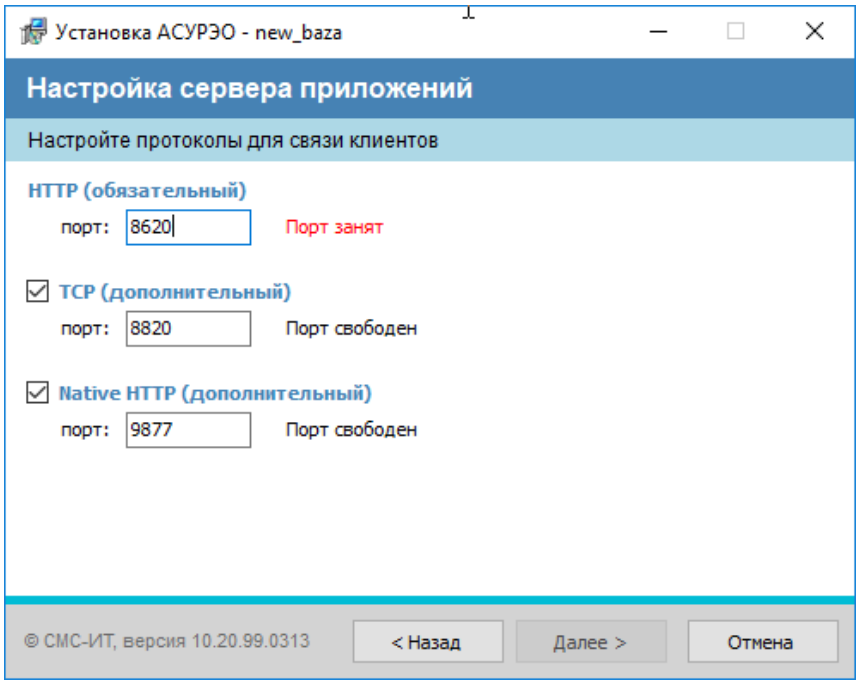

Рисунок 10.33 – Настройка протоколов для связи клиентов

Мастер установки автоматически проверяет, занят ли указанный порт (например, другим экземпляром), и выводит соответствующее сообщение напротив поля ввода номера порта (Рисунок 10.33). Кнопка *«Далее >»* становится активной, если все указанные порты свободны (Рисунок 10.34).

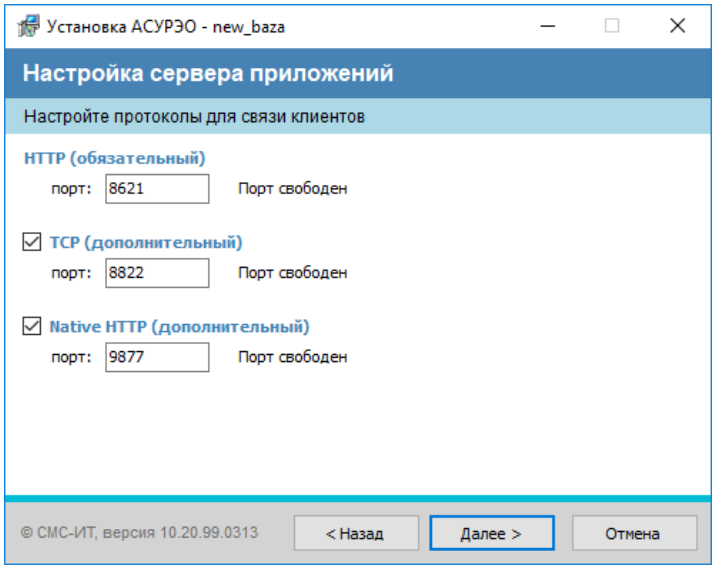

Рисунок 10.34 – Проверка портов

Внимание! Для того, чтобы пользователи смогли запустить ПК с клиентских машин, на сервере где установлен программный комплекс, в настройках FireWall, необходимо добавить в исключение порты HTTP, TCP, Native HTTP, которые указываются при установке ПК.

На шаге *«Настройка учетной записи (Учетная запись для Windows службы)»* производится настройка учетной записи для запуска службы сервера приложений (zvkservice.exe) (Рисунок 10.35).

1. Установить флаг напротив пункта *«Использовать системную учетную запись»* (установлен по умолчанию);
2. Нажать кнопку «Далее».

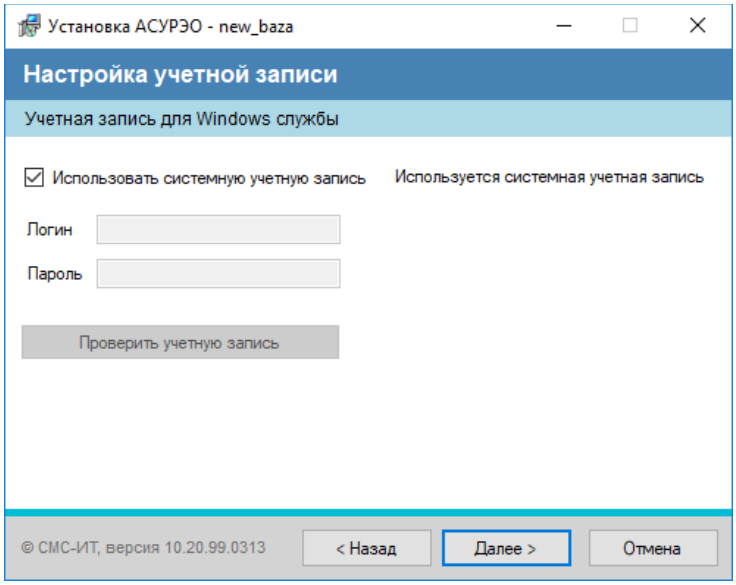

Рисунок 10.35 – Использование системной учетной записи

10.6.5 Выбор базы данных

На следующем шаге необходимо выбрать поддерживаемую базу данных *«MSSQL»* или *«PostgreSQL»* (Рисунок 10.36).

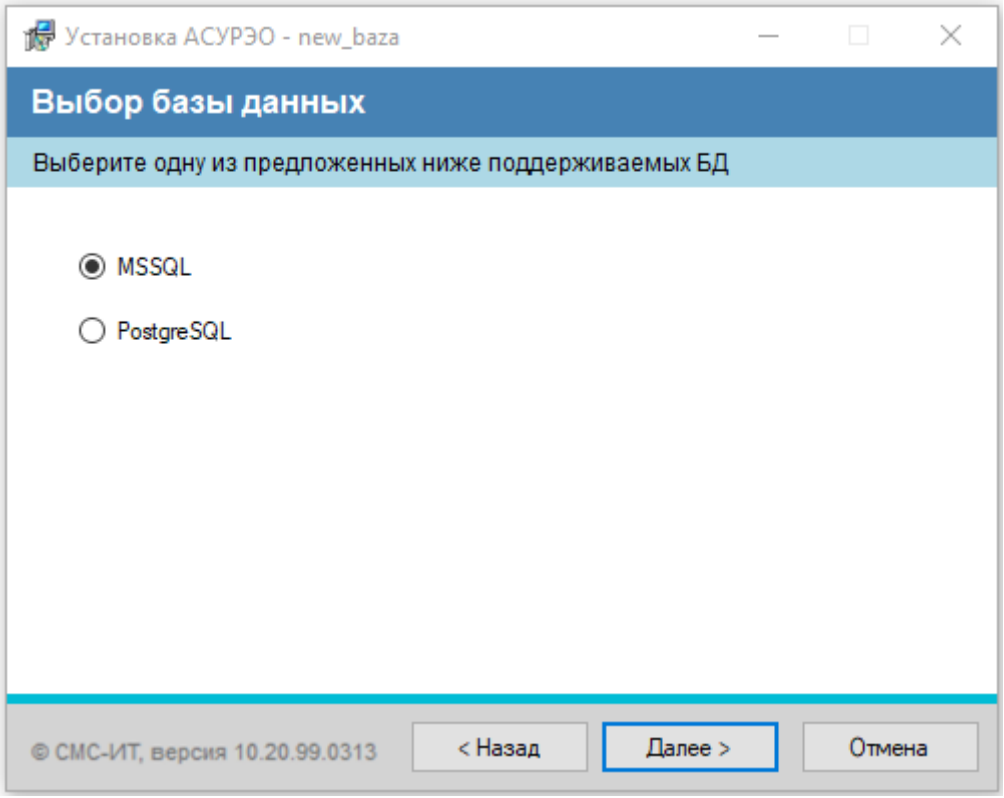

Рисунок 10.36 – Выбор базы данных

10.6.6 Настройка подключения к MSSQL/PostgreSQL

На следующем шаге производится настройка подключения к MSSQL/PostgreSQL. В окне *«Настройка подключения к MSSQL/PostgreSQL»* необходимо ввести имя или IP-адрес сервера баз данных, имя пользователя и пароль, используемые для подключения к MSSQL/PostgreSQL (Рисунок 10.37).

Данные о пользователе должны соответствовать настройкам созданной ранее учетной записи пользователя (см. разделы «10.1.3 Настройка прав учетной записи пользователя» и «10.2.4 Настройка прав учетной записи пользователя»).

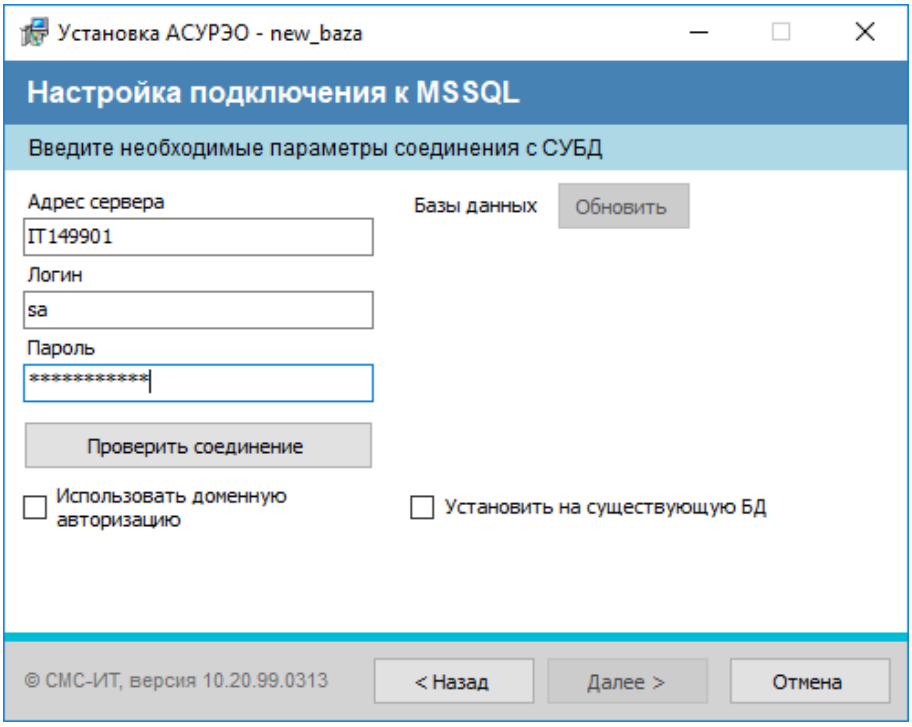

Рисунок 10.37 – Настройка соединения с сервером БД

После ввода данных необходимо проверить подключение к БД по нажатию кнопки *«Проверить соединение»*. При неудачной попытке соединения с БД появится сообщение об ошибке (Рисунок 10.38).

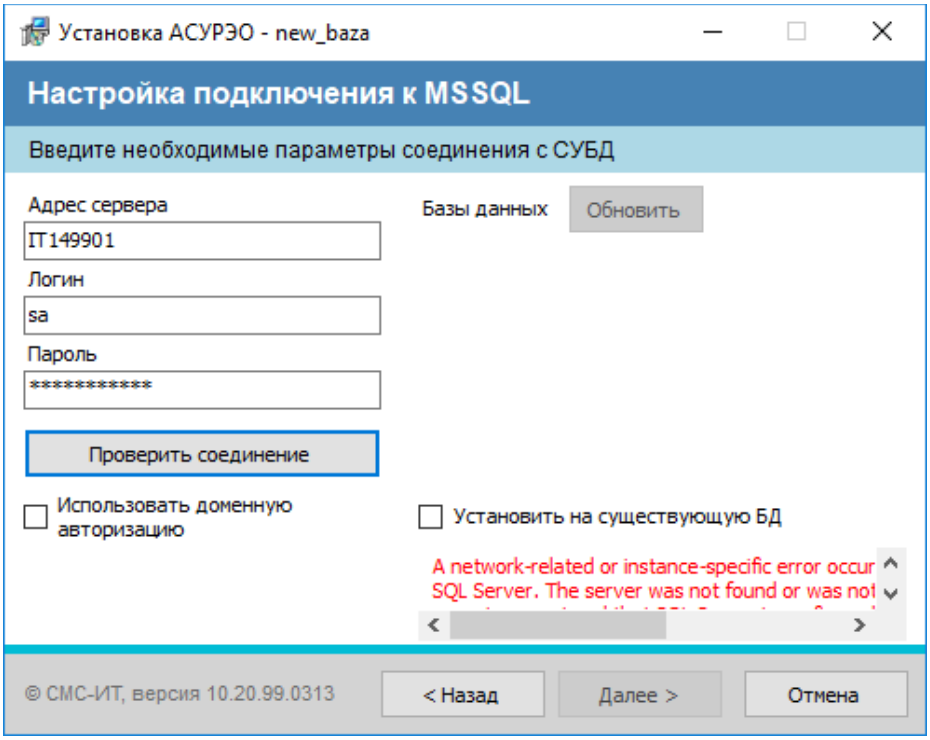

Рисунок 10.38 – Проверка соединения

Установку можно продолжить только при успешном соединении с БД.

После успешного соединения с БД необходимо выбрать БД для установки ПК из списка существующих БД на данном сервере (Рисунок 10.39). После сообщения об успешном подключении к базе данных выводится подсказка с текстом: «При установке на WSFC необходимо в поле «Адрес сервера» указать имя прослушивателя группы доступности Always-On».

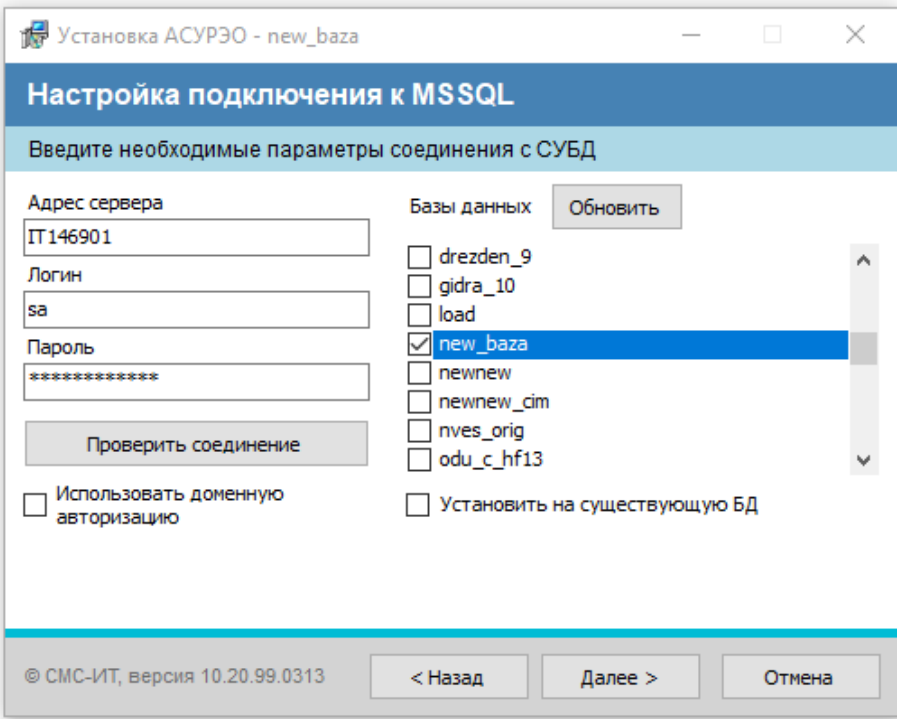

Рисунок 10.39 – Выбор базы данных для установки

БД для установки ПК создается заранее (см. раздел «10.1.1 Создание базы данных»).

Для установки экземпляра на восстановленную БД, на которой уже функционировал ПК, необходимо установить флаг *«Установить на существующую БД»*. При этом устанавливаемая версия программного комплекса должна соответствовать версии, с которой был снят дамп БД.

10.6.7 Настройка параметров ключа защиты

На следующем шаге требуется ввести идентификатор электронного ключа защиты, поставляемого вместе с ПК (Рисунок 10.40).

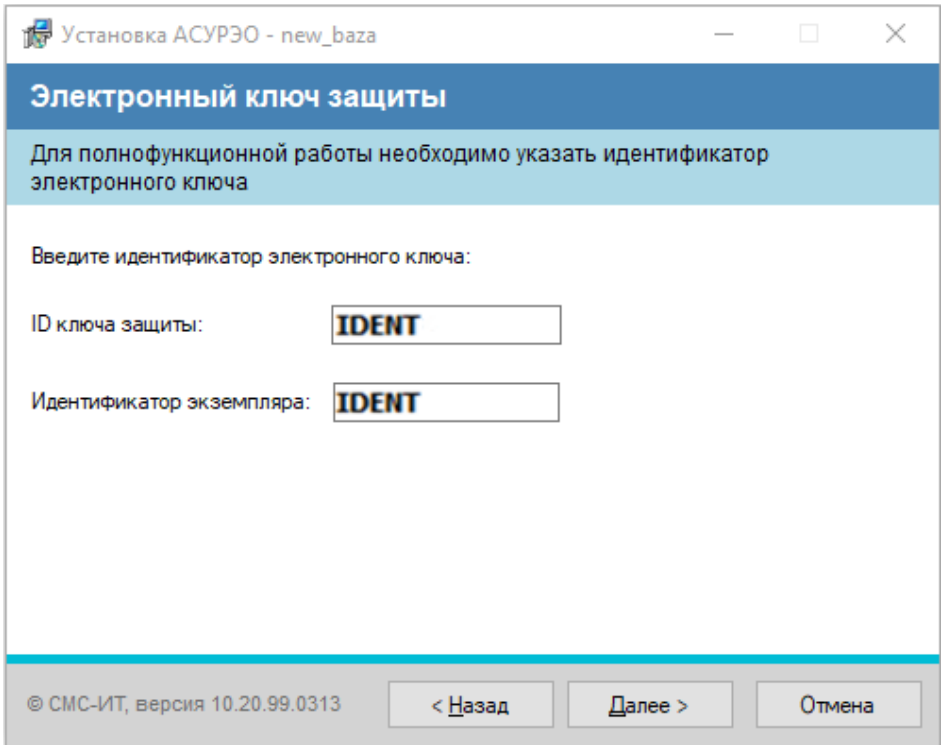

Рисунок 10.40 – Ввод идентификатора электронного ключа

10.6.8 Завершение сбора информации

На следующем шаге в окне мастера отображается вся информация, полученная программой установки (Рисунок 10.41). В случае необходимости можно вернуться на предыдущие шаги установки и внести изменения.

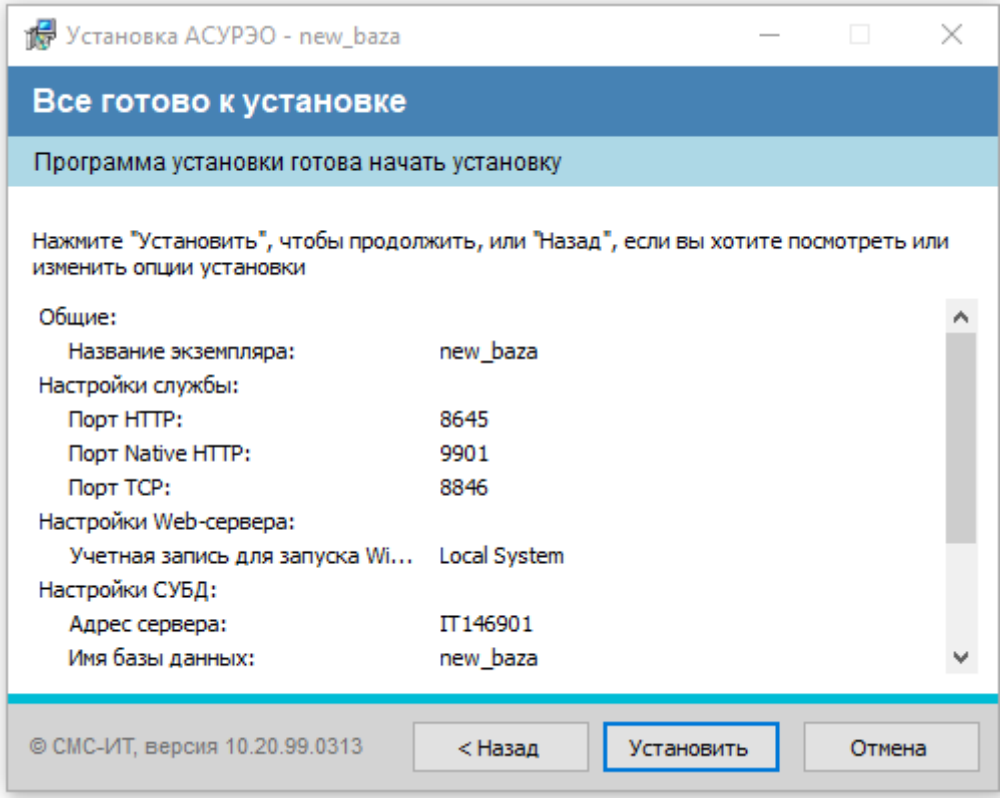

Рисунок 10.41 – Завершение сбора информации

Последним этапом является процесс копирования файлов и настройка системы (Рисунок 10.42).

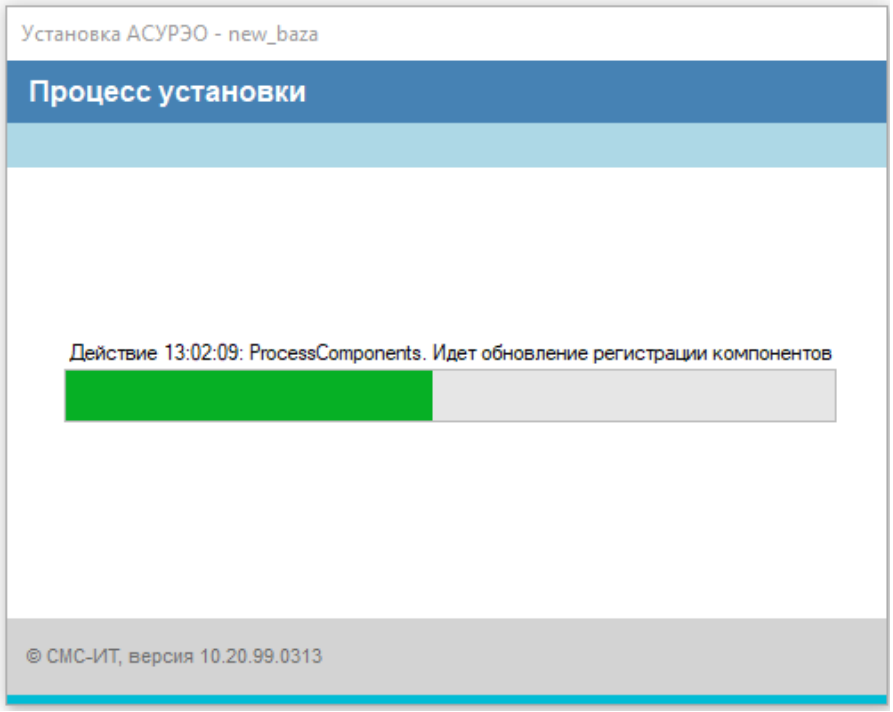

Рисунок 10.42 – Копирование файлов и настройка системы

По окончанию процесса установки появляется окно завершения мастера установки, в котором отображается адрес доступа к ПК (Рисунок 10.43). Также на рабочем столе создается ярлык доступа к ПК. Администратор приложения должен назначить Yandex.browser, как браузер по умолчанию. Созданный ярлык открывается браузером по умолчанию.

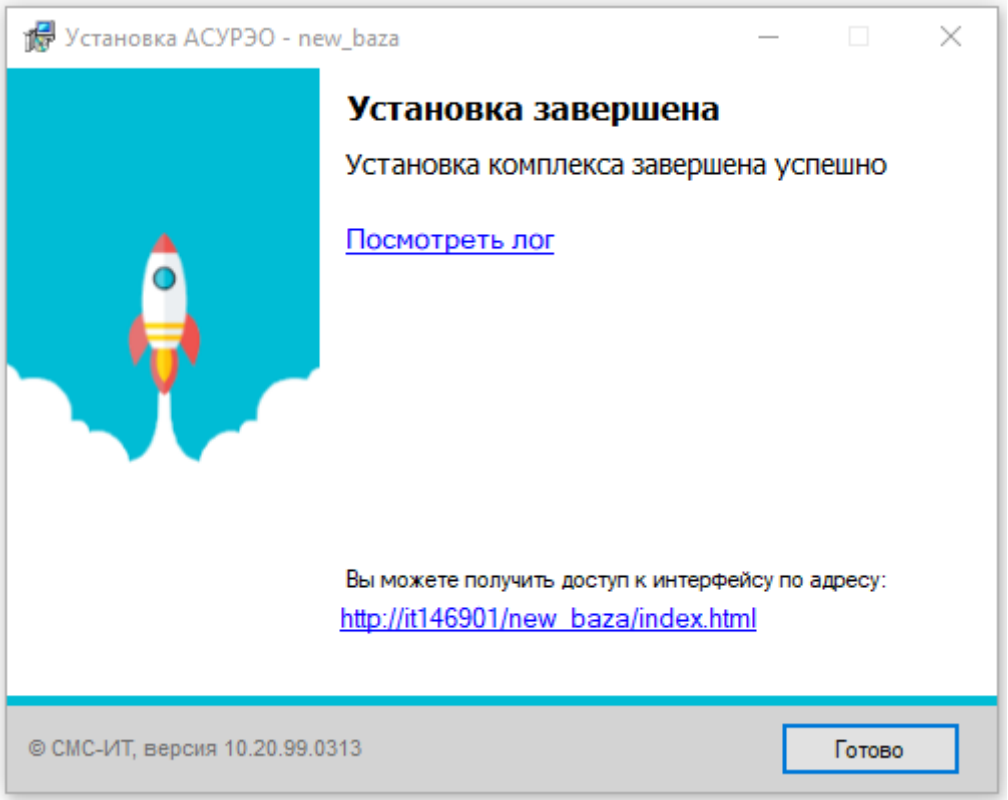

Рисунок 10.43 – Завершение установки

Для выхода из программы установки необходимо нажать на кнопку *«Готово»*.

10.7 Установка АСУРЭО на ОС семейства Linux

Установка ПК «АСУРЭО» на ОС семейства Linux осуществляется с помощью docker контейнеров. Для выполнения установки необходимо выполнить следующие действия:

1. Создать каталог. Выполнить команду: *mkdir /opt/asureo* (Рисунок 10.44).

```
root@astral:/opt# mkdir /opt/asureo
```

Рисунок 10.44 – Выполнение команды mkdir /opt/asureo

2. Скопировать в каталог /opt/asureo комплект поставки, который включает в себя:
   - docker-compose.yml файл с образами ПК «АСУРЭО» и веб-сервера nginx;
   - конфигурационные файлы zvk.ini, config.json, confighost.txt.

3. В конфигурационный файл zvk.ini внести необходимые правки в секцию подключения к СУБД [DBConnection] согласно описанию, приведенному на рисунке 10.45.

```
  GNU nano 3.2                    /opt/asureo/Zvk.ini

[Service]
SessionTimeout=5
Name=asu
DisplayName=asu
HTTPPort=8625
TCPPort=8825
NativeHTTPPort=9880
UseTCPKeepAlive=1
TCPKeepAliveProbeTime=5000
TCPKeepAliveProbeInterval=1000
ContractorLogic=1

[DBConnection]
Driver=postgres
HostName=10.3.29.187
Database=B6HF1
User_Name=sa
Password=A4E174833291
Port=5432

[DBPool]
DBPoolSize=50
DBPoolWaitTimeoutMS=3000
DBPoolCleanupDelayMinutes=5
DBPoolCleanupHangingMinutes=10
DBPoolConnectionLifeTimeHours=2

[Logger]
Level=debug
LogsFolder=C:\server\Logs
                    [ Read 63 lines (Converted from DOS format) ]
^G Помощь    ^O Записать   ^W Поиск      ^K Вырезать   ^J Выровнять  ^C ТекПозиц
^X Выход     ^R ЧитФайл    ^\ Замена     ^U Отмен. вырез ^T Словарь  ^_ К строке
```

Рисунок 10.45 – Правки в секции [DBConnection]

4. В файл конфигурации мигратора БД (config.json) внести правки подключения к СУБД (Рисунок 10.46).

```
  GNU nano 3.2                    /opt/asureo/config.json

{
  "DbType": "postgres",
  "ConnectionString": "Server=10.3.29.187;Port=5432;Database=B6HF1;User Id=sa;Password=
  "Version": "10.22.581.0530",
  "DisplayVer": "ASUREO B6 HF1",
  "ProductKey": "asu",
  "SqlRootDir": "../../_data",
  "TemplateDir": "../../_data/Templates"
}
```

Рисунок 10.46 – Правки подключения к СУБД

5. В файл конфигурации confighost.txt внести правки: изменить адрес на ip хост сервера (Рисунок 10.47).

```
  GNU nano 3.2                                                    confighost.txt

ApplicationUrl=http://192.168.242.20/SMSITLoader
Version=11.22.8308.0719
```

Рисунок 10.47 – Правки confighost.txt

6. Перейти в каталог. Выполнить команду: *cd /opt/asureo/* (Рисунок 10.48).

```
root@astral:/opt# cd /opt/asureo/
root@astral:/opt/asureo#
```

Рисунок 10.48 – Выполнение команды cd /opt/asureo/

7. Загрузить образ ПК «АСУРЭО» из файла на диске с помощью docker команды.

Выполнить команду: *docker load* (Рисунок 10.49).

```
root@astral:/opt/asureo# docker load < B6HF1.tar
3ea85cc9ded0: Loading layer  779.9MB/779.9MB
886d0ab388ae: Loading layer  35.77MB/35.77MB
9240b6f9cad7: Loading layer  180.5MB/180.5MB
c35764e588e3: Loading layer  779.9MB/779.9MB
61e84f4c92ae: Loading layer  35.77MB/35.77MB
81671f64b35f: Loading layer  180.5MB/180.5MB
c545e21f5600: Loading layer  3.032MB/3.032MB
547b32605171: Loading layer  4.608kB/4.608kB
Loaded image: zvk-linux:B6HF1
root@astral:/opt/asureo#
```

Рисунок 10.49 – Выполнение команды docker load

8. Проверить успешную загрузку образа ПК «АСУРЭО», отобразив список образов.

Выполнить команду: *docker image ls* (Рисунок 10.50).

```
root@astral:/opt/asureo# docker image ls
REPOSITORY                          TAG                 IMAGE ID            CREATED
      SIZE
dpage/pgadmin4                      latest              94c0924749b6        13 days ago
      366MB
zvk-linux                           B6HF1               269ca8c1a416        3 weeks ago
      4.4GB
```

Рисунок 10.50 – Выполнение команды docker image ls

9. Запустить контейнеры ПК «АСУРЭО» и nginx с помощью docker-compose команды.

Выполнить команду: *docker-compose up –d* (Рисунок 10.51).

```
root@astral:/opt/asureo# docker-compose  up -d
Creating webserver ... done
Creating asureo ... done
```

Рисунок 10.51 – Выполнение команды docker-compose up -d

10. Проверить успешный запуск docker контейнеров отобразив список всех активных контейнеров.

Выполнить команду: *docker ps* (Рисунок 10.52).

```
root@astral:/opt/asureo# docker ps
CONTAINER ID        IMAGE                 COMMAND                  CREATED             ST
ATUS              PORTS
 NAMES
99bab3f72d6e        zvk-linux:B6HF1       "/bin/sh -c 'cd ${mi…"   About a minute ago   Up
 About a minute   0.0.0.0:8625->8625/tcp, 0.0.0.0:8825->8825/tcp, 0.0.0.0:9880->9880/tcp
 asureo
fddc6865bfae        dpage/pgadmin4        "/entrypoint.sh"         17 hours ago         Up
 17 hours         443/tcp, 0.0.0.0:8889->80/tcp
```

Рисунок 10.52 – Выполнение команды docker ps

10.8 Настройка ПК «АСУРЭО» с помощью конфигуратора

Конфигуратор позволяет вносить изменения в конфигурации сервера приложений и сервера авторизации.

Важно! При настройке ПК «АСУРЭО» через конфигуратор необходимо осуществлять сохранение настроек на каждой вкладке конфигуратора.

Открытие конфигуратора осуществляется на стартовой странице комплекса ПК «АСУРЭО» по нажатию на пункт «Конфигуратор» (Рисунок 10.53).

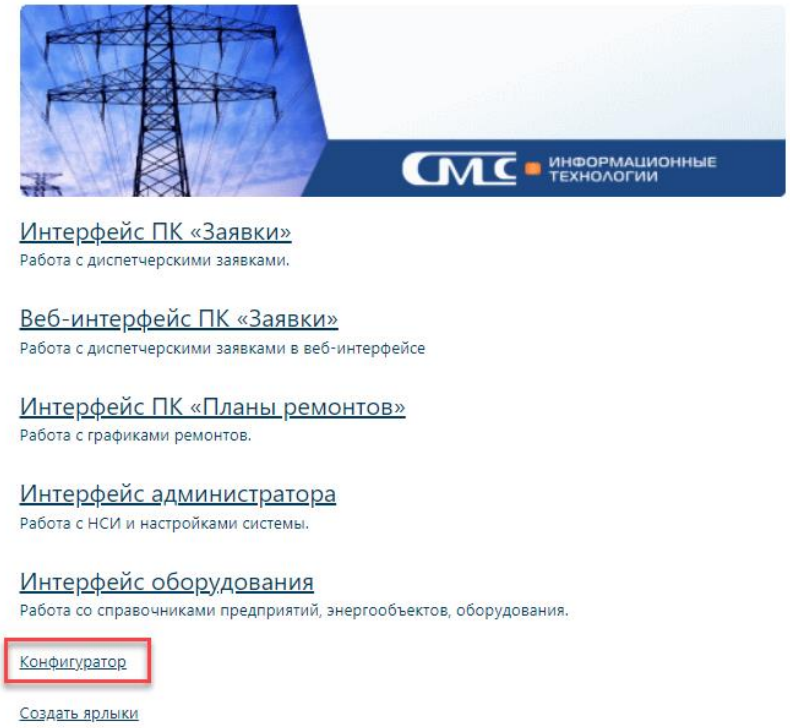

Рисунок 10.53 – Открытие конфигуратора

После перехода по ссылке на экране появится окно авторизации. Пользователю необходимо ввести стандартные логин и пароль для авторизации (Логин: admin Пароль: DefaultPassword123!).

При первом входе система попросит Вас сменить пароль. Требования к паролю следующие:

- не меньше 10 символов;
- символы должны быть в нижнем и верхнем регистре;
- должна быть одна цифра и один спец. символ.

При необходимости смена пароля осуществляется в разделе «Доп.настройки» (см. раздел «10.8.1 Дополнительные настройки») по нажатию кнопки «Сменить пароль». После нажатия кнопки открывается окно «Смена пароля», где необходимо указать старый и новый пароли (Рисунок 10.54). Данные логин и пароль необходимо запомнить, так как в дальнейшем они должны использоваться пользователем для авторизации в конфигураторе.

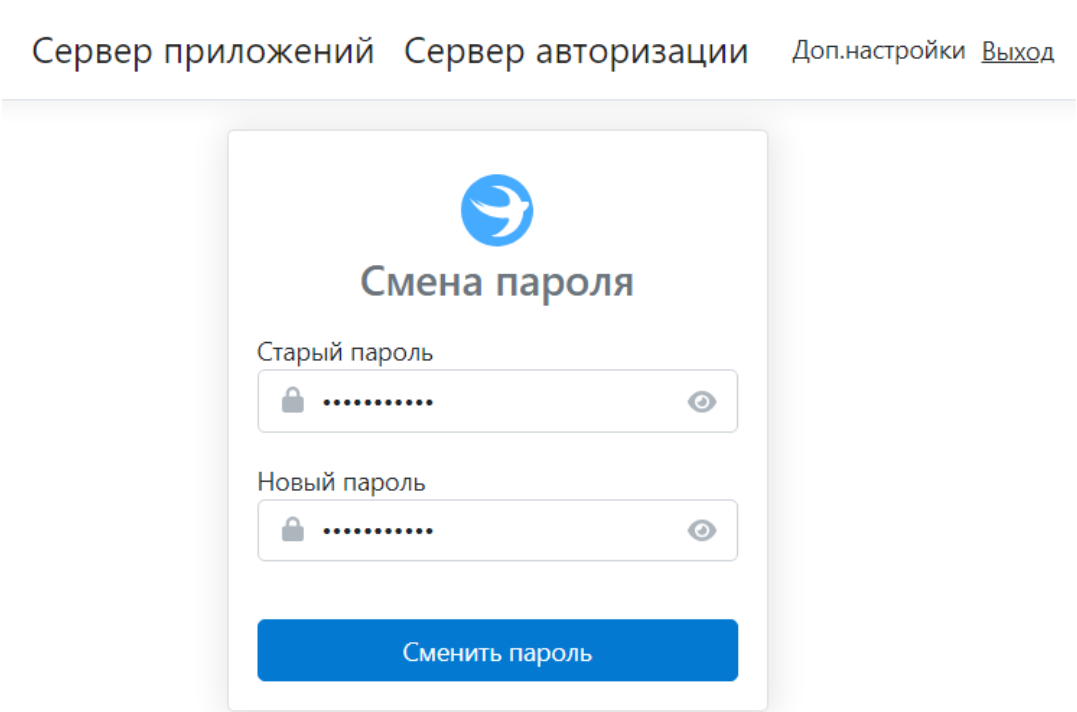

Рисунок 10.54 – Окно «Смена пароля»

10.8.1 Дополнительные настройки

Для настройки веб-конфигуратора необходимо перейти в раздел «Доп.настройки», где отображаются следующие параметры (Рисунок 10.55):

- «Уровень логирования» – параметр настройки уровня логирования. По умолчанию выбран – «Information».
- «Сервер авторизации» – параметр, указывающий пути к файлу конфигурации внутри docker контейнера (путь по умолчанию изменять не нужно).
- «Сервер приложений» – параметр, указывающий путь к файлу конфигурации внутри docker контейнера (путь по умолчанию изменять не нужно).
- «Сервер приложений Delphi» – параметр, указывающий путь к файлу конфигурации внутри docker контейнера (путь по умолчанию изменять не нужно).
- «Имя контейнера с Delphi заявками» – имя docker контейнера. Указанный в данном параметре контейнер перезапускается по нажатию на кнопку «Перезапустить контейнеры и сервисы».

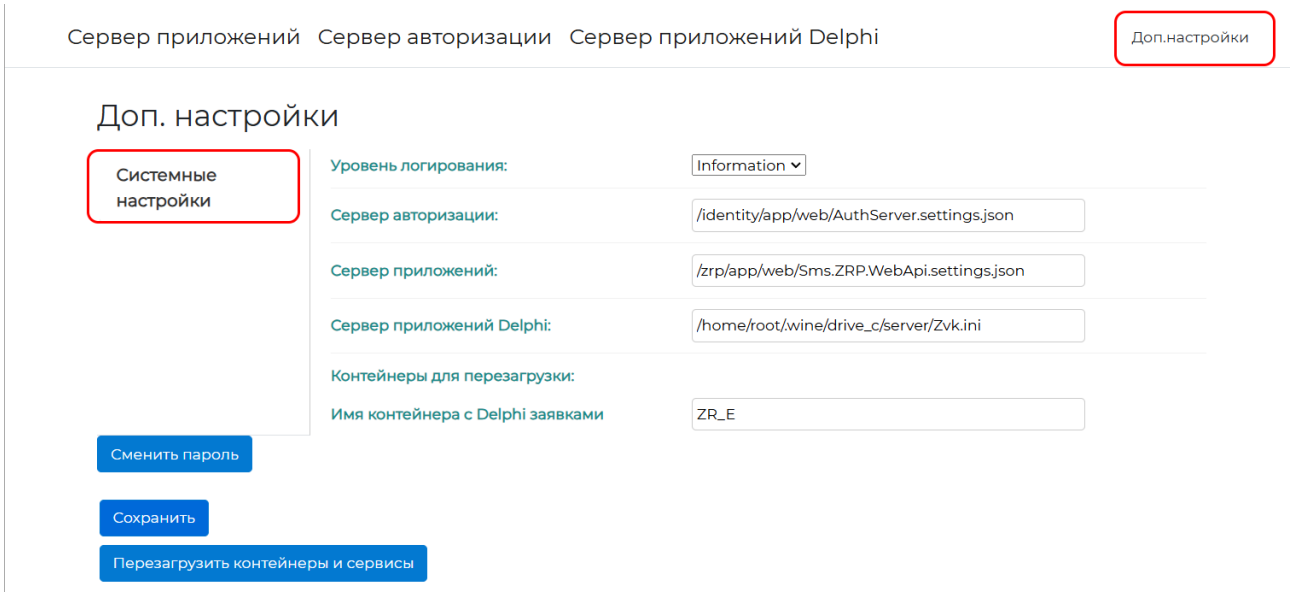

Рисунок 10.55 – Настройка веб-конфигуратора

Для сохранения изменений необходимо нажать на кнопку *«Сохранить»*.

10.8.2 Настройка Сервера приложений

После изменения пароля откроется страница настроек Сервера приложений.

В разделе «Системные настройки» сервера приложений настраивается подключение к БД. При установке ПК «АСУРЭО» необходимо заполнить следующие параметры:

- «Разрешенные хосты» – указывается фильтр допустимых имен хоста, которые может иметь сервер.
- «Провайдер БД» – указывается тип системы управления базой данных (СУБД). Необходимо выбрать «PostgreSQL».
- «Подключение к БД» – указываются параметры настройки подключения к БД. В зависимости от выбранного параметра «Провайдер БД» будет использована соответствующая строка подключения.

При необходимости пользователь может включить логирование для настроек к БД, установив соответствующие флаги (Рисунок 10.56). По умолчанию логирование выключено.

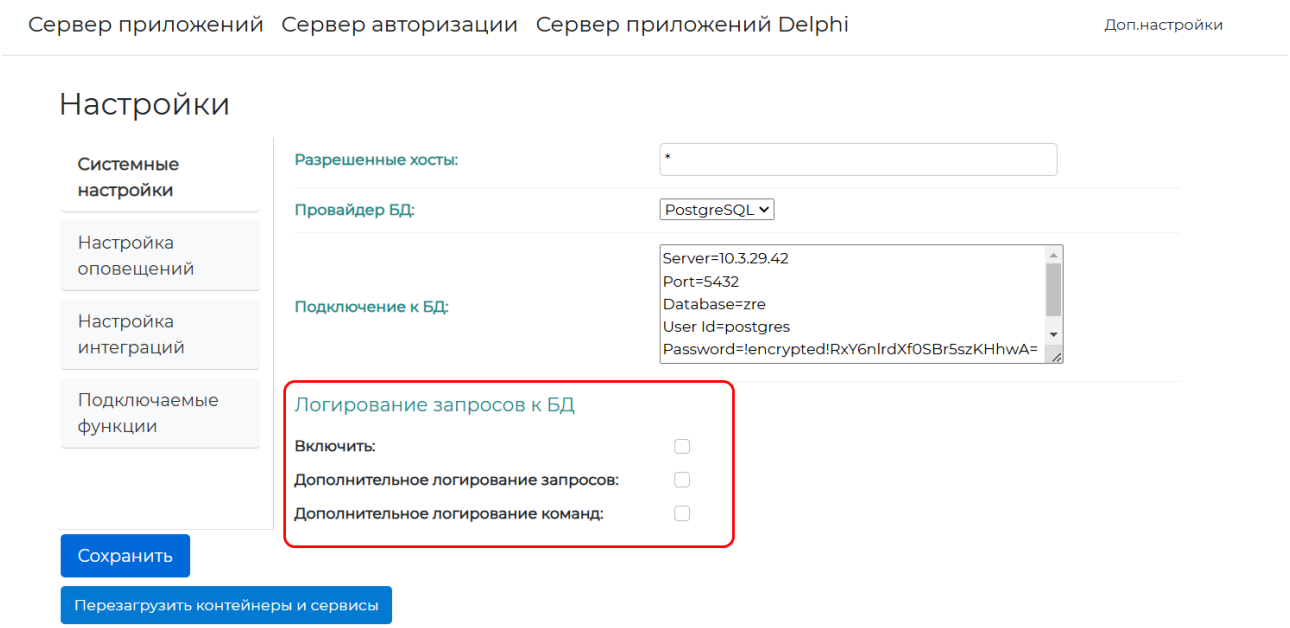

Рисунок 10.56 – Системные настройки сервера приложений

В разделе «Настройка оповещений» настраиваются оповещения о заявках и пользовательские оповещения. Параметры настройки оповещений задаются в виде стандартного Cron – выражения. По умолчанию установлено значение с периодом обновления в 1 минуту - */1 * * * * (Рисунок 10.57).

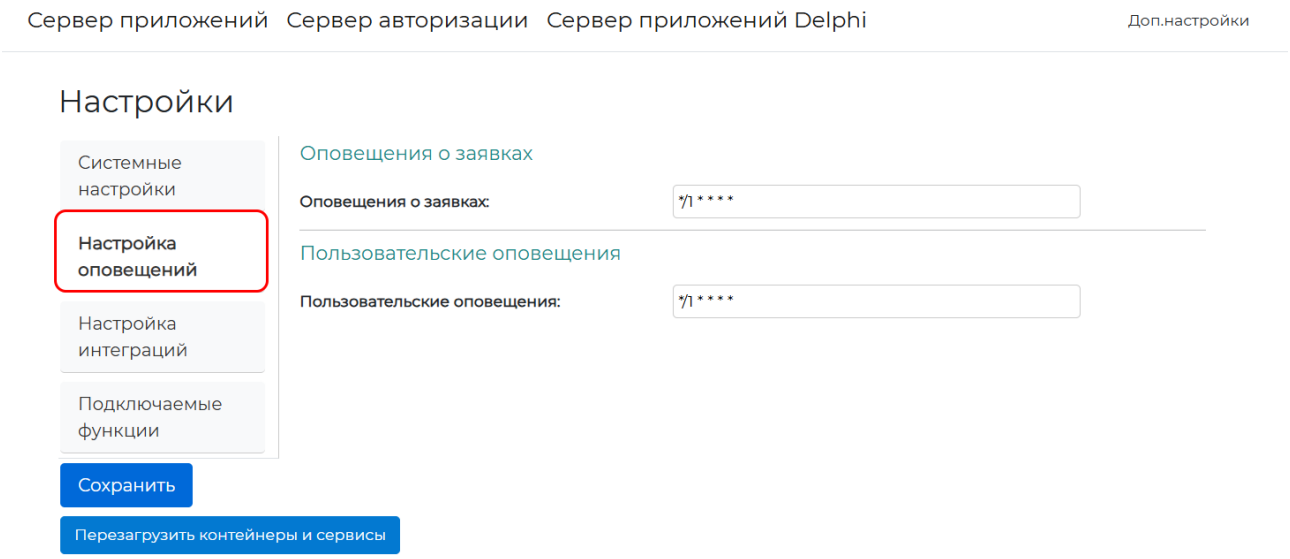

Рисунок 10.57 – Настройка оповещений

Для смены адреса аутентификации пользователю необходимо зайти в раздел «Настройка интеграции» и в поле «Адрес аутентификации» указать адрес в формате:

http://<container_name>:5001, где <container_name> – название контейнера; порт 5001 – порт, по умолчанию используемый внутри docker для сервера авторизации.

Для настройки сервиса интеграции с сервером приложений Delphi необходимо установить флаги «Включить интеграцию с сервером приложений Delphi» и в поле «URL к интеграции» указать адрес интеграции с SOAP в формате http://имя сервера:http-порт/SOAP, где http-порт – порт из zvk.ini. Использование протокола HTTPS не допускается! (Рисунок 10.58).

Флаги «Проксировать запросы создания/редактирования заявки в сервер приложений Delphi» и «Проксировать запросы предопределенных маршрутов в сервер приложений Delphi» не должны быть установлены. Установка может потребоваться только при возникновении критичных ошибок в функционале создания/редактирования заявки и предопределенных маршрутов на сервере приложений ЗР.Net.

Для настройки взаимодействия с внешними сервисами необходимо установить флаг «Включено» в разделе «Настройка взаимодействия с внешними сервисами» и установить флаг «Активно» для etcd (Рисунок 10.58).

Для настройки интеграции через etcd также необходимо в поле «Строка подключения» указать адрес подключения в формате: http://имя сервера:порт и в поле «Группа клиентов» указать группу.

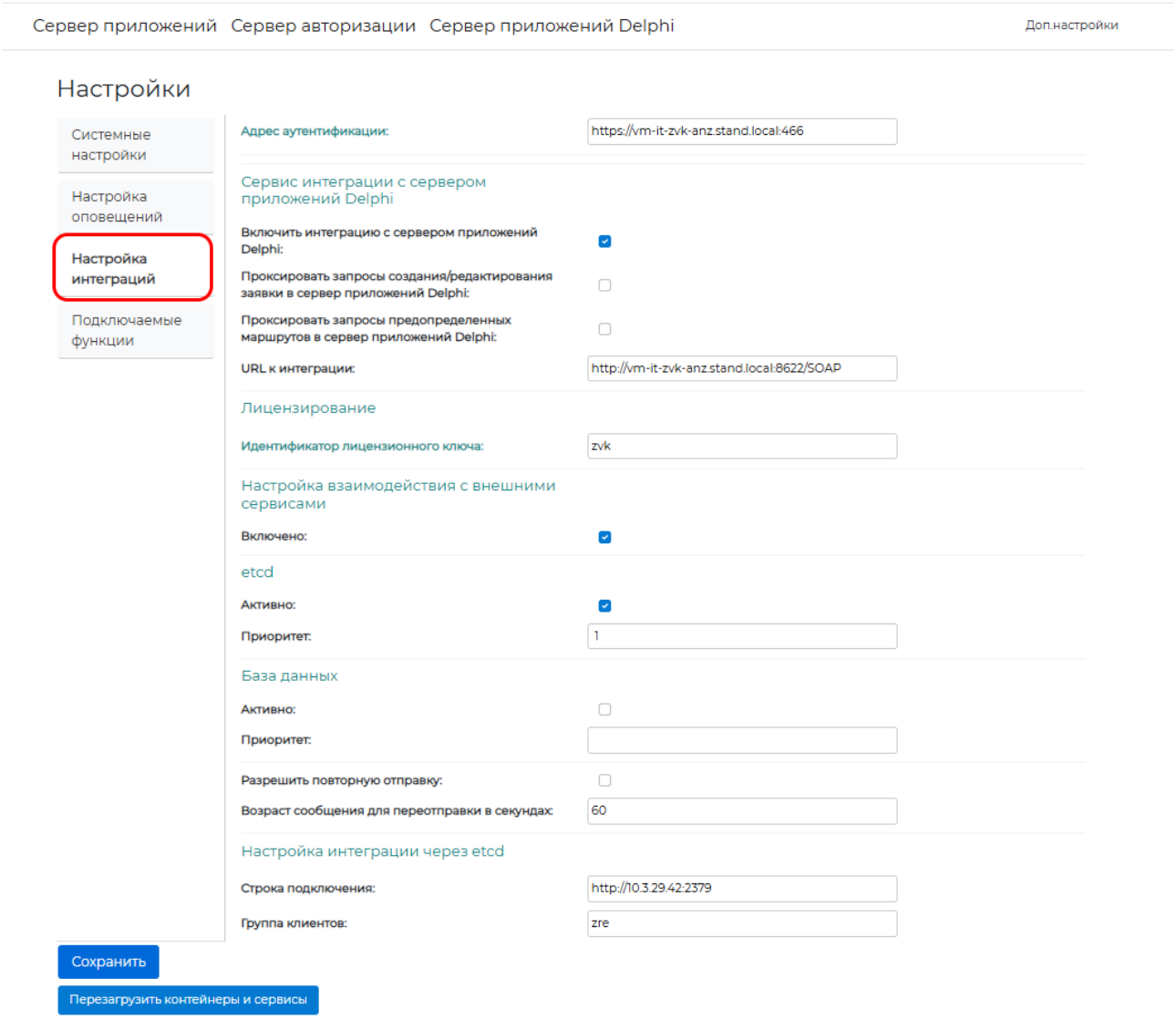

Рисунок 10.58 – Настройка интеграций

При включении etcd изменяются не только значения в конфигурационном файле sms.ZRP.WebApi.settings.json, но и значения в файле zvk.ini.

В конфигурационном файле sms.ZRP.WebApi.settings.json меняются следующие параметры:

"EtcdEventWatchSettings": {

"Enable": false,

"ConnectionString": "http://localhost:2379"

},

В конфигурационном файле zvk.ini меняются следующие параметры:

Пример:

```
[MessageServerConnection]
ServerType=ETCD
Host=localhost
Port=2379
GroupID=test1
ConnectTimeout=1
ReadTimeout=1
MessageEncryption=0
PingIntervalSec=60
UseResendExpired=0
ResendExpiredIntervalSec=60
UseEtcdChannel=1
UseDatabaseChannel=0
```

Etcd не должен влиять на правильную работу ЗР.Net. В связи с этим, реализован резервный канал через базу данных. Для работы резервного канала необходимо в разделе «База данных» установить флаг «Активно».

Для каждого канала необходимо задать приоритеты в поле «Приоритет» для etcd и базы данных в виде целого положительного числа, где чем меньше число, тем выше приоритет. Рекомендуется устанавливать высший приоритет для etcd. Если приоритет не задан, для одного из каналов, то он будет считаться высшим. Если приоритет не задан для обоих каналов, то установка приоритета осуществляется в алфавитном порядке от A-Z (база данных будет приоритет выше).

Обязательно необходимо установить флаг «Разрешить повторную отправку» при настройке резервного канала.

В разделе «Подключаемые функции» настраивается отображение сообщений СУПА в Журнале сообщений (Рисунок 10.59). При установке флага «Включить отображение сообщений СУПА в ЖС» в Журнале сообщений становится доступным отображение сообщений СУПА. По умолчанию данный флаг не установлен. Данный флаг заполняет настройку UseSapMsg в конфигурационном файле appsettings.json.

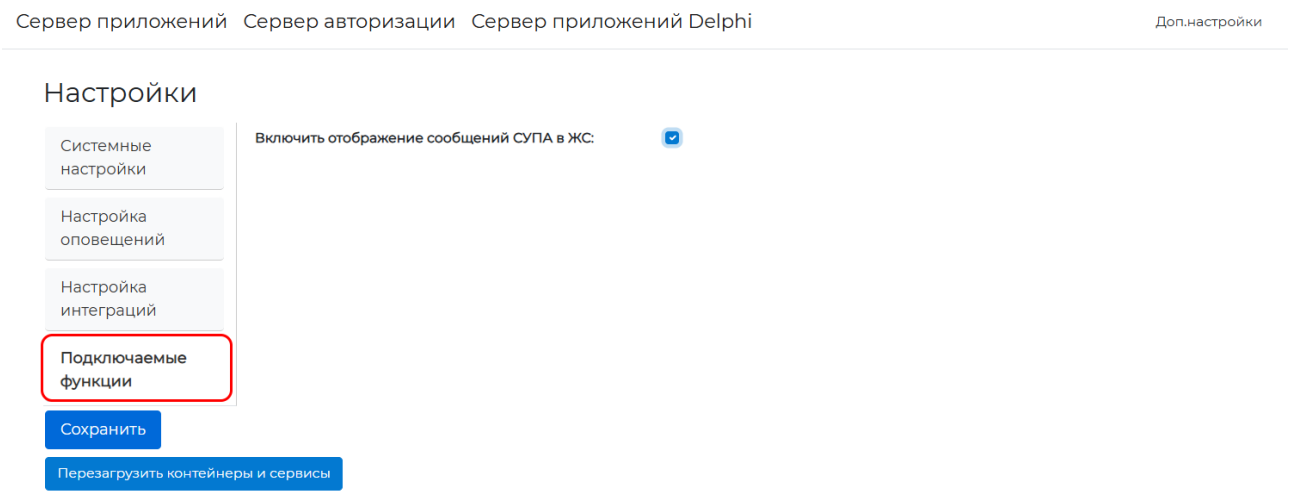

Рисунок 10.59 – Настройка подключаемых функций

После внесения изменений необходимо нажать кнопку «Сохранить».

10.8.3 Настройка Сервера авторизации

Для настройки сервера авторизации необходимо перейти в раздел «Системные настройки» (Рисунок 10.60). В данном разделе отображаются следующие параметры:

- «Разрешенные хосты» – указывается фильтр допустимых имен хоста, которые может иметь сервер.
- «NT Аутентификация» – признак использования доменной аутентификации. По умолчанию не установлен.
- «Домен» – домен, в котором находится KDC (Key Distribution Center).
- «AccessTokenLifetime» – параметр задает время жизни токена доступа к клиенту. По умолчанию указано 3600.
- «AllowedCorsOrigins» – параметр задает хосты, с которых будет доступен переадресация на сервер авторизации. Доступно указание несколько данных параметров в конфигураторе.

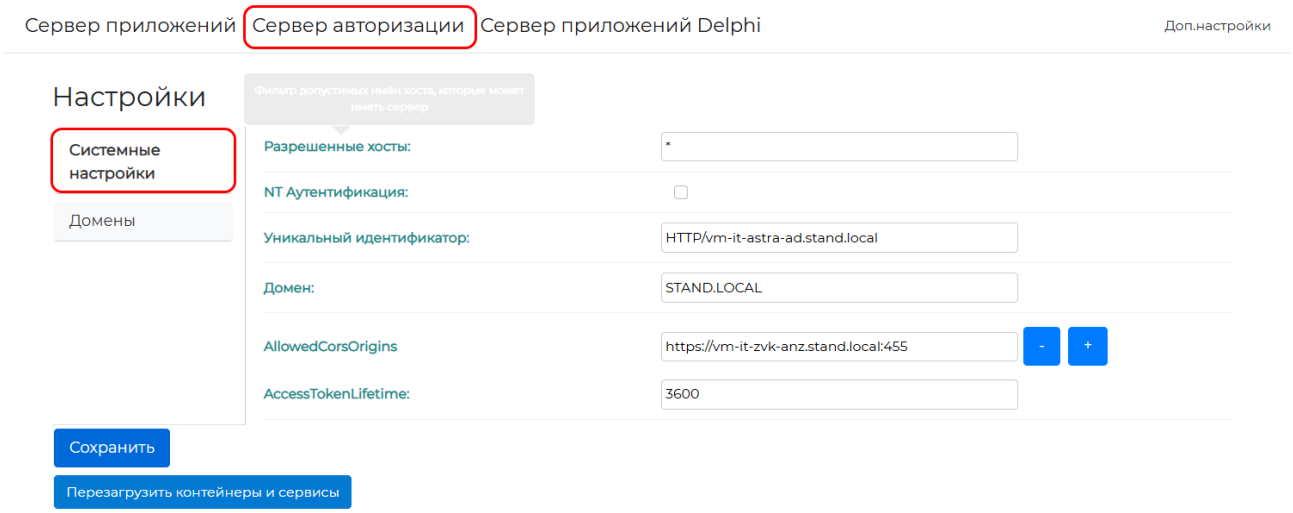

Рисунок 10.60 – Настройка сервера авторизации

В разделе «Домены» настраивается доменная авторизация (Рисунок 10.61). При осуществлении авторизации с нескольких доменов необходимо указать имена всех доменов и их возможные алиасы (псевдонимы).

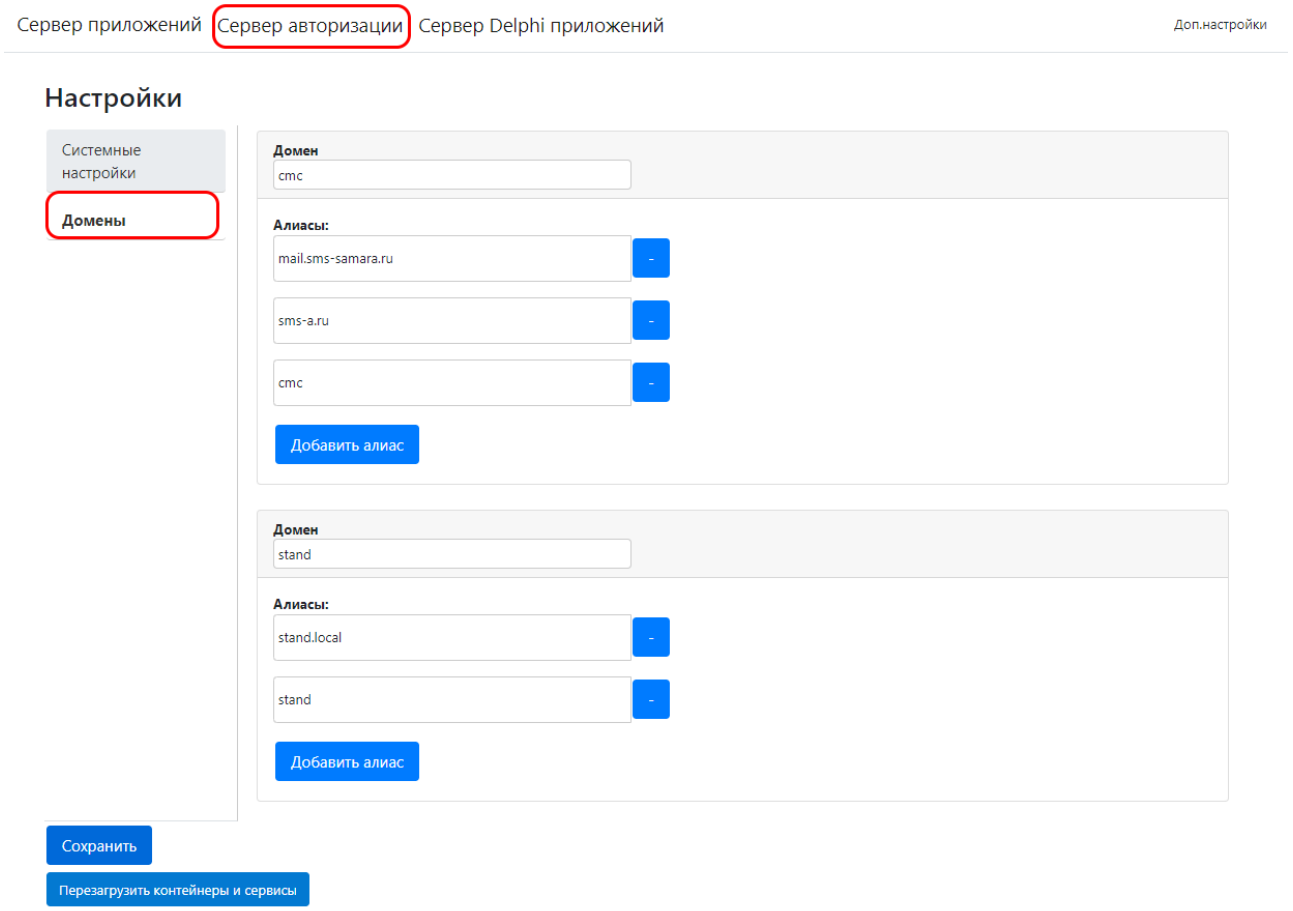

Рисунок 10.61 – Настройка доменной авторизации

10.8.4 Настройка Сервера Delphi приложений

Для настройки сервера Delphi приложений необходимо перейти в раздел «Системные настройки» (Рисунок 10.62). В данном разделе отображаются следующие параметры:

- «Таймаут сессии на веб-сервере» – указывается время жизни сессии с момента последнего обновления. По умолчанию указано – 5 минут.
- «Имя экземпляра» – указывается имя службы при ее установке.
- «Отображаемое имя экземпляра» – указывается отображаемое наименование службы.
- «HTTPPort экземпляра» – указывается Super HTTP-порт сервера приложений.
- «TCPPort экземпляра» – указывается TCP-порт сервера приложений.
- «NativeHTTPPort экземпляра» – указывается HTTP-порт, предназначенный только для первоначального подключения сервера приложений и клиента с последующим переходом на работу по HTTPPort или, что предпочтительно, по TCPPort.
- «UseTCPKeepAlive» – использовать механизм (по умолчанию не используется).
- «TCPKeepAliveProbeTime» – указывается таймаут перед отправкой отправки первого зондирующего TCPKeepAlive-пакета. По умолчанию 5000 мсек.
- «TCPKeepAliveProbeInterval» – указывается период отправки зондирующих TCPKeepAlive-пакетов. По умолчанию 1000 мсек.

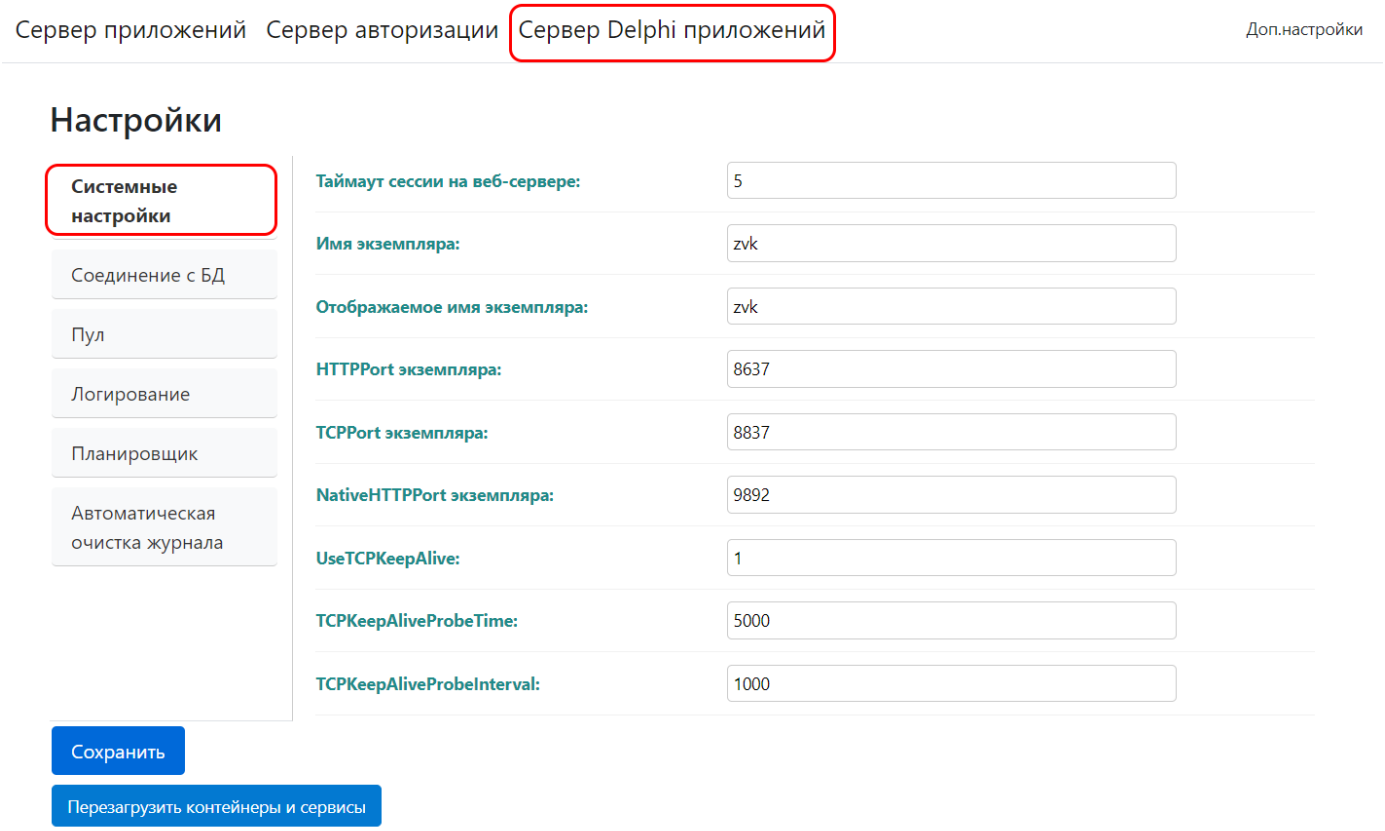

Рисунок 10.62 – Системные настройки сервера Delphi приложений

Для настройки соединения с БД необходимо перейти в раздел «Соединение с БД», где отображаются следующие параметры (Рисунок 10.63):

- «Провайдер БД» – указывается используемый драйвер БД.
- «HostName» – указывается сервер БД.
- «Наименование базы данных» – указывается наименование БД.
- «Логин пользователя в СУБД» – указывается логин пользователя в СУБД.
- «Пароль» – указывается пароль пользователя БД.
- «Порт СУБД» – если необходимо указывается номер порта для соединения с БД.

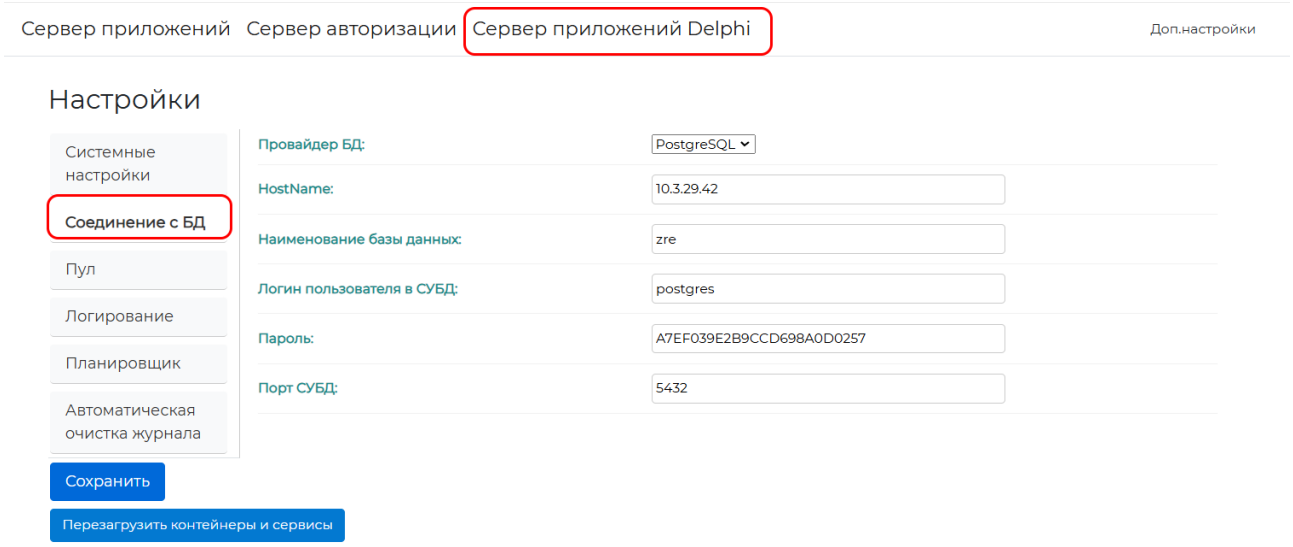

Рисунок 10.63 – Настройки соединения с БД

Для настройки пула необходимо перейти в раздел «Пул», где отображаются следующие параметры (Рисунок 10.64):

- «Размер пула» – указывается размер пула (макс. количество соединений в пуле).
- «Время ожидания при получении соединения» – указывается время ожидания при получении соединения в миллисекундах.
- «Время удаления из пула свободных соединений» – указывается время удаления из пула свободных соединений.
- «Время принудительного удаления из пула» – указывается время принудительного удаления из пула занятых (взятых из пула) соединений.
- «Время жизни соединения в пуле» – указывается время жизни соединения в пуле с момента его создания в часах = время жизни сессии в БД (проверяется при возврате соединения в пул).

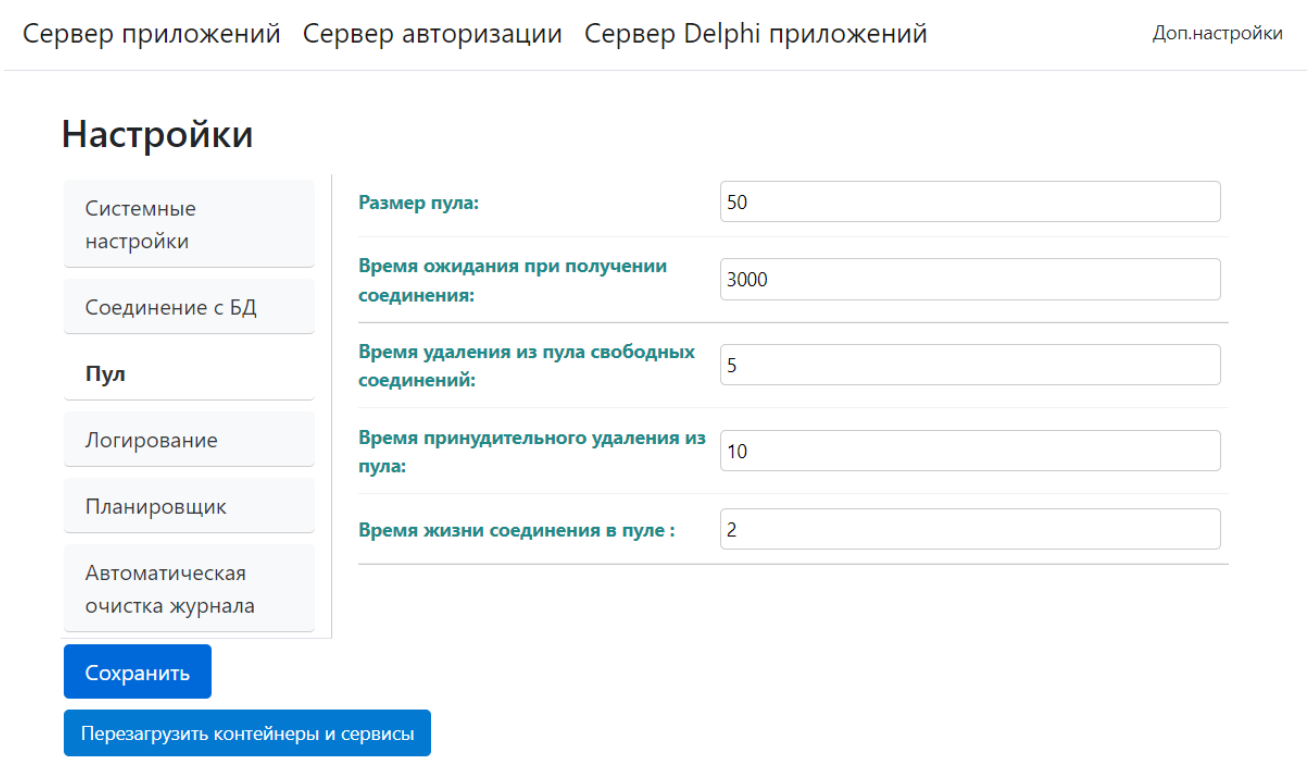

Рисунок 10.64 – Настройки пула

Для настройки логирования необходимо перейти в раздел «Логирование». В данном разделе отображаются следующие параметры:

- «Уровень логирования» – указывается нижний уровень сообщений, попадающих в лог: debug, info, warm, error, fatal.
- «Папка записи логов» – указывается путь к папке записи логов.
- «Формат лога» – указывается формат при формировании записи лога. При отсутствии параметра используется формат по умолчанию.
- «Включить логирование вызова веб-методов в основной лог» – для включения логирования вызова веб-методов в основной лог необходимо установить флаг.
- «Исключить из логирования методы» – при включенном логировании исключает из логируемых методов те, что указаны здесь через запятую (например, метод Ping).
- «IntegrationWebCalls.Level» – включает информацию о вызовах методов сервисов IntegrationService и RPIntegrationService.
- «InternalWebCalls.Level» – включает информацию о вызовах внутренних методов ЗРП.

- «InternalWebCalls.FileName» – включает информацию о вызовах внутренних методов ЗР.
- «ShedulerTasks.FileName» – включает логирование расширенной информации по работе задач планировщика. По умолчанию присутствует в zvk.ini в формате ShedulerTasks.FileName=ShedulerTasks.

Для настройки планировщика необходимо перейти в раздел «Планировщик», где отображаются следующие параметры (Рисунок 10.65):

- «Частота опроса планировщика» – указывается частота опроса планировщика в миллисекундах.
- «Пауза перед первым запуском» – указывается пауза перед первым запуском в миллисекундах.

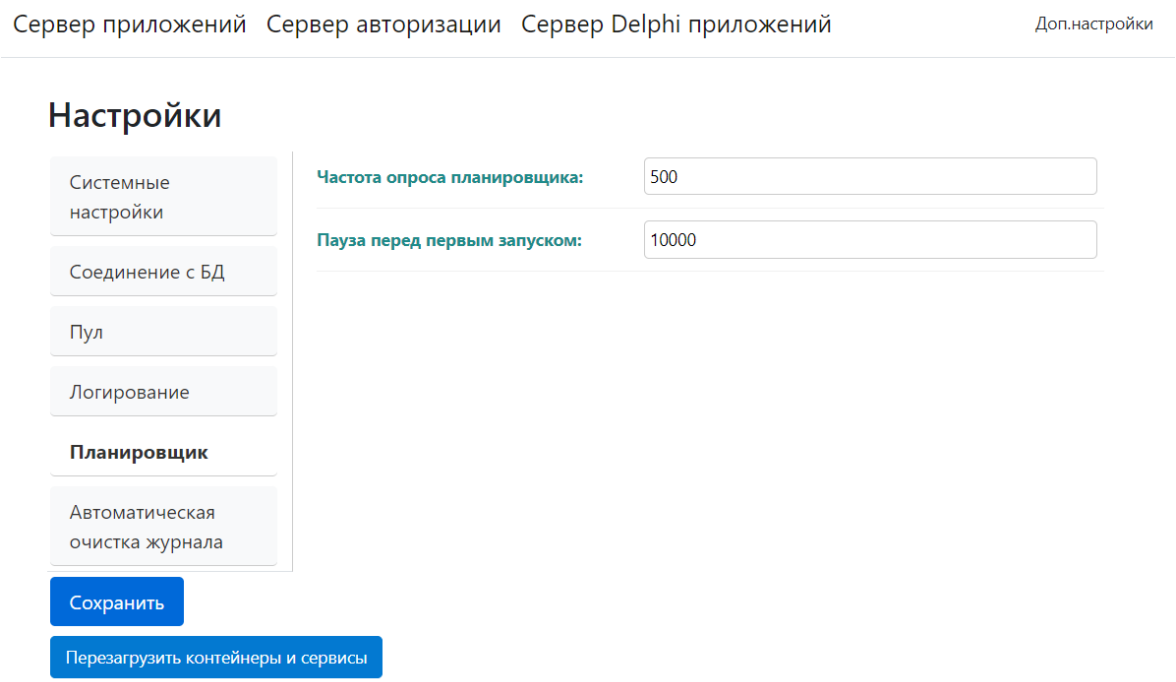

Рисунок 10.65 – Настройка планировщика

Для настройки автоматической очистки журнала необходимо перейти в раздел «Автоматическая очистка журнала», где отображаются следующие параметры (Рисунок 10.66):

- «Задача отправки сообщений» – указывается задача отправки сообщений.
- «Задача приема сообщений» – указывается задача приема сообщений.
- «Задача проверки квитанций» – указывается задача проверки квитанций.

- «Задача архивации очистки данных и автоудаления диспетчерских заявок» – указывается задача архивации очистки данных и автоудаления диспетчерских заявок.
- «Архивации заявок по сроку давности с интервалом» – указывается параметр, предназначенный для архивации заявок по сроку давности с указанным интервалом (846400 сек = 1 сутки) и временем запуска (01:30).

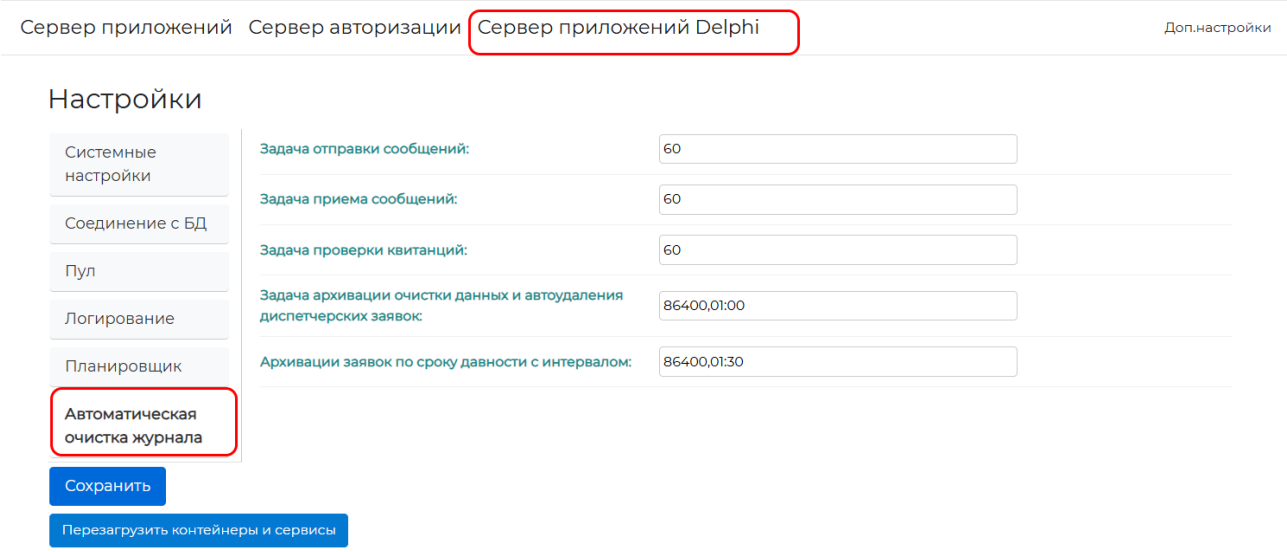

Рисунок 10.66 – Настройка автоматической очистки журнала

После внесения изменений необходимо нажать кнопку *«Сохранить»*.

Примечание. При нажатии на кнопку «Сохранить» в конфигурационный файл автоматически добавится параметр InstanceName.

Важно. Все изменения применяются только после перезапуска контейнеров, поэтому пользователю необходимо нажать на кнопку *«Перезагрузить контейнеры и сервисы»*.

По нажатию кнопки *«Перезагрузить контейнеры и сервисы»* выполняется перезагрузка Docker-контейнера, в котором работает Сервер приложений Delphi заявок, а также перезапуск Сервера приложений Web заявок и Сервера авторизации.

10.9 Описание параметров файла web.config

После успешной установки или обновления ПК на web-сервере IIS версии 7 и выше в папке «C:\Program Files (x86)\ZVK\<название экземпляра>» будет создан файл web.config (конфигурационный файл модуля rewrite).

Пример:

```
<rule name="Rewrite SuperHTTP" stopProcessing="true">
  …
<action type="Rewrite" url=http://test-pc:8621 {R:2}"
redirectType="Permanent" /> здесь указывается HTTPPort
</rule>
<rule name="Rewrite Native" stopProcessing="true">
<match url="^appsrv(/proxy.dll)?(,*)$"/>
<action type="Rewrite" url=http://test-pc:9877 {R:2}"
redirectType="Permanent" /> здесь указывается NativeHTTPPort
</rule>
```

В конфигурационном файле web.config содержится информация о настройках переадресации запросов с веб-сервера IIS на порты сервера приложений: NativeHTTP и HTTPPort.

Внимание! Файл web.config создается только на веб-сервере IIS версии 7 и выше.

Для редактирования файл web.config открывается любым текстовым редактором и представляет собой по структуре xml файл.

При изменении портов в файле zvk.ini также следует изменить и конфигурационный файл web.config. В примере полужирным шрифтом выделены строки, которые необходимо изменить.

10.10 Описание параметров файла zvk.ini

После успешного завершения процесса установки ПК «АСУРЭО» на ОС MS Windows в папке «C:\Program Files (x86)\ZVK\<название экземпляра>\server» будет создан файл zvk.ini.

Файл конфигурации zvk.ini ПК «АСУРЭО» на ОС семейства Linux монтируется с хоста сервера в docker контейнер. Файл располагается по адресу /opt/asureo/zvk.ini. При необходимости его параметры можно скорректировать.

Пример:

```
[Service]
SessionTimeout=5
Name=TEST
DisplayName=TEST
HTTPPort=8621
TCPPort=8822
ContractorLogic=1
NativeHTTPPort=9877
ServerThreadCount=64
SessionManager=DB
```

```
IsTestInstance=1
AdditionalTitle=(ПОЛИГОН)

[DBConnection]
Driver=mssql
HostName=book\SQLEXPRESS
Database=test
User_Name=zvk
Password=zvk
RowsetSize=32768
ForcedDisconnectDelay=15

[DBPool]
DBPoolSize=50
DBPoolMinReserved=10
DBPoolMaxReserved=20
DBPoolWaitTimeoutMS=3000
DBPoolCleanupDelayMinutes=5
DBPoolCleanupHangingMinutes=10
DBPoolConnectionLifeTimeHours=2

[Logger]
; Допустимы следующие уровни
; debug, info, warn, error, fatal
Level=debug
LogsFolder=D:\zvk\ZVK\baza6_Odu_Sib\Logs\
IntegrationWebCalls.Level=debug
IntegrationWebCalls.FileName=WebCalls
InternalWebCalls.Level=debug
InternalWebCalls.FileName=WebCalls
RPAdditional.Level=debug
RPAdditional.FileName=Additional
TransportManager.Level=debug
TransportManager.FileName= TransportManager
LogRequests.Level=debug
LogRequests.FileName=Requests
DBRouterLog.Level=debug
DBRouterLog.FileName=RouterLog
ExcludedLogWebMethods=Ping,GetNotify

[Scheduler]
; частота опроса планировщика (милисек)
Duration=500
; пауза перед первым запуском (милисек)
StartPause=10000
; необязательное значение таймаута (милисек) ожидания завершения задач
; в диапазоне 0..2147483647 (максимум примерно 24 суток) или -1 (INFINITE),
; отсутствие параметра или пустое его значение трактуется как -1
TaskTerminationWaitTimeout=-1

[SchedulerTasks]
; параметры для задач:
; 1 значение - интервал между выполнениями задачи в секундах (1 сутки = 86400 сек)
; 2 значение (может быть опущено) - время первого запуска задачи в формате hh:mm
OutTransportTask=60
InTransportTask=60
CheckAckTimeoutTask=60
ClearDataTask=86400,01:00
RPTask=86400,15:00
```

```
RPLimitDay=30
ArchiveZVKTask=86400,01:30

[Key]
Number=27157AA6
Instance=asu

[Transport]
SendTimeout=180
ReceiveTimeout=180

[DTEK_INTEGRATION]
URL=http://&lt;client_name&gt;:&lt;clientPort&gt;/?command=goto&point_id=&lt;componentAlias

[AdditionalFunctions]
UseInsideReglament=1
CalculateChangeInitiator=1
ConsiderChilds=1
IsRepairDiffActive=1
ShowAllManagementDevices=1
FixedPowerObjectList=1
IsAdjustmentDateEditable=1
DeviceDescrDefaultPO=1
AutoNotification=Русгидро
AutoNotificationSheduleType=rptENRG,rptELT
CreateBindRepairs=1
CopyRepairs=1
CommonScheduleforAgreee=1
ForAgreeAcceptInReglament=1
CachedClientVersionCount = 6
ScheduleCreateWarning=1
EnableSendOpenCloseMsgFromAnyLevel=1
LinkedDeviceZVK=1
DisableDelegationLastSign=1
AutoTransferNCI=1
ShowYearDisconnectedZVK=1
AutoTakeDeviceVisibility=1
IsEmergencyReadiness=1
ShowResponsibleUser=1
ScheduleAgreeComparison=1
ChangePassword=1
FinesForecast=1
CheckForDuplicateInstance=1
```

В секции **[Service]** указываются следующие параметры:

- SessionTimeout – время жизни сессии с момента последнего обновления, минуты. *Примечание.* Если пользователь закрывает окно браузера, без нажатия кнопки «Выход», то сессия пользователя остается до применения задачи автоматической очистки на сервере, как правило это 5 минут, или пока администратор не удалит её в списке;
- Name – имя службы при ее установке;
- DisplayName – отображаемое наименование службы;
- HTTPPort – Super HTTP – порт сервера приложений;

- TCPPort – TCP – порт сервера приложений;
- ContractorLogic – включение логики работы с контрагентами (0 или 1). По умолчанию значение параметра равно 1;
- NativeHTTPPort – HTTP-порт, предназначенный только для первоначального подключения сервера приложений и клиента с последующим переходом на работу по HTTPPort или, что предпочтительно, по TCPPort;
- ServerThreadCount – размер пула рабочих нитей (максимальное кол-во кодовых потоков, обслуживающих клиентские запросы), по умолчанию 20, в высоконагруженной среде с большим кол-вом одновременно активных пользователей увеличение этого значения способствует ускорению реакции сервера на одновременные клиентские запросы, максимально-возможный размер ограничен ресурсами Windows-процесса, в Win32 для комфортного параллельного обслуживания до 50 активных пользователей рекомендуемое значение – 64;
- SessionManager – режим работы менеджера сессий, возможные значения: DB – чтение и сохранения контекстов пользовательских сессий в БД, Mem – только чтение (контексты пользовательских сессий хранятся в памяти сервера и не записываются в БД), по умолчанию устанавливается режим DB;
- IsTestInstance – параметр оформления интерфейсов, например, «тестовых»;
- AdditionalTitle – параметр, в котором указывается текст, добавляемый в конец заголовка интерфейса (не рекомендуется использовать длинный текст, перенос текста не предусмотрен).

Пример:

```
[Service]
SessionTimeout=5
Name=TEST
DisplayName=TEST
HTTPPort=8621
TCPPort=8822
ContractorLogic=1
NativeHTTPPort=9877
ServerThreadCount=64
SessionManager=DB
IsTestInstance=1
AdditionalTitle=(ПОЛИГОН)
```

В секции **[DBConnection]** указываются настройки соединения с БД:

- Driver – используемый драйвер БД;
- HostName – имя сервера БД;
- Database – название БД;
- User_Name – имя пользователя БД.
- Password – пароль пользователя БД. После установки/изменения пароля и при последующем запуске сервера приложений производится шифрование пароля и каждый символ пароля отображается знаком «*». Пароль в зашифрованном виде сохраняется в поле «Password=» взамен ранее заданного пользователем.

- RowsetSize – кол-во записей в одном блоке данных, формируемом СУБД-сервером при возврате серверу приложений очередного фрагмента результатов выполнения запроса к БД. Необязательный параметр, в ряде случаев может быть использован для достижения оптимального соотношения «производительность запроса - виртуальная память, выделяемая для сохранения результатов запроса».
- ForcedDisconnectDelay – целочисленное значение времени задержки в секундах перед принудительным снятием с выполнения незавершенных запросов к СУБД-серверу. Необязательный параметр, по умолчанию равен 15 сек (рекомендуемое значение). Используется модулем DBProvider.sms.

Пример:

```
[DBConnection]
Driver=mssql
HostName=book\SQLEXPRESS
Database=test
User_Name=zvk
Password=zvk
RowsetSize=32768
ForcedDisconnectDelay=15
```

В секции **[DBPool]** указываются следующие параметры:

- DBPoolSize – размер пула = макс. количество соединений в пуле;
- DBPoolWaitTimeoutMS – время ожидания при получении соединения, миллисекунды;
- DBPoolCleanupDelayMinutes – время удаления из пула свободных соединений;
- DBPoolCleanupHangingMinutes – время принудительного удаления из пула занятых (взятых из пула) соединений;
- DBPoolConnectionLifeTimeHours – время жизни соединения в пуле с момента его создания в часах = время жизни сессии в БД (проверяется при возврате соединения в пул);
- DBPoolMinReserved – минимальное кол-во подготовленных к использованию соединений, добавляемых в пул сразу при его создании, по умолчанию 3;
- DBPoolMaxReserved – максимальное кол-во готовых к использованию соединений, добавленных в пул сверх минимального в ходе их создания и не удаляемых из пула после использования, по умолчанию 5.

Пример:

```
DBPoolSize=50
DBPoolMinReserved=10
DBPoolMaxReserved=20
DBPoolWaitTimeoutMS=3000
DBPoolCleanupDelayMinutes=5
DBPoolCleanupHangingMinutes=10
DBPoolConnectionLifeTimeHours=2
```

В секции **[Logger]** указываются следующие параметры:

- Level – нижний уровень сообщений, попадающих в лог: debug, info, warn, error, fatal;
- LogsFolder – папка записи логов;
- IntegrationWebCalls.Level – уровень логирования вызовов методов IntegrationService и RPIntegrationService;
- IntegrationWebCalls.FileName – имя файла лога, в который будет записываться информация о вызовах методов IntegrationService и RPIntegrationService;
- InternalWebCalls.Level – уровень логирования вызовов внутренних методов ПК;
- InternalWebCalls.FileName – имя файла лога, в который будет записываться информация о вызовах внутренних методов ПК;
- RPAdditional.Level – уровень логирования Планов ремонтов;
- RPAdditional.FileName – имя файла лога, в который будет записываться информация логирования Планов ремонтов;
- TransportManager.Level – уровень логирования сообщений при получении/отправке;
- TransportManager.FileName – имя файла лога, в который будет записываться информация по получению/отправке сообщений;
- LogRequests.Level – уровень логирования тел запросов/ответов к ЗРП;
- LogRequests.FileName – имя файла лога, в который будут записываться тела запросов/ответов к ЗРП;
- DBRouterLog.Level – уровень логирования маршрутизации заявок перечня;
- DBRouterLog.FileName – имя файла лога, в который будет записываться информация маршрутизации заявок перечня;
- ExcludedLogWebMethods – указываются методы, которые необходимо исключить из логирования при включенном логировании (например, метод Ping и GetNotify);
- DiagnosticMsgData – логирование работы детекторов.

Пример:

```
; Допустимы следующие уровни
; debug, info, warn, error, fatal
Level=debug
LogsFolder=D:\zvk\ZVK\baza6_Odu_Sib\Logs\
IntegrationWebCalls.Level=debug
IntegrationWebCalls.FileName=WebCalls
InternalWebCalls.Level=debug
InternalWebCalls.FileName=WebCalls
RPAdditional.Level=debug
RPAdditional.FileName=Additional
TransportManager.Level=debug
TransportManager.FileName= TransportManager
```

```
LogRequests.Level=debug
LogRequests.FileName=Requests
DBRouterLog.Level=debug
DBRouterLog.FileName=RouterLog
ExcludedLogWebMethods=Ping,GetNotify
```

В секции **[Scheduler]** указываются следующие параметры:

- Duration – частота опроса планировщика, миллисекунды;
- StartPause – пауза перед первым запуском, миллисекунды.
- TaskTerminationWaitTimeout – таймаут ожидания нормального завершения фоновых задач, при превышении которого задача снимается с выполнения принудительно, миллисекунды, по умолчанию = -1 (т.е., бесконечное ожидание).

Пример:

```
; частота опроса планировщика (милисек)
Duration=500
; пауза перед первым запуском (милисек)
StartPause=10000
; необязательное значение таймаута (милисек) ожидания завершения задач
; в диапазоне 0..2147483647 (максимум примерно 24 суток) или -1 (INFINITE),
; отсутствие параметра или пустое его значение трактуется как -1
TaskTerminationWaitTimeout=-1
```

Секция **[SchedulerTasks]** предназначена для автоматической очистки журналов:

- OutTransportTask – задача отправки сообщений;
- InTransportTask – задача приема сообщений;
- CheckAckTimeoutTask – задача проверки квитанций;
- ClearDataTask – задача архивации очистки данных и автоудаления диспетчерских заявок;
- RPTask – параметр, предназначенный для очистки уведомлений пользователя по сроку давности с указанным интервалом (86400 сек = 1 сутки) и временем запуска (15:00);
- RPLimitDay – параметр хранения журнала изменений;
- RMDataMarket – параметр запуска расчета периода для формирования аналитических отчетов;

– ArchiveZVKTask - параметр, предназначенный для архивации заявок по сроку давности с указанным интервалом (86400 сек = 1 сутки) и временем запуска (01:30).

Пример:

```
; параметры для задач:
; 1 значение - интервал между выполнениями задачи в секундах (1 сутки = 86400 сек)
; 2 значение (может быть опущено) - время первого запуска задачи в формате hh:mm
OutTransportTask=60
InTransportTask=60
CheckAckTimeoutTask=60
ClearDataTask=86400,01:00
RPTask=86400,15:00
RPLimitDay=30
ArchiveZVKTask=86400,01:30
```

В секции **[Key]** указываются следующие параметры (Рисунок 10.40):

– Number – ID ключа защиты. Данный параметр присутствует, когда KeyType=usb;
– Instance – идентификатор экземпляра;
– KeyType – тип ключа. Имеет два значения: usb-физический ключ, crypto - электронный ключ;
– KeyFileName – наименование файла ключа. Данный параметр присутствует, когда KeyType=crypto.

Пример подключения физического ключа:

```
[Key]
Number=27157AA6
Instance=asu
KeyType=usb
```

Пример подключения электронного ключа:

```
[Key]
KeyType=crypto
KeyFilmeName=zvkkey.lic
```

Секция **[Transport]** предназначена для анализа проблем отправки/приёма сообщений путем увеличения времени ожидания соответствующих ниток. Секция **[Transport]** не обязательна. Секция **[Transport]** добавлена, начиная с версии 7.1310.01.10.

В секции **[Transport]** указываются следующие параметры:

– SendTimeOut – время ожидания отправки сообщений (в секундах);

– ReceiveTimeOut – время ожидания приема сообщений (в секундах).

Если значения не указаны, то берутся значения по умолчанию равные 120 секунд.

Пример:

SendTimeout=180
ReceiveTimeout=180

Внимание! Изменения вступают в силу после перезапуска сервера приложений, с которым работает экземпляр программного комплекса.

Секция **[DTEK_INTEGRATION]** предназначена для включения взаимодействия с системой PowerOn.

В секции **[DTEK_INTEGRATION]** указывается параметр URL. В качестве значения параметра указывается ссылка в следующем виде: http://<client_name>:<clientPort>/?command=goto&point_id=<componentAlias, в которой:

- <client_name> - имя рабочей станции;
- <clientPort> - порт, по которому осуществляется взаимодействие;
- <componentAlias> - уникальный идентификатор оборудования в системе PowerOn.

Пример:

[DTEK_INTEGRATION]

URL=http://<client_name>:<clientPort>/?command=goto&point_id=<componentAlias

Секция **[AdditionalFunctions]** предназначена для подключения дополнительных функций ПО «Планы ремонтов» и других продуктов.

В секции **[AdditionalFunctions]** указываются следующие параметры:

– UseInsideReglament – активирует функцию настройки регламента приема графика для внутренних служб предприятия. По умолчанию значение параметра равно 1;

– CalculateChangeInitiator – функция вычисления инициатора изменений заявки. По умолчанию параметр отсутствует;

– ConsiderChilds – подключает возможность настройки согласования графика с нижестоящим предприятием. По умолчанию значение параметра равно 1;

- IsRepairDiffActive – активирует функцию «сравнения версий» в режимах параллельного просмотра. По умолчанию значение параметра равно 1;
- ShowAllManagementDevices – изменяет фильтрацию в поле «объект» на форме одного ремонта, позволяя создавать заявки на оборудование объектов нижестоящих предприятий, и объектов, имеющих оборудования в управлении\ведении текущего предприятия. По умолчанию параметр отсутствует;
- FixedPowerObjectList – снимает ограничения функции «Ограничение на создание заявки» в части работы с пользовательским интерфейсом в ПО «Планы ремонтов». По умолчанию параметр отсутствует;
- IsAdjustmentDateEditable – делает поля «дата последнего кап.ремонта» и «дата наладки/восстановления» редактируемыми для графиков, полученных с целью «утверждение». По умолчанию значение параметра равно 1;
- DeviceDescrDefaultPO – задание в качестве фильтра энергообъекта, который под текущим предприятием, на вкладке оборудования в Интерфейсе оборудования. Если под текущим предприятием нет энергообъектов, то фильтр не задастся. По умолчанию параметр отсутствует;
- AutoNotificationAll – включение автоотправления уведомления на предприятие, указанное в параметре AutoNotification. Отправка графика для уведомления осуществляется после перехода графика в состояние «Утвержденный». В графике для уведомления отправляются все заявки независимо от того находится ли оборудование по данной заявке в информационном ведении/ведении данного предприятия. Параметр добавляется вручную. По умолчанию параметр отсутствует;
- AutoNotificationSheduleType – типы графиков для которых нужно отправлять уведомление. Через запятую (указывается идент): rptENRG, rptELT, rptRZA, rptSDTU, rptMO. По умолчанию параметр отсутствует;
- CreateBindRepairs – функционал создания ремонтов на связанное оборудование. Если значение параметра равно 1, то в режиме редактирования ФОР рядом с полем «Связанные ремонты» отображается кнопка «🖇», с

помощью которой осуществляется добавление ПРЗ на связанное оборудование. Если параметр отсутствует или значение равно 0, то функционал скрывается и игнорируется. По умолчанию значение параметра CreateBindRepairs равно 1;

- CopyRepairs – функционал копирования своих ремонтов в будущие периоды (0 – скрыть режим «Копирование заявок» для ПО «Планы ремонтов»; 1 – отобразить режим «Копирование заявок» для ПО «Планы ремонтов»). По умолчанию значение параметра CopyRepairs равно 1. Если параметр CopyRepairs отсутствует в секции [AdditionalFunctions], то режим «Копирование заявок» для ПО «Планы ремонтов» должен быть скрыт;
- CommonScheduleforAgreee – функционал формирования сводного графика на уровне согласования. При добавлении параметра графики, присланные для согласования на один период объединяются в один сводный график ремонтов, в интерфейсе администратора в Регламент графиков ремонтов добавляется функционал настройки регламента для сводного графика. Если параметр отключен (отсутствует или CommonScheduleforAgreee=0), то функционал недоступен. Параметр добавляется вручную. По умолчанию параметр отсутствует;
- ForAgreeAcceptInReglament – включение функционала для сводных графиков, позволяющего выполнять ручное накрытие корректировок сводных графиков согласования и предварительного согласования без нарушения регламента при начатом рассмотрении. Работа функционала накрытия зависит от наличия включенного функционала сводных графиков согласования (CommonScheduleforAgree=1). Если хотя бы один из двух параметров отключен (отсутствует или CommonScheduleforAgree=0 или ForAgreeAcceptInReglament=0), то функционал недоступен. Параметр добавляется вручную. По умолчанию параметр отсутствует;
- CachedClientVersionCount – функционал настройки количества хранимых версий. В качестве значений указывается необходимое количество хранимых версий. «CachedClientVersionCount = <Необходимое количество хранимых версий>», например, «CachedClientVersionCount = 6», в таком случае будут храниться файлы шести последних версий подсистемы. В качестве

необходимого количества хранимых версий можно указать значения от 4 до 9. При указании других значений будут храниться по умолчанию файлы трех последних версий подсистемы. Параметр добавляется вручную. По умолчанию параметр отсутствует. Если параметр отсутствует в секции [AdditionalFunctions] или =0, то функционал отключен и хранятся файлы трех последних версий подсистемы;

- ScheduleCreateWarning – функционал оповещений о необходимости создании графика. По умолчанию значение параметра равно 1;
- EnableSendOpenCloseMsgFromAnyLevel – включение функционала формирования и отправки сообщения типа «Информация об открытии/закрытии заявки» независимо от того является предприятие инициатором или утверждающей стороной. Если параметр подключен (EnableSendOpenCloseMsgFromAnyLevel=1), то любое предприятие, с которым ведется обмен по модулю «Xml OpenClose», может изменить статус заявки. Если параметр отключен (отсутствует или EnableSendOpenCloseMsgFromAnyLevel=0), то при формировании сообщения типа «Информация об открытии/закрытии» осуществляется проверка, является ли предприятие инициатором заявки или утверждающей стороной, сообщение типа «Информация об открытии/закрытии заявки» не формируется и не отправляется на другие предприятия, при этом на данном предприятии доступно изменение состояния заявки и состояния оборудования. Если предприятие не является инициатором или утверждающей стороной, то при приеме и разборе сообщения типа «Информация об открытии/закрытии» осуществляется автоматическая отправка сообщений типа «Информация об открытии/закрытии» по маршруту текущего предприятия. **Внимание!** При обновлении на новую версию 10.21.1025.0817 и при установке АСУРЭО версии 10.21.1025.0817 с нуля в секцию [AdditionalFunctions] по умолчанию прописывается параметр EnableSendOpenCloseMsgFromAnyLevel=1. Если данный параметр уже прописан, то при обновлении на версию 10.21.1025.0817 параметр не изменяется;
- LinkedDeviceZVK – включение функционала отображения заявок на связанное оборудование. При добавлении параметра в мастере создания заявок на шаге

«8/12. Заполнение просимого времени и аварийной готовности» отображается кнопка «», на панели инструментов ФОЗ отображается кнопка «Связанные», на формах «Разрешить», «Открытие заявки», «Изменение состояния» на вкладке «Маршрут» отображается кнопка «», в списке заявок в служебном столбце для заявок на связанное оборудование отображается иконка связанного оборудования, на форме «Информация об оборудовании» в области «Зависимое оборудование» отображаются связанные единицы оборудования, в ведомости учета заявок становится доступна возможность посмотреть заявки на связанное и несовместимое оборудование. Если параметр отключен (отсутствует или LinkedDeviceZVK=0), то функционал отображения заявок на связанное оборудование недоступен. Параметр добавляется вручную. По умолчанию параметр отсутствует;

– DisableDelegationLastSign – запрет использования ППП, если в следующем внутреннем этапе есть другой пользователь с ППП. По умолчанию параметр отсутствует;

– AutoTransferNCI – функционал автоматической передачи НСИ (добавится настройка «Обмен изменениями в справочниках» в Интерфейсе администратора, добавится вкладка «Импорт изменений из ЖС» на форме Импорт в Интерфейсе администратора, добавится вкладка «Импорт изменений из ЖС» на форме Импорт в Интерфейсе оборудования). При включении данного функционала автоматически к системе подключается модуль «smsnotifier». Параметр добавляется вручную. Если параметр отсутствует в секции [AdditionalFunctions], то настройки функционала автоматической передачи НСИ игнорируются и скрываются. По умолчанию параметр отсутствует. При включении данного функционала в логах возможно увидеть задачу NCIInTransportTask. Это нормальная работа сервера приложений, осуществляется запуск служебной функции ПК «АСУРЭО»;

– CheckRepairDates – включение функционала по проверке превышения сроков ремонтов и оповещений пользователей о превышениях по EMAIL. По умолчанию параметр отсутствует. При включенном состоянии функционала:

- на форму «Регламент приема заявки (вкладка «Общие») | Интерфейс администратора» добавляются поля «Нормативный срок ремонта» и настройка периода запуска проверки на наличие превышения сроков (см. руководство по работе с приложением «Интерфейс администратора» раздел «Настройка нормативного срока по заявкам»);
- на форму «Настройки (вкладка «EMAIL - оповещения») | Интерфейс пользователя» в блок «Оповещение по электронной почте» добавляются поле «Превышение нормативного срока ремонта» (см. руководство по работе с приложением «Интерфейс пользователя» раздел «Настройка СМС-оповещений и Email-оповещений»).

При выключенном состоянии функционала поля «Нормативный срок ремонта», настройка периода запуска проверки на наличие превышения сроков и «Превышение нормативного срока ремонта» не отображаются;

– ShowYearDisconnectedZVK – включение функции просмотра заявок с отключением, поданных сначала года. При добавлении параметра в подсистеме «Заявки» в мастере создания заявки отображается дополнительное предупреждение и на форме одной заявки на панели инструментов отображается кнопка «Заявки с отключениями», становится доступна возможность просмотра заявок с отключениями в ведомости учета заявок. Если параметр отключен (отсутствует или ShowYearDisconnectedZVK=0), то недоступна функция просмотра заявок с отключением, поданных сначала года. Все дополнительные настройки скрываются. Параметр добавляется вручную. По умолчанию параметр отсутствует;

– AutoTakeDeviceVisibility – включение функционала автоматического изменения признака видимости у оборудования при ручном изменении видимости у оборудования через область «Видимость» справочника «Оборудование», при изменении иерархии дерева оборудования, а также при импорте оборудования. Если указано значение 0 или функция отсутствует, то функционал автоматического изменения признака видимости у оборудования отключен;

- IsEmergencyReadiness – включение функционала и отображения в графиках ремонтов РЗА столбца «Аварийная готовность» и поля «А/Г» (на ФОР и формах добавления заявок в график ремонтов РЗА). Если параметр отсутствует или =0, то функционал отключен. По умолчанию параметр отсутствует;
- ShowResponsibleUser – включение функционала и отображения поля «Ответственный за заявку» на ФОР, в котором указывается пользователь для создания диспетчерской заявки на основе плановой. Если указано значение 0 или функция отсутствует, то поле не отображается и функционал не активен. Если указано значение 1, то на ФОР отображается поле «Ответственный за заявку» и в сообщения Demands (информация о ремонтах ГР) и IncompatibleDemands (ремонты на несовместимое оборудование) добавляется параметр ResponsibleUser;
- ScheduleAgreeComparison – включение функционала сопоставления диспетчерских заявок «Согласования» с плановыми заявками из графиков с целью «Согласование». Если указано значение 0 или функция отсутствует, то пользователю доступен обычный функционал сопоставления только с плановыми заявками из графиков с целью «Утверждение», а также в сопоставлении не участвуют диспетчерские заявки с целью «Согласование». Если указано значение 1, то диспетчерские заявки, созданные на предприятии, присланные для согласования или утверждения могут быть сопоставлены с плановыми заявками из графиков с целью «Утверждение» и «Согласование». Если в ScheduleAgreeComparison указано значение 1, то диспетчерские заявки могут быть сопоставлены с плановыми ремонтными заявками из графиков с целью «Утверждение», «Согласование» и «Предварительное согласование»;
- AddUV=<Идентификатор предприятия> – указывает идентификатор предприятия, которое необходимо добавить в ведение ПК «Планы ремонтов» для импортируемого оборудования. Через «;» можно указать несколько разных предприятий, каждое из которых добавится в ведение ПК «Планы ремонтов»;
- ChangePassword – функция изменения пароля для входа в систему через Интерфейс пользователя. По умолчанию функция ChangePassword отключена. Если функция ChangePassword отключена (0), кнопка «Сменить пароль» не

отображается на форме «Списка интерфейсов для переключения» Интерфейса пользователя. Если функция ChangePassword включена (1) кнопка «Сменить пароль» отображается на форме «Списка интерфейсов для переключения» Интерфейса пользователя. Если функция ChangePassword отключена (0), функция установки «Срок действия пароля» не отображается в разделе «Системные настройки» во вкладке «Общие» Интерфейса администратора. Если функция ChangePassword включена (1): функция установки «Срок действия пароля» отображается в разделе «Системные настройки» во вкладке «Общие» Интерфейса администратора и когда срок действия пароля истек, в Интерфейсе пользователя отображается модальное окно с предупреждением о необходимости сменить пароль;

– FinesForecast – включение функционала по формированию отчета по прогнозу штрафов от простоя энергетического оборудования. Если значение параметра равно 1, то в боковом меню Интерфейса пользователя ПК «Планы ремонтов» отображается пункт меню «Прогноз потерь», в справочнике «Территории» Интерфейса оборудование отображается столбец «Цена мощности (руб.\МВт)», в Интерфейсе оборудования отображается справочник «Коэффициент сезонности», в Интерфейсе администратора в блоке ПК «Планы ремонтов» отображается право «Формирование отчета «Прогноз потерь»». Если параметр отсутствует значение равно 0, то функционал скрывается и игнорируется. Параметр добавляется вручную. По умолчанию параметр отсутствует;

– CheckForDuplicateInstance – включение функционала по проверке активных сессий пользователя при авторизации в Систему. Если значение параметра равно 1, то при авторизации пользователя в Систему будет выполняться проверка на наличие активной сессии пользователя в запускаемом интерфейсе и ему не будет доступен запуск несколько экземпляров одного интерфейса под одной учетной записью. Если параметр отсутствует или значение параметра равно 0, то при авторизации пользователя в Систему не будет выполняться проверка на наличие активной сессии пользователя в запускаемом интерфейсе и ему будет доступен запуск несколько экземпляров одного интерфейса под одной учетной записью. По умолчанию параметр отсутствует.

–

– NumberApplicationNotice – функция добавления дополнительного столбца «№ заявки предприятия уведомления» в список формы «Состав столбцов» списка заявок. В параметре указывается идентификатор предприятия, указать можно только одно предприятие. Пример: NumberApplicationNotice=ОДУ Центр. По умолчанию параметр отсутствует.

Пример:

```
[AdditionalFunctions]
UseInsideReglament=1
CalculateChangeInitiator=1
ConsiderChilds=1
IsRepairDiffActive=1
ShowAllManagementDevices=1
FixedPowerObjectList=1
IsAdjustmentDateEditable=1
DeviceDescrDefaultPO=1
AutoNotification=Русгидро
AutoNotificationSheduleType=rptENRG,rptELT
CreateBindRepairs=1
CopyRepairs=1
CommonScheduleforAgreee=1
ForAgreeAcceptInReglament=1
CachedClientVersionCount = 6
ScheduleCreateWarning=1
EnableSendOpenCloseMsgFromAnyLevel=1
LinkedDeviceZVK=1
DisableDelegationLastSign=1
AutoTransferNCI=1
CheckRepairDates=1
ShowYearDisconnectedZVK=1
AutoTakeDeviceVisibility=1
IsEmergencyReadiness=1
ChangePassword=1
FinesForecast=1
CheckForDuplicateInstance=1

NumberApplicationNotice=ОДУ Центр
```

10.11 Описание параметров файла sms.ZRP.WebApi.settings.json для ЗРП.Net

Веб-интерфейс ЗРП.Net поставляется отдельно и доступен при наличии соответствующей лицензии. Если у Вас есть ЗРП.Net, следуйте указанным ниже настройкам. Если ЗРП.Net отсутствует, игнорируйте данный раздел.

В ЗРП.Net используется три конфигурационных файла:

– файл с параметрами сервера приложений Sms.ZRP.WebApi.settings.json (раздел «10.11 Описание параметров файла sms.ZRP.WebApi.settings.json для ЗРП.Net»);
– файл с параметрами Identity сервера IdentityServer\AuthServer.settings.json (раздел «10.12 Описание параметров файла authServer.settings.json сервера авторизации»);
– файл с параметрами сервера авторизации ZRP.NET\wwwroot\Content\assets\config\config.json (раздел «10.13 Описание параметров файла config.json сервера авторизации»).

10.11.1Настройки базы данных

- **DatabaseProvider** – тип системы управления базой данных (СУБД);
  – возможные значения: SqlServer/PostgreSQL;
  – значение по умолчанию – SqlServer;

```
"DatabaseProvider": "SqlServer"
```

- **ConnectionStrings** – настройки подключения к БД;
  – **ZrpPostgreSQL**: "<specify conn str here>" – строка подключения к серверу баз данных PostgerSQL; Пароль в поле шифруется в Production режиме. При зашифрованном состоянии начинается и заканчивается с подстроки **!encrypted!**.
  – **ZrpSqlServer**: "<specify conn str here>" – строка подключения к серверу баз данных Microsoft SQL Server; Пароль в поле шифруется в Production режиме. При зашифрованном состоянии начинается и заканчивается с подстроки **!encrypted!**.
  – В зависимости от выбранного DatabaseProvider используется соответствующая строка подключения.

10.11.2Настройки логирования запросов к базе данных

```
"DbLoggerSettings": {
    "Enable": true,
    "IsLogQueriesActive": true,
```

```
        "IsLogDbContextActive": true
    },
```

- **Enable** – включить логирование запросов к БД;
- **IsLogQueriesActive** – включить логирование запросов в контексте чтения данных;
- **IsLogDbContextActive** – включить логирование запросов в контексте изменения данных.

10.11.3Настройки для подключения

- **InstanceName** – наменование экземпляра из zvk.ini [Service].Name;
- **AllowedHosts** – фильтр допустимых имён хоста, которые может иметь сервер. Если пользователь отправит запрос с именем хоста, отсутствующим в AllowedHosts сервер вернёт ошибку 400 BadRequst;
  - AllowedHosts: "*" – сервер может иметь любое имя хоста;
- **AuthAuthority** – адрес сервера авторизации. Указывается путь к серверу авторизации (IdentityServer);
  - обязательна;
  - ограничение: абсолютный URL адрес или ip адрес сервера авторизации (IdentityServer);

```
    "AuthAuthority": "https://localhost:5001"
```

- **RequireHttps** – признак требования безопасного соединения с сервером авторизации;
  - Возможные значения: true / false:
    - **true** – сервер авторизации использует протокол https, и сервер приложений должен подключаться к нему по этому протоколу;
    - **false** – допускается использование сервером авторизации протокола http, сервер приложений должен обращаться по этому протоколу;

- **ВНИМАНИЕ: не допускается использование сервером авторизации протокола http, только https.**

10.11.4Настройка доступа к серверу приложений Delphi_

- **IntegrationServiceSettings** – настройки интеграции с Delphi сервером приложений заявок;
  - **UseIntegrationService** – признак использования интеграции, true – используется проксирование запросов через делфи-сервер;
  - **IntegrationServiceUri** – адрес транспорта SOAP в формате host:port/SOAP, где:
    - **host** – абсолютный URL адрес или ip адрес сервера Delphi;
    - **port** – HttpPort или NativeHttpPort (смотреть zvk.ini) сервера Delphi.

```
"IntegrationServiceSettings": {
    "UseIntegrationService": false,
    "IntegrationServiceUri": "localhost:8620/SOAP>"
}
```

10.11.5Настройки подключения к etcd серверу

Etcd сервер может быть использован как место хранения кэша веб-запросов, а также как средство коммуникации с внешними сервисами (СП Delphi).

- **ConnectionString** – строка подключения к серверу etcd;
- **GroupId** – идентификатор группы серверов. Под группой серверов подразумевается два и более серверов приложений, которые должны «общаться» только между собой. При этом к серверу etcd могут быть подключены и другие СП, как объединенные в группы, так и нет. GroupId используется в качестве префикса к ключам etcd;
- **UseAuth** – использовать авторизацию на ETCD сервере;
- **UserName** – имя пользователя;
- **Password** – пароль.

```
"EtcdSettings": {
  "ConnectionString": "http://localhost:2379",
  "GroupId": "",
  "UseAuth": true,
  "UserName": "<ETCD user name>",
  "Password": "<ETCD user password>"
}
```

10.11.6Настройки кэширования веб-запросов

Кэширование веб-запросов – сохранение результата какого-либо эндпойнта (веб-метода) куда-либо на определенный промежуток времени. Если в течение этого времени приходит еще один такой же запрос, то возвращается сохраненный результат без выполнения логики.

- **Enable** – включить или выключить кэширование;
- **Type** – тип кэша. Имеет два значения: *etcd* и *memory*.

Если выбран тип etcd, то необходимо настроить секцию EtcdSettings (см. раздел «10.11.5 Настройки подключения к etcd серверу»).

```
"RequestCacheSettings": {
  "Enable": false,
  "Type": "etcd"
},
```

10.11.7Настройки коммуникации с внешними сервисами

Веб-сервер заявок коммуницирует с внешними сервисами только через etcd.

- **Enable** – включить или выключить коммуникацию с внешними сервисами;
- **Type** – способ коммуникации. Допускается только одно значение: *etcd*.

Если выбран тип etcd, то необходимо настроить секцию EtcdSettings (см. раздел «10.11.5 Настройки подключения к etcd серверу»).

```
"ExternalCommunicationSettings": {
 "Enable": false,
  "Type": "etcd"
```

```
    }
```

10.11.8Настройки оповещений

Сообщения от администратора и оповещения о снятии блокировки заявки приходят по каналу, настроенному в секции ExternalCommunicationSettings (см. раздел «10.11.7 Настройки коммуникации с внешними сервисами»).

Для того чтобы оповещения МОПОП появились в Журнале сообщений ЗРП.Net после включения настройки взаимодействия с сервисом «МОПОП» в Интерфейсе администратора ЗРП.Delphi, нужно перезапустить сервер приложений ЗРП.Net.

Примечание. В ЗРП.Net версии 11R4HF10 отсутствуют форматы сообщений МОПОП: оперативное оповещения – НСИ, квитанция оперативного оповещения – НСИ. Эти форматы сообщений МОПОП поддерживаются только в ЗРП.Delphi.

10.11.9Настройка Cross-Origin Resource Sharing

- **Cors** – настройки разрешений на доступ к серверу с выбранных ресурсов.

```
"Cors": {
    "Origins": "http://localhost:4200,https://localhost:5001",
    "Methods": "GET,POST,PUT,PATCH,DELETE",
    "Headers": "*"
}
```

10.11.10 Настройки JWT_

- **Jwt** – настройки генерации JWT токенов для проверки авторизации на выполнение запроса.

```
"Jwt": {
    "Issuer": "sms.ru",
    "Audience": "sms.ru",
    "Key": "giga-mega-secret-key",
    "Ttl": "01:00:00"
}
```

10.11.11 Запланированные задачи

- **ScheduledJobs** – секция настроек фоновых задач, которые выполняются по заданному расписанию. В каждой настройке используется cron-выражение.

Cron-выражения предназначены для возможности задавать периодичность и время срабатывания задач планировщика.

```
# ┌──────────── секунда (0-59) - опционально (отличается от стандартного cron-выражения)
# │ ┌──────────── минута (0-59)
# │ │ ┌──────────── часы (0-23)
# │ │ │ ┌──────────── число (1-31)
# │ │ │ │ ┌──────────── месяц (1-12)
# │ │ │ │ │ ┌──────────── день недели (0-6) (0 - воскресенье)
# │ │ │ │ │ │
# │ │ │ │ │ │
# │ │ │ │ │ │
# * * * * * *
```

Секция **ScheduledJobs** со следующими параметрами:

- **PurgeZvkAcknowledgement** – задача очистки устаревших значений таблицы квитирования. По умолчанию запускается один раз в сутки в 03:00.
- **UserSessionDropping** – задача сверяет пользовательские сессии в БД и в памяти веб-сервера. Если какая-либо из сессий «умерла», то пишет об этом в системный журнал. По умолчанию запускается один раз в минуту.
- **KeepAlive** – задача проверяет и продлевает пользовательскую сессию у всех действующих подключений по протоколу web-socket. Если сессия для какого-либо подключения не найдена или истекла, то отправляет сообщение UserSessionExpired. По умолчанию запускается один раз в минуту.
- **UserNotification** – задача рассылает накопившиеся с последнего запуска пользовательские оповещения. По умолчанию запускается один раз в минуту.
- **UserNotificationsDbCache** – задача синхронизирует пользовательские оповещения в памяти сервера с БД. Не отправляет оповещения. По умолчанию запускается один раз в три секунды.

- **ZvkForReviewNotification** – задача рассылает оповещения о новых заявках. По умолчанию запускается один раз в минуту.

```
"ScheduledJobs": {
  "PurgeZvkAcknowledgement": "0 3 * * *",
  "UserSessionDropping": "*/1 * * * *",
  "KeepAlive": "/10 * * * * *",
  "UserNotification": "*/1 * * * *",
  "UserNotificationDbCache": "/3 * * * * *",
  "ZvkForReviewNotification": "*/1 * * * *"
}
```

10.11.12 Системные настройки

- **SystemSettings**
  - **showItemCount** – максимальное количество плашек в поле при множественном выборе (Раскрывающийся список), целочисленное значение. Параметр добавляется автоматически инсталлятором. По умолчанию равен 15.
  - **isDemoMode** – параметр для маркировки что площадка является тестовым полигоном (выводит красную плашку «Внимание! Вы работаете на тестовом экземпляре»). По умолчанию: false. Не обязательный.
  - **waitToUnlockZvkInMinutes** – параметр для указания времени через которое будет сброшена блокировка заявки на неактивной вкладке системы. Параметр добавляется автоматически инсталлятором. По умолчанию установлено значение 45. Нельзя указывать в параметре значение меньше 30. Не рекомендуется устанавливать значение более 45 минут, т.к. может быть уже произведена выгрузка информации по вкладке браузером. Если в параметре указано значение 0, то функционал отключен.

```
"SystemSettings": {
  "showItemCount": 15,
  "isDemoMode": false
  "waitToUnlockZvkInMinutes": 30
}
```

10.11.13 Настройки интеграции с SAP

- **UseDelphiPlugin** – использовать дельфореализацию SAP-транспорта – значение = true, использовать шарпореализацию SAP-транспорта – значение = false. Значение устанавливается в соответствии с тем на каком экземпляре настраивается интеграция с SAP;
- **IsLoadForTest** – true - включение / false – выключение режима эмуляции интеграции с SAP;
- **SendZVK** – адрес сервиса передачи ДЗ в SAP ERP.

10.11.14 Настройки менеджера дополнительно подключаемых функций

- **FeatureManagerSettings**. Блок параметров не является обязательным. В случае отсутствия всего блока для всех функций применяются значения по умолчанию. Для не заданных в блоке функций применяются значения по умолчанию.
  - **SubscriberEnterprise** – включение функционала предприятий-абонентов. По умолчанию: false;
  - **EnableSendOpenCloseMsgFromAnyLevel** – включение функционала формирования и отправки сообщения типа «Информация об открытии/закрытии заявки» независимо от того является предприятие инициатором или утверждающей стороной. По умолчанию: true;
  - **CheckIdentity** – включение функционала «Проверка подлинности». По умолчанию: false;
  - **ContractorInfo** – включение отображения информации о Контрагентах на форме «Информация об оборудовании» во всех интерфейсах. По умолчанию: false;
  - **ShowYearDisconnectedZVK** – включение функционала по просмотру заявок с отключением, поданных с начала года. По умолчанию: false;
  - **NumberApplicationNotice** – включение функционала по добавлению столбца «№ заявки предприятия уведомления» в список заявок;

– **UseSapMsg** – включение отображения сообщений о передаче ДЗ и ПРЗ в SAP в соответствующих журналах сообщений подсистем «Заявки» и «Планы ремонтов». Если значение параметра True, то в Журнале сообщений отображаются типы сообщений «Заявка (СУПА)» и «Квитанция (СУПА)». Если параметр отсутствует, то в журнале сообщений новые типы сообщений скрываются игнорируются. Параметр добавляется вручную. По умолчанию параметр отсутствует;

– **ScheduleAgreeComparison** – включение функционала по сопоставлению ДЗ с целью «Для согласования», «Поданная на своем предприятии», и «Для утверждения» с ПРЗ из месячных графиков с целью «Утверждение», «Согласование» и «Предварительное согласование»;

– **ScheduleCreateWarning** – включение отображения настроек о необходимости создания графика в веб-интерфейсе. По умолчанию параметр отсутствует.

```
"FeatureManagerSettings": {
   "SubscriberEnterprise": false,
   "ScheduleAgreeComparison": false,
   "EnableSendOpenCloseMsgFromAnyLevel": true,
   "CheckIdentity": false,
   "ContractorInfo": false,
   "ShowYearDisconnectedZVK": false,
   "LinkedDeviceZVK": false,
   "NumberApplicatoinNotice": "ОДУ СВ",
   "UseSapMsg": false
 }
```

10.11.15 Настройки Swagger

- **UseSwagger** – флаг, устанавливающий необходимость использования Swagger. True - swagger будет использоваться, false - не будет.

```
"UseSwagger": true
```

10.11.16 Настройки лицензирования

- **Key**. Настройка лицензирования. Предназначена для подключения файла (библиотеки), которая необходима для работы физического/электронного ключа;
- **Instance** – уникальный идентификатор лицензионного ключа.

```
"Key": {
   "Instanse": "zvk"
}
```

10.11.17 Настройки сжатия ответов

По умолчанию СП веб-заявок сжимает ответы, включая статический контент (js, css, html) с оптимальным уровнем компрессии, который гарантирует хорошее качество сжатия при допустимом снижении скорости обработки ответа.

Чтобы изменить этот уровень необходимо в конфигурационный файл добавить настройку CompressionLevel, которая может принимать следующие значения:

- Optimal – баланс между размером сжатого ответа и скоростью его формирования;
- Fastest – наиболее быстрый способ сжатия, размер может быть больше;
- NoCompression – без сжатия;
- SmallestSize – наименьший размер сжатого ответа, но скорость его формирования меньше.

```
"CompressionLevel": "Fastest"
```

10.12 Описание параметров файла authServer.settings.json сервера

авторизации

10.12.1Настройки базы данных и подключения

- **AllowedHosts**, **DatabaseProvider** и **ConnectionStrings** работают точно так же, как и на сервере приложений.

10.12.2Настройки NT авторизации

- **NTAuthentication** – признак использования доменной авторизации. При использовании доменной авторизации указывается значение – **true**. При использовании не доменной авторизации (ввод логина/пароля пользователя) указывается значение – **false**;
  - ограничение: true / false;
  - значение по умолчанию – задаётся в инсталляторе на этапе «Настройка Identity ЗРП.NET», флаг «Доменная авторизация»;

```
"NTAuthentication": false
```

- **KerberosSettings** – настройки протокола Kerberos для проверки подлинности пользователя;
  - **ServicePrincipalName** – уникальный идентификатор экземпляра службы. Требуется для непрозрачной аутентификации. Шаблон: «HTTP/<полное имя компьютера>.<полное имя домена>»;
  - **UseKdcConfig** – признак использования конфигурационного файла kdc внутри системы. Если true, извлекает данные из специальных файлов, которые хранятся по путям:
    - в папке, путь к которой указан в переменной среде %KRB5_CONFIG%;
    - %APPDATA%\\Kerberos.NET\\krb5.conf – windows. Для windows требуется специальный Kerberos Client: https://github.com/dotnet/Kerberos.NET/releases;
    - Library/Preferences/Kerberos.NET/krb5.conf – osx;
    - /etc/krb5.conf – linux;

- **UseCurrentConfig** – ...
- **Domain** – адрес key distribution center;
- **KdcPort** – порт key distribution center;
- **UseWindowsKerberos** – признак обязательности использования протокола Kerberos на windows. Если стоит false, для windows будет использоваться протокол NTLM, а для linux Kerberos.

```
"KerberosSettings": {
    "ServicePrincipalName": "HTTP/vm-it-astra-ad.stand.local",
    "Domain": "STAND.LOCAL",
    "KdcPort": 88,
    "UseKdcConfig": false,
    "UseCurrentConfig": false,
    "UseWindowsKerberos": false
}
```

- **DomainAliasMap** – сопоставление домена в бд и набора реальных доменных имён для NT-авторизации;
  - **domain** – основной домен;
  - **values** – значения (Alias) с которыми пользователю разрешена NT-авторизация;
    - значения (Alias) которые есть у указанного домена. Указываются через запятую;
    - должны быть прописаны все возможные имена домена, в том числе указанное в domain;
    - значение по умолчанию: пусто.

```
"DomainAliasMap": [
    {
      "domain": "cmc",
      "values": [
        "mail.sms-samara.ru",
        "sms-a.ru",
        "cmc"
      ]
```

```
        },
        {
          "domain": "stand",
          "values": [
            "stand.local",
            "stand"
          ]
    }
```

10.12.3Настройки безопасности

- **Certificate** – настройки служебных сертификатов;
  - **UseDeveloperSigningCredential** – признак использования автогенерируемого сертификата разработчика. Не рекомендуется использовать на продуктовом сервере;
  - **PrivateSecret** – ....
  - **CertificateThumbprint** – хеш сертификата \ уникальный идентификатор сертификата для поиска сертификата в хранилище сертификатов;

```
"Certificate": {
    "UseDeveloperSigningCredential": true,
    "PrivateSecret": "<put your certificate password>",
    "CertificateThumbprint":     "<put     your     thumbprint
certificate>"
}
```

- **HashEncoding** – настройка кодировки строки для снятия хэша (например, пароля). Должно совпадать с кодировкой сервера на Delphi, иначе хэш паролей будет различен (по умолчанию в Windows это «windows-1251»).

10.12.4Настройки клиентов

- **AllowAuthenticateWithResourceOwnerPassword** – специальный защитный признак, блокирующий возможность прямого входа по логину и паролю с использованием resource owner password flow;

  - подробности о resource owner password flow: https://auth0.com/docs/authenticate/login/oidc-conformant-authentication/oidc-adoption-rop-flow

- **Clients** – набор всех клиентов, которые могут быть использованы для аутентификации и авторизации пользователя;
  - **RequireClientSecret** – признак обязательности указания специального секрета клиента - коллекция ClientSecrets текущего объекта (по умолчанию не используется);
  - **ClientId** – уникальный идентификатор клиента. Должен совпадать с идентификатором, полученным от клиента.
    - Файл конфигурации клиента можно найти по пути <корень экземпляра>\ZRP.NET\wwwroot\Content\assets\config\config.json
  - **ClientName** – наименование клиента. Отображается в логах сервера авторизации.
  - **RedirectUris** – набор допустимых адресов, которые может прислать клиент как точки возврата пользователя после завершения аутентификации;
    - Файл конфигурации клиента можно найти по пути <корень экземпляра>\ZRP.NET\wwwroot\Content\assets\config\config.json
  - **PostLogoutRedirectUris** – набор допустимых адресов, которые может прислать клиент как точки возврата пользователя после завершения выхода из приложения;
  - **AllowedCorsOrigins** – набор origins (схема, имя хоста, порт), откуда может попасть пользователь на сервер авторизации;
  - **AccessTokenLifetime** – время жизни токена доступа в секундах. По истечении этого времени будет запрошен новый токен доступа с использованием токена обновления;

- **AllowedGrantTypes** – набор доступных для текущего клиента типов входа (authorization flows).
  - По умолчанию: authorization_code
  - Прочитать о способах аутентификации и авторизации можно здесь: https://auth0.com/docs/authenticate/login/oidc-conformant-authentication/oidc-adoption-rop-flow

```
"AllowAuthenticateWithResourceOwnerPassword": false,
"Clients": [
    {
      "RequireClientSecret": false,
      "ClientId": "angular_spa",
      "ClientName": "Angular SPA",
      "RedirectUris": [ "http://localhost:4200/zvk/auth-callback" ],
      "PostLogoutRedirectUris": [ "http://localhost:4200" ],
      "AllowedCorsOrigins": [ "http://localhost:4200" ],
      "AccessTokenLifetime": 3600,
      "AllowedGrantTypes": [ "authorization_code" ]
    }
]
```

10.13 Описание параметров файла config.json сервера авторизации

- **stage** – настройка, определяющая в каком режиме, запускается приложение:
  - prod – от production (режим производственный);
  - dev – от development (режим разработки);
- **settingsIdentityServer** – настройки сервера авторизации, используются для корректной переадресации пользователя на страницу прохождения авторизации;
- **authority** – адрес сервера авторизации. На него произойдёт обращение при входе неавторизованного пользователя на страницу списка заявок;
- **client_id** – ИД клиента. Такой же указывается в конфигурациях сервера авторизации;

- **redirect_uri** – адрес, куда пользователь будет перенаправлен после успешной аутентификации пользователя;
- **post_logout_redirect_uri** – адрес, куда будет перенаправлен пользователь после успешного выхода из системы.

```
{
  "stage": "prod",
  "settingsIdentityServer": {
    "authority": "https://localhost:5001",
    "client_id": "angular_spa",
    "redirect_uri": "http://localhost:4200/zvk/auth-callback",
    "post_logout_redirect_uri": "http://localhost:4200"
  }
}
```

10.14 Настройка взаимодействия сервера приложений и пользовательских интерфейсов

Файлы, позволяющие осуществить доступ к пользовательским интерфейсам (*ZVKUser.htm, ZVKAdmin.htm, DeviceDescr.htm*).

В указанных файлах присутствует тэг *OBJECT*, ответственный за взаимодействие между клиентским рабочим местом и сервером приложений:

– параметр *codebase* содержит информацию о версии продукта;

– тэг Param указывает URL-адрес, по которому доступен сервер приложений.

По умолчанию при установке в значении *value* автоматически указывается относительный путь value=«/appsrv/proxy.dll». Но при любых изменениях имени сервера, значение *value* следует изменять.

Пример:

```
<OBJECT
        classid="clsid:DC13D53F-010F-4DA9-AF57-32BFC0A0980A"
        codebase="SMSITLoader.cab#version=5,1104,12,1016"
        width=100%
        height=100%
        align=center
        hspace=0
```

```
        vspace=0
>
<PARAM name="URL" value="http://zvk-server/tgk/appsrv/proxy.dll " value type="data">
…
</OBJECT>
```

10.14.1 Дополнительные настройки журналирования действий сервера приложений

Если при установке ПК задана своя (отличная от System) учетная запись для запуска сервера приложений, то для корректной журнализации (формирования и записи сообщений в log-файлы) всех действий сервера приложений ПК необходимо на папку, содержащую журналы работы (по умолчанию это «C:\Program Files (x86)\ZVK\<название экземпляра>\Logs»), дать право на запись данному пользователю.

Порядок действий.

Открыть панель «Свойства» для папки C:\Program Files (x86)\ZVK\<название экземпляра>\Logs.
На закладке *«Безопасность»* нажать на кнопку *«Добавить»*.
Выбрать пользователя, который был настроен при установке экземпляра ПК, и дать ему право на полный доступ.

Если при установке учетная запись для запуска сервера приложений не вводилась, то никаких дополнительных настроек не требуется.

Примечание. Если сервер приложений не стартует, то в лог добавляется информация о зацикливании оборудования: «Ошибка создания справочника оборудования: элемент Id='1111' ссылается сам на себя». Данная ошибка означает, что произошло зацикливание оборудования самого на себя. Старт сервера приложений не возможен: необходимо обратиться в службу поддержки СМС-ИТ.

10.15 Обновление ПК «АСУРЭО» на ОС MS Windows

Внимание! В случае использования веб-сервера IIS 7 и выше необходимо установить два дополнительных компонента, не входящих в стандартную поставку IIS:

- переадресация запросов URL Rewrite 2.0;
- прокси-переадресация Application Request Routing 2.0.

Для установки компонента переадресации запросов URL Rewrite 2.0 необходимо скачать дистрибутив с сайта Microsoft.

Для 32-х и 64-х разрядных ОС выпущены отдельные дистрибутивы:

- для x86: http://download.microsoft.com/download/6/9/C/69C1195A-123E-4BE8-8EDF-371CDCA4EC6C/rewrite_2.0_rtw_x86.msi;
- для x64: http://download.microsoft.com/download/6/7/D/67D80164-7DD0-48AF-86E3-DE7A182D6815/rewrite_2.0_rtw_x64.msi.

Для установки компонента прокси-переадресации Application Request Routing 2.0 необходимо скачать дистрибутив с сайта Microsoft.

Для 32-х и 64-х разрядных ОС выпущены отдельные дистрибутивы:

- для x86: http://download.microsoft.com/download/4/D/F/4DFDA851-515F-474E-BA7A-5802B3C95101/ARRv2_setup_x86.EXE;
- для x64: http://download.microsoft.com/download/3/4/1/3415F3F9-5698-44FE-A072-D4AF09728390/ARRv2_setup_x64.EXE.

Для установки компонента прокси-переадресации Application Request Routing 3.0 необходимо скачать дистрибутив с сайта Microsoft.

Для 32-х и 64-х разрядных ОС выпущены отдельные дистрибутивы:

- для x86: https://www.microsoft.com/en-us/download/details.aspx?id=47334;
- для x64: https://www.microsoft.com/en-us/download/details.aspx?id=47333.

Требуется обновление дополнительных модулей.

Требуется обновление плагинов интеграции с подсистемами ПК «АСУРЭО»: Оперативный журнал и ПК «Метролог», если они были установлены ранее.

Внимание! При обновлении папка с установленным экземпляром ПК «АСУРЭО» должна быть **обязательно закрыта**. Если старая версия ПК «АСУРЭО» при обновлении находилась:

- в папке «C:\Program Files», то она будет перенесена в папку «**C:\Program Files (x86)**»;
- в любой другой папке, то её размещение не изменится.

Внимание! При обновлении ПК «АСУРЭО» на СУБД PostgreSQL необходимо включить для пользователя опцию «Superuser». После завершения обновления опция должна быть выключена.

Обновление установленной версии ПК до новой версии осуществляется с помощью мастера установки. Для этого необходимо запустить под правами администратора файл *«Setup.exe»* из каталога *«install»* установочного диска ПК (см. раздел «10.6 Установка АСУРЭО на СУБД MSSQL/PostgreSQL»).

Для обновления необходимо в окне мастера *«Выбор производных действий»* выбрать пункт *«Обновить экземпляры»* и в списке *«Установленные экземпляры»* выбрать нужные экземпляры (Рисунок 10.67). Выбор нескольких экземпляров производится с помощью клавиш *«Shift»* или *«Ctrl»*.

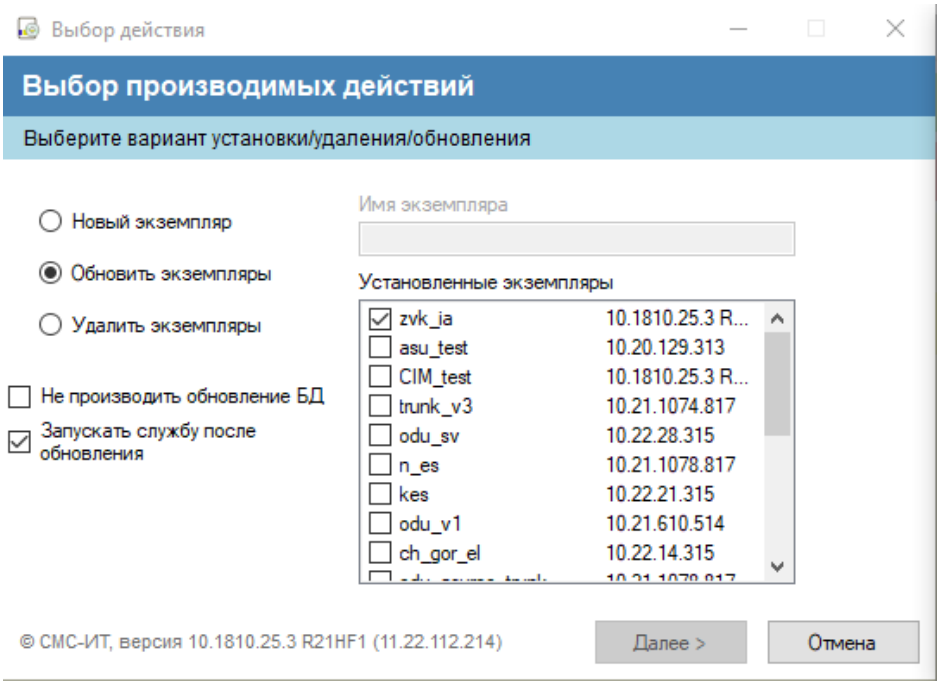

Рисунок 10.67 – Выбор экземпляров для обновления

В случае, если база данных экземпляра уже была обновлена до последней версии и обновить требуется только файлы сервера приложений, необходимо установить флаг *«Не производить обновление БД»*. При этом будут обновлены только файлы приложения, не затрагивая структуру базы.

Следующим шагом необходимо выбрать компоненты, которые должны быть обновлены (Рисунок 10.68). По умолчанию установлены флаги «Планы ремонтов» и «ПК Заявки».

Внимание! При обновлении с версий B5, B6 и B7 флаги об обновлении шаблонов ПК Заявки и Планы ремонтов отсутствуют. Для обновления шаблонов администратору необходимо самостоятельно установить флаги «Обновить шаблоны ПК Заявки» и «Обновить шаблоны Планы ремонтов».

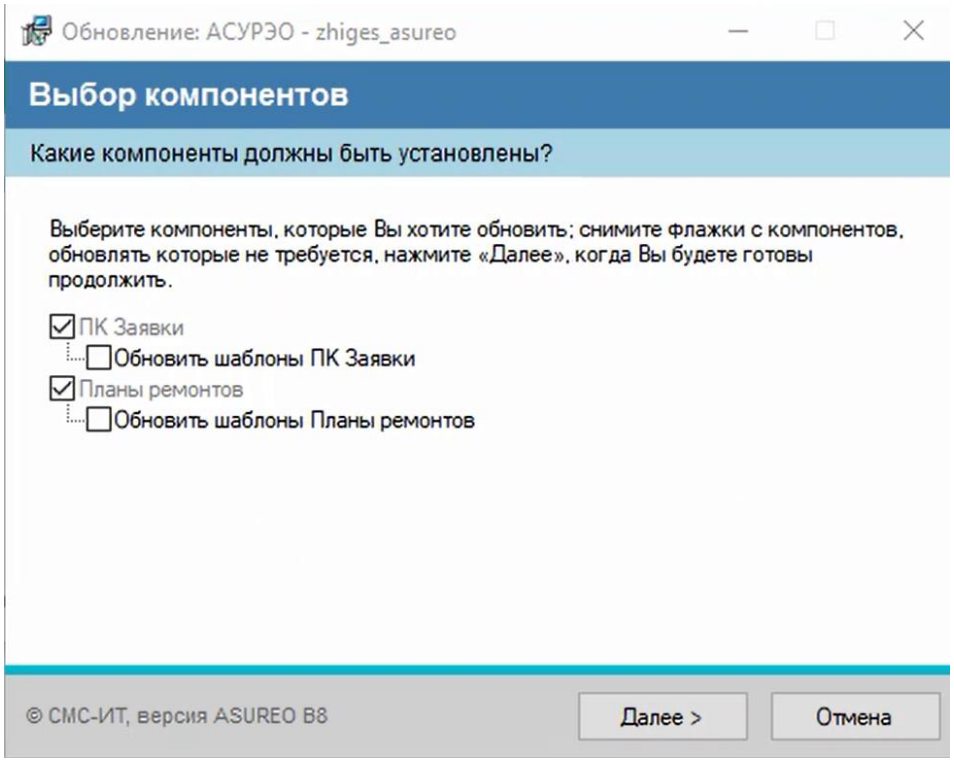

Рисунок 10.68 – Выбор компонентов обновления

После выбора компонентов по нажатию кнопки *«Далее>»* процедура обновления ПК запускается автоматически.

После старта обновления сначала останавливается Web-сервер. После этого выполняется последовательное обновление установленных экземпляров. Для каждого экземпляра сначала выполняется обновление структуры БД, после этого выполняется замена серверной и клиентских частей (Рисунок 10.69).

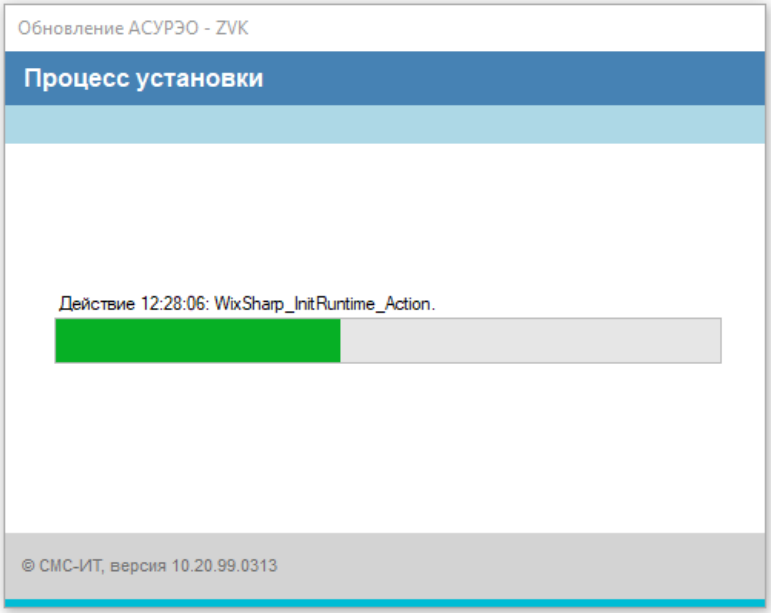

Рисунок 10.69 – Процесс обновления

По окончанию процесса обновления для выбранных компонентов появляется окно завершения мастера установки (Рисунок 10.70).

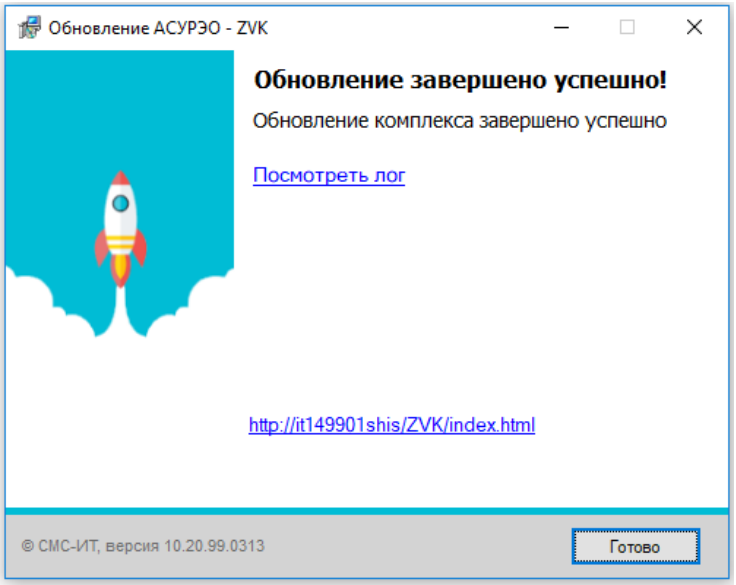

Рисунок 10.70 – Завершение обновления

Для выхода из программы обновления необходимо нажать на кнопку *«Готово»*.

Внимание! Начиная с версии 10.20.115.0313 часть параметров файла instali.ini переносится в системный реестр (Рисунок 10.71).

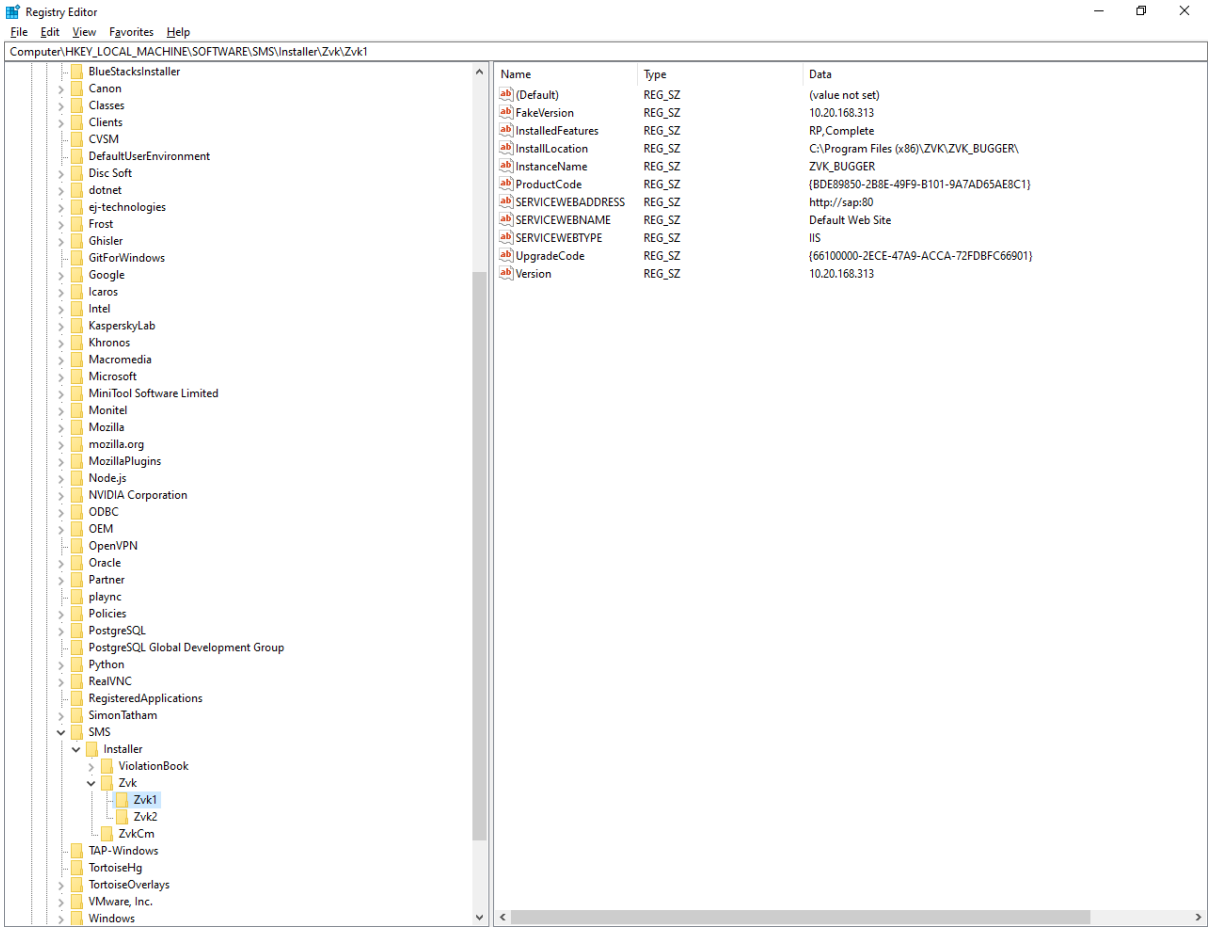

Рисунок 10.71 – Системный реестр

Внимание! Начиная с версии 10.21.1048.0817 при обновлении инсталлятором выполняется проверка в системном реестре на корректность параметра URL-адреса (должен начинаться с http, либо https). Если при запуске обновления выдается предупреждение (Рисунок 10.72), то администратору системы необходимо прервать обновление и в системном реестре вручную внести изменения с указанием полного корректного пути в параметр SERVICEWEBADDRESS (с http, либо https) (Рисунок 10.73). Параметр SERVICEWEBADDRESS указывается в реестре, в разделе «Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\SMS\Installer\Zvk\», далее необходимо выбрать папку с номером Zvk X, соответствующую текущему экземпляру. После этого запустить обновление.

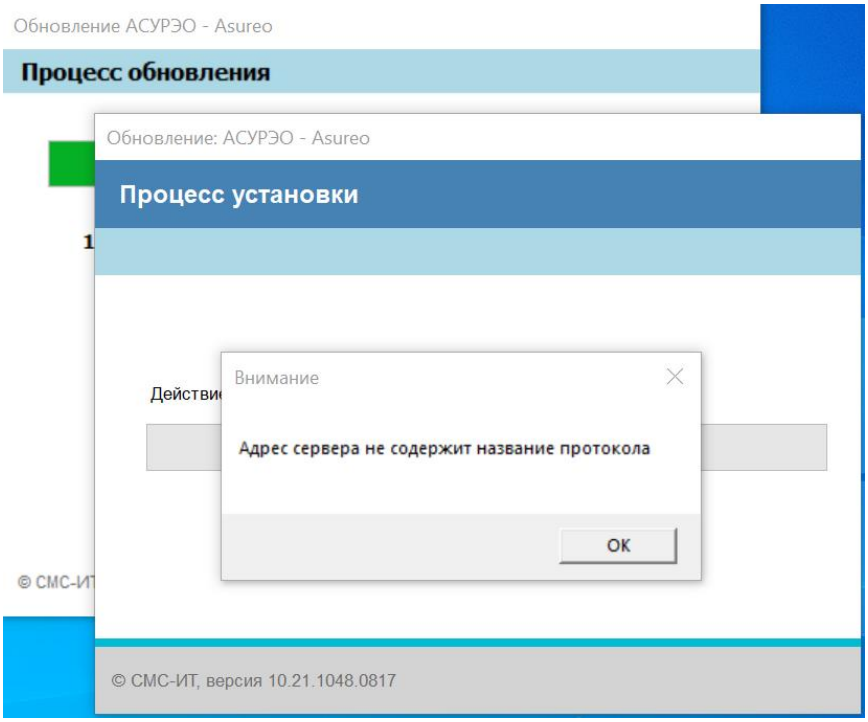

Рисунок 10.72 – Предупреждение

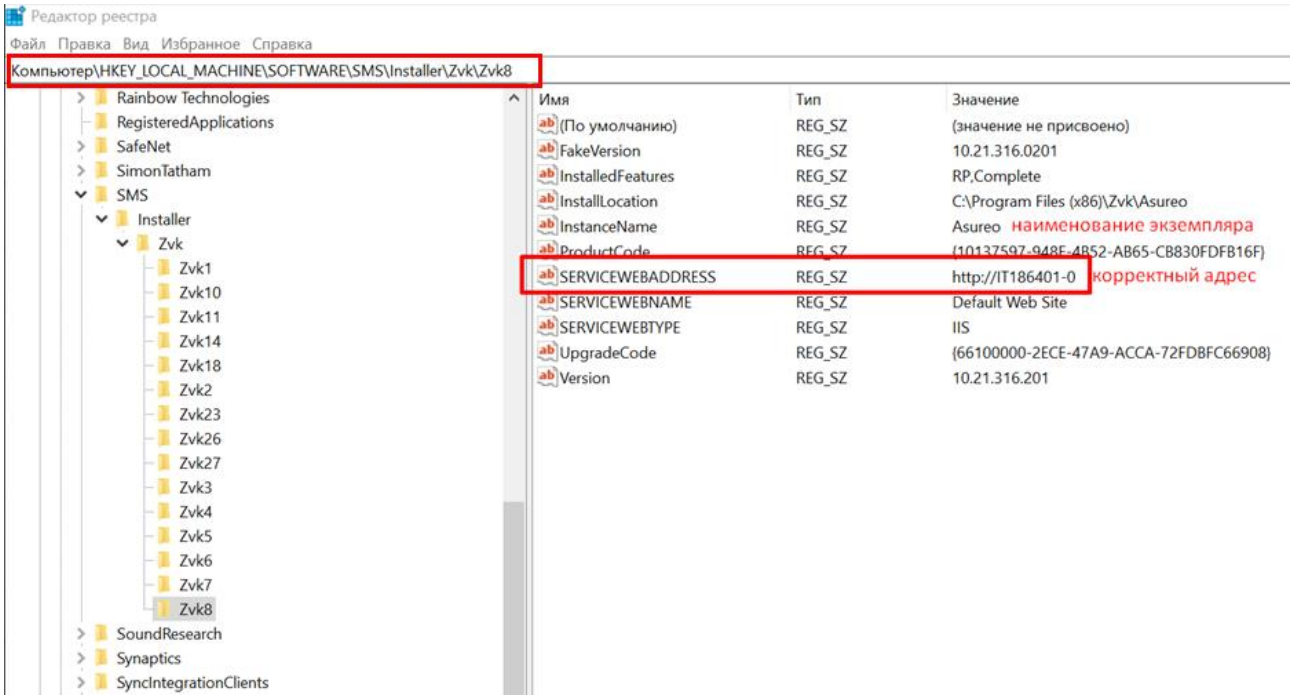

Рисунок 10.73 – Корректный полный адрес в реестре

10.16 Обновление ПК «АСУРЭО» на ОС семейства Linux

В состав дистрибутива для обновления АСУРЭО входят docker образы: **АСУРЭО.Delphi** и **АСУРЭО.Net (поставляется при наличии лицензий для веб-версии**

АСУРЭО). Обновление ПК «АСУРЭО» на ОС семейства Linux производится путём замены соответствующих docker образов на новые и запуском docker контейнеров. Для обновления ПК «АСУРЭО» необходимо выполнить следующие действия:

1. Выполнить остановку сервера приложений ПК «АСУРЭО» и очистку томов docker. Для этого в серверной директории (далее по тексту /opt/asureo) выполнить команду:

sudo docker-compose down -v

Также остановку можно выполнить с помощью скрипта **serverstop.sh**. Подробное описание см. в разделе «15.6 Рекомендации по штатному останову серверов приложений».

В случае остановки сервера приложений с помощью скрипта необходимо дополнительно удалить docker тома. Для удаления docker тома АСУРЭО выполнить команду:

sudo docker volume rm asureo_www

Для удаления docker томов АСУРЭО.Net выполнить команды:

sudo docker volume rm asureo_config

sudo docker volume rm asureo_sqlite

2. При наличии каталога /opt/asureo/www очистить его, выполнив команду:

   *sudo rm -r /opt/asureo/www/**:

   *sudo rm -r /opt/asureo/www/**

   Крайне важно перед обновлением комплекса очищать папку /opt/asureo/www, в составе которой находится файл «migrator_first_run_complete». Иначе БД не будет обновляться!!!

3. Вывести список docker образов, чтобы увидеть полное имя образа, выполнив команду: sudo docker images

   Например, на рисунке 10.74 полное имя *asu:v9sd7_release* для АСУРЭО и *asu-web:latest* для АСУРЭО.Net

   Примечание. Имена ваших docker-образов могут отличаться.

```
sysadmin@zvk-test:/opt/asureo$ sudo docker images
REPOSITORY   TAG          IMAGE ID      CREATED       SIZE
nginx        alpine       1ff4bb4faebc  4 weeks ago   47.9MB
asu-web      latest       af3c3a544c47  3 months ago  569MB
asu          v9sd7_release 7d45237304c0 3 months ago  4.51GB
```

Рисунок 10.74 – Выполнение команды sudo docker images

4. Удалить docker образы предыдущей версии комплекса. Выполнить команду:

   sudo docker rmi <имя:тег>

   (Ваше имя образа может отличаться) (Рисунок 10.75):

```
sysadmin@zvk-test:sudo docker rmi asu-web:latest asu:v9sd7_release
```

Рисунок 10.75 – Команда удаления docker образа

5. Скопировать в папку /opt/asureo файлы образов новой версии (образы для АСУРЭО.Delphi и АСУРЭО.Net). Чтобы убедиться в присутствии всех необходимых файлов в каталоге комплекса выполнить команду:

   ls /opt/asureo

   Пример представлен на рисунке 10.76.

```
sysadmin@zvk-test:/opt/asureo$ ls /opt/asureo
asu_v9sd8_release.tar   asu_web_v9sd8   docker-compose.yml   Zvk.ini
```

Рисунок 10.76 – Выполнение команды ls /opt/zvk

6. Загрузить docker образы из файлов новой версии, выполнив команду:

   sudo docker load < ‘название файла образа’

   Название вашего файла может отличаться.

   Пример загрузки приведен на рисунке 10.77.

```
sysadmin@zvk-test:sudo docker load < asu_v9sd8_release.tar
sysadmin@zvk-test:sudo docker load < asu_web_v9sd8.tar
```

Рисунок 10.77 – Команды для загрузки новых образов docker load

7. Проверить успешную загрузку docker образов путём вывода списка образов, выполнив команду:

   sudo docker image ls

   Пример представлен на рисунке 10.78.

```
admin@cluster:/opt/asureo# sudo docker image ls
REPOSITORY        TAG        IMAGE ID        CREATED        SIZE
asureo-web        release    02f34g56ho50    1 week ago     1GB
asureo_linux      release    02f34g56ho51    1 week ago     4GB
```

Рисунок 10.78 – Выполнение команды docker image ls

(Примечание: возможно имя образа будет отличаться от старого, поэтому нужно сверить имя образа с именем в docker-compose.yml и если нужно исправить на актуальное)

8. Запустить docker контейнеры новой версии АСУРЭО, выполнив команду: *sudo docker-compose up -d*
9. Проверить успешный запуск docker контейнеров путём вывода списка активных контейнеров, выполнив команду:

   sudo docker ps

   Пример представлен на рисунке 10.79.

```
sysadmin@zvk-test:/opt/asureo$ sudo docker ps
CONTAINER ID   IMAGE        COMMAND        CREATED     STATUS        PORTS        NAMES
d7ba745e2b9a   asu_web:v9sd8   "/bin/bash /opt/dock…"   2 minutes ago   Up 2 minutes     ASUREO-Net
21d04029d064   asu:v9sd8_release   "/home/root/docker-e…"   2 minutes ago   Up 2 minutes (healthy)
0.0.0.0:8625->8625/tcp, :::8625->8625/tcp, 0.0.0.0:8825->8825/tcp, :::8825->8825/tcp, 0.0.0.0:9880->9880/tcp,
:::9880->9880/tcp   ASUREO
d4179730ec58   nginx:alpine        "/docker-entrypoint.…"   2 minutes ago   Up 2 minutes          0.0.0.0:80-
>80/tcp, :::80->80/tcp, 0.0.0.0:83->83/tcp, :::83->83/tcp, 0.0.0.0:443-444->443-444/tcp, :::443-444->443-444/tcp
webserver
```

Рисунок 10.79 – Выполнение команды docker ps

10.16.1Последовательность действий на клиентах после обновления Системы

При обновлении АСУРЭО происходит разрыв связи с сервером приложений. Пользователю отображается модальное окно «Ошибка соединения с сервером приложений» (Рисунок 10.80).

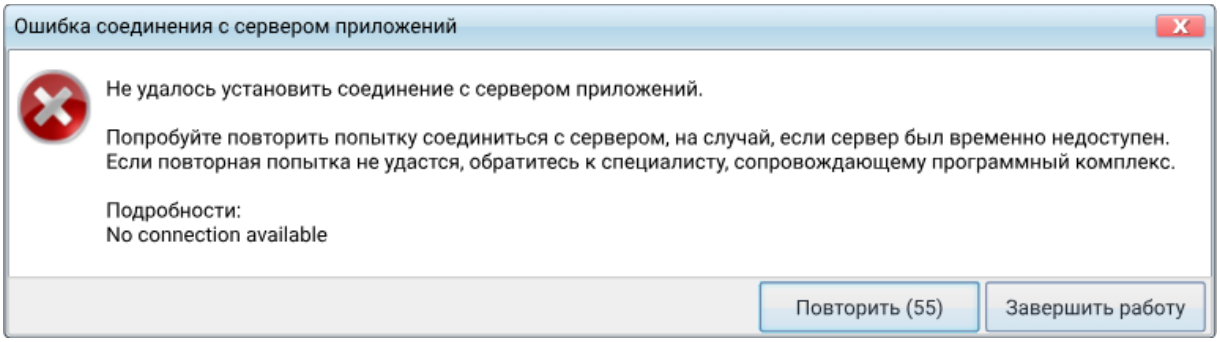

Рисунок 10.80 – Модальное окно «Ошибка соединения с сервером приложений»

По нажатию на кнопку «Повторить» форма закрывается и выполняется повторная попытка соединения с сервером приложений. При успешном соединение пользователю станет доступна работа с интерфейсом в штатном режиме. При повторной ошибке вновь отобразится форма «Ошибка соединения с сервером приложений». По нажатию на кнопку «Завершить работу» форма закрывается совместно с открытым интерфейсом без сохранения внесенных изменений.

После завершения обновления версия клиента и сервера приложений может не совпадать. На клиенте осуществляется проверка версии сервера приложения для сравнения с версией клиента (Проверка осуществляется на любом клиенте ПК «АСУРЭО», ПО «Ремонты», Интерфейс оборудования, Интерфейс Администратора).

Начиная с версии АСУРЭО B9 SD10, если версии клиента и сервера приложений не совпадают, то пользователю перестает отображаться модальное окно «Ошибка соединения с сервером приложений» и отображается модальное окно «Обновить версию клиентского приложения» (Рисунок 10.81).

В лог сервера приложений записывается информация о различии версий в следующем виде: «Сессия {GUID сессии} несовместима с данной версией сервера (интерфейс = <номер версии клиентского приложения>, сервер = <номер версии сервера приложений>). При переоткрытии интерфейса версия клиента обновляется, и пользователь продолжает работу с комплексом.

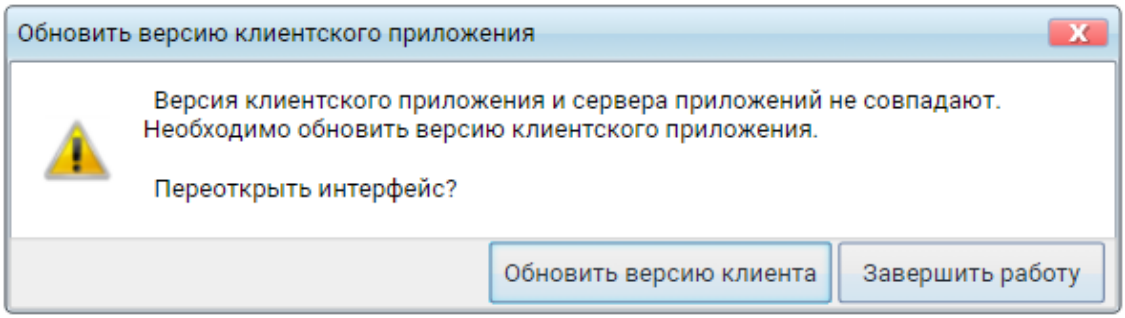

Рисунок 10.81 – Модальное окно «Обновить версию клиентского приложения»

При нажатии на кнопку «Обновить версию клиента» осуществляется перезапуск интерфейса. Версия клиента обновляется при перезапуске. При хотфиксах версия сервера не меняется. Данный функционал не будет отрабатывать, так как версии клиента и сервера должны совпадать. По нажатию кнопки «Завершить работу» приложение закрывается.

Важно! Функционал отрабатывает только если версия клиентского приложения B9 SD10 и выше. Таким образом, функционал будет отрабатывать только со следующей версии, например, при обновлении на B9 SD10 функционал не отработает, так как клиентские версии будут отличаться от B9 SD10. При обновлении на следующую версию после B9 SD10 функционал будет отрабатывать согласно описанию выше.

Если версия клиентского приложения ниже B9 SD10, то клиентское приложение не может запустить загрузчик для обновления самого себя на новую версию. Поэтому возможно возникновения следующих сценариев:

<u>Сценарий 1</u>

Условия:

СП обновлен до новой версии (B9 SD10).

Клиентское приложение не обновлено (B9 SD9 и ниже) и запущено на рабочем месте пользователя.

Открыта форма авторизации.

Действия:

Пользователь пытается залогиниться в комплексе.

Результат:

На форме авторизации отображается ошибка с текстом: «Ошибка авторизации на сервере. An exception was raised on the server. Версия клиентского приложения и сервера приложений не совпадают. Необходимо обновить версию клиентского приложения. (Версия клиента=<версия клиента>, Версия сервера=<Версия сервера>. Пользователь не может авторизоваться пока не обновится клиент.».

Пользователю необходимо закрыть клиентское приложение и открыть заново, чтобы запустить загрузчик для обновления самого себя на новую версию.

Примечание. При переоткрытии приложения (по F5) загрузчик не запускается. Версия клиентского приложения не обновляется.

Сценарий 2

Условия:

СП обновлен до новой версии (B9 SD10).

Клиентское приложение не обновлено (B9 SD9 и ниже) и запущено на рабочем месте пользователя.

Пользователь авторизован и открыта любая форма комплекса.

Результат:

После обновления приложения пользователю отображается модальное окно «Ошибка связи с сервером приложений» по нажатию на кнопку «Повторить» ничего не происходит, а именно, не отображается новое модальное окно «Обновить версию клиентского приложения».

Если сервер приложений успевает полностью загрузиться, то модальное окно автоматически закрывается.

При совершении любого действия пользователю отображается модальное окно «Ошибка авторизации» с текстом «Ошибка авторизации на сервере. An exception was raised on the server. Версия клиентского приложения и сервера приложений не совпадают. Необходимо обновить версию клиентского приложения. (Версия клиента=<версия клиента>, Версия сервера=<Версия сервера>. Попробуйте повторить попытку еще раз.».

Если отображается прогресс-бар, то кнопки «Повтор» и «Завершить приложение» не отрабатывают. По нажатию на кнопки ничего не происходит.

10.17 Интеграция с Avanpost FAM

Для интеграции с Avanpost FAM реализовано изменение заголовка окна приложения на время показа формы авторизации на «Интерфейс пользователя | ПК АСУРЭО | Аутентификация», а после прохождения успешной аутентификации заголовок меняется обратно на стандартный - «Интерфейс пользователя | ПК АСУРЭО».

10.18 Настройка клиентского рабочего места

10.18.1Настройка браузера Internet Explorer

Пользователи с ограниченными правами не могут загружать и выполнять приложения ClickOnce, возможно потребуется разрешение на загрузку файлов. Для корректной работы рабочих мест следует выполнить следующие настройки для клиентских рабочих машин:

1) Выбрать в меню «Сервис» \ «Свойства обозревателя Internet Explorer» закладку «Безопасность».

2) Выбрать соответствующую зону безопасности:

- если сервер приложений находится в местной интрасети, то выбрать зону «Местная интрасеть»;
- если сервер приложений находится на удаленном сервере в Интернет, то выбрать зону «Надежные узлы». В данном случае необходимо внести удаленный узел ПК в список надежных веб-узлов (нажать на кнопку «Узлы…» и добавить в доверенную зону web-узел ПК).

3) Разрешить загрузку файлов. Для этого необходимо:

- для выбранной зоны нажать на кнопку «Другой» и выбрать параметр «Загрузка» \ «Скачивание файла»;
- установить параметр «Включить» (Рисунок 10.82).

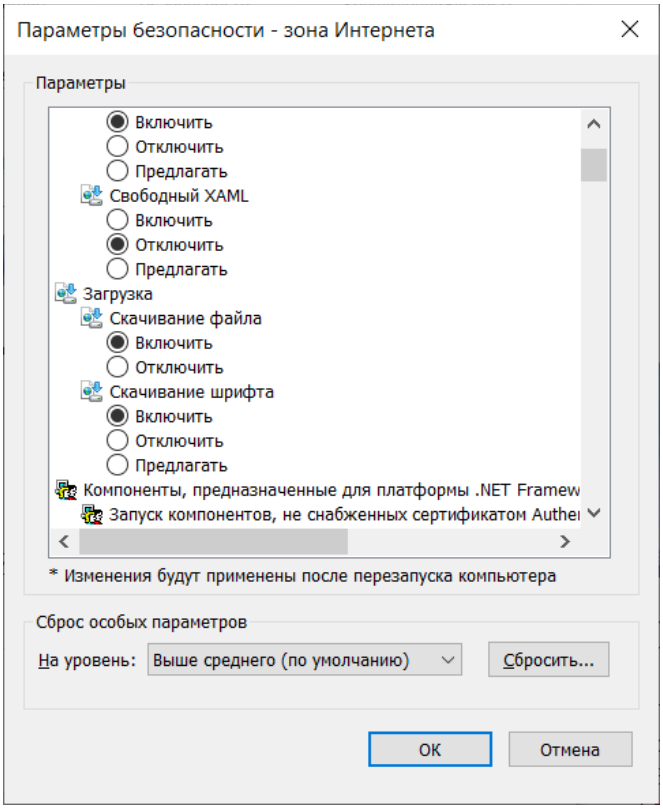

Рисунок 10.82 – Настройка обозревателя Internet Explorer

10.18.2Настройка ClickOnce

Установка клиента ПК «АСУРЭО» реализована по технологии ClickOnce, что позволяет пользователю устанавливать и запускать клиента, по нажатию на ссылку на веб-странице, либо в сетевом окружении. Изначально ClickOnce настроен на подключение по протоколу http. Если необходимо подключаться к ПК «АСУРЭО» по протоколу https или изменился путь, по которому происходит подключение к ПК «АСУРЭО», необходимо пересобрать ClickOnce.

Для это необходимо выполнить следующие действия:

1. Сделать резервную копию папки ПК «АСУРЭО».
2. Остановить службу ПК «АСУРЭО».
3. Выполнить изменения в файле «ClickOnceGen.cmd», расположенном по пути «C:\Program Files (x86)\ZVK\{имя_экземпляра}\SMSITLoader\Tools\»:
   - изменить строку подключения к ClickOnce «http://it200909-0/click1/SMSITLoader» в формате: «http(https)://{имя_сервера}/{имя_экземпляра}/SMSITLoader».

     Указывается полное имя сервера на которое выпущен сертификат. Если

экземпляр установлен в кластере, то вместо {имя_сервера} необходимо указать имя точки доступа (можно посмотреть в Failover Cluster Manager);

- заменить версию экземпляра «10.19.3273.1104», изменив, например, последнюю цифру;
- сохранить сделанные изменения.

4. Открыть командную строку с правами администратора, перейти в папку «C:\Program Files (x86)\ZVK\{имя_экземпляра}\SMSITLoader\Tools\» и выполнить «ClickOnceGen.cmd». Дождаться успешного завершения.
5. Запустить службу ПК «АСУРЭО» и проверить запуск интерфейсов.

В случае необходимости возврата к изначальным настройкам необходимо:

1. Остановить службу ПК «АСУРЭО».
2. Скопировать из резервной копии содержимое папки ПК «АСУРЭО».
3. Запустить службу ПК «АСУРЭО» и проверить запуск интерфейсов.

Для корректной работы ПК «АСУРЭО» необходимо на сервер установить сертификат. Для получения сертификата необходимо обратиться в службу поддержки СМС-ИТ.

При установке сертификата в качестве хранилища должен быть выбран локальный компьютер или импортировать сертификат в доверенные корневые центры сертификации (Рисунок 10.83).

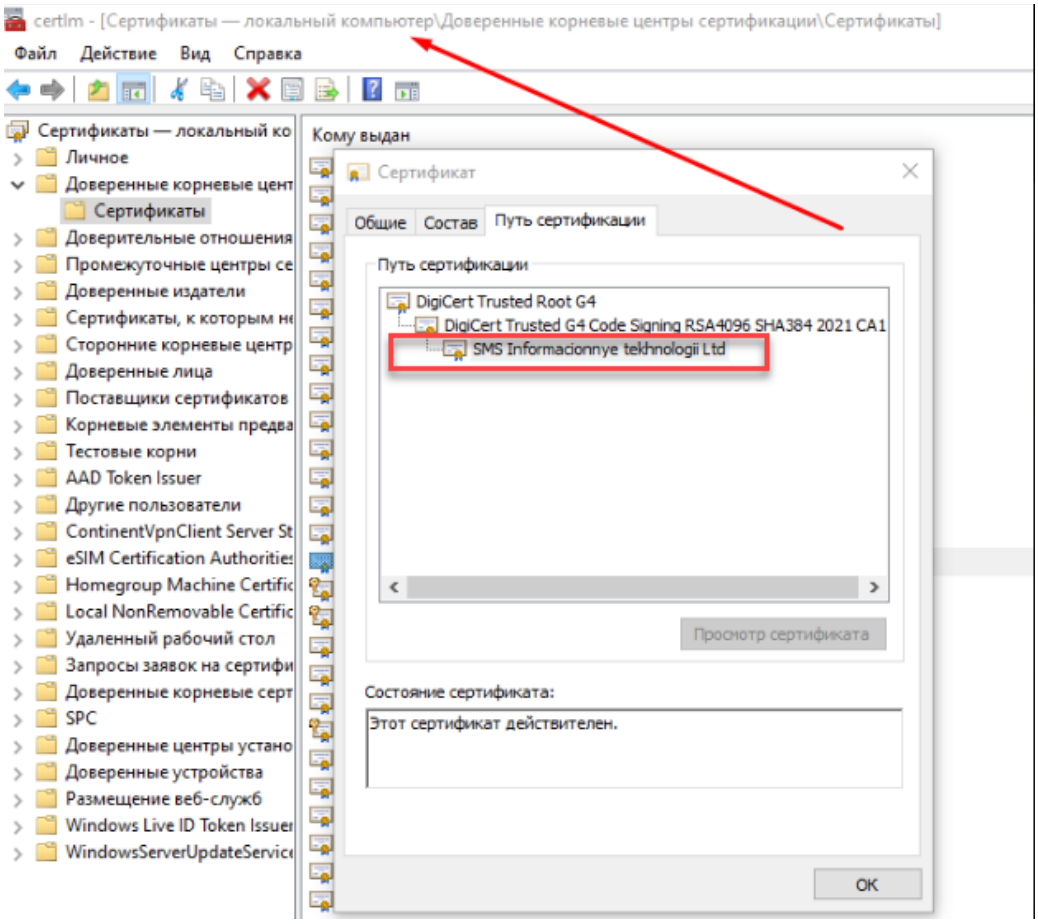

Рисунок 10.83 – Управление сертификатами

10.18.3Запуск приложений через ClickOnce

Для работы с ПК существует возможность использования браузеров Yandex, Firefox и Chrome.

Для автоматического запуска ClickOnce в разных браузерах должно быть установлено расширение под необходимый браузер.

Установка или обновление пользовательского приложения с помощью компонента ClickOnce осуществляется следующим образом:

1. При выборе приложения для запуска на HTML странице проверяется текущая установленная версия и при необходимости запускается установка ClickOnce.
2. Скачиваются и устанавливаются файлы из каталога SMSITLoader в %CurrentUser%\AppData\Local\Apps\2.0.
3. Если ClickOnce-приложение уже установлено, то оно запускается.

4. ClickOnce-приложение вызывает Zvk.exe, который находится в той же папке, и передает ему параметры для запуска соответствующего интерфейса.

5. Производится запуск интерфейса.

Если расширение не установлено, то браузер будет скачивать файл установщика каждый раз при переходе по ссылке экземпляра ПК.

При использовании браузеров Yandex и Chrome клиентские интерфейсы скачиваются каждый раз в загрузки и их необходимо запускать вручную (Рисунок 10.95).

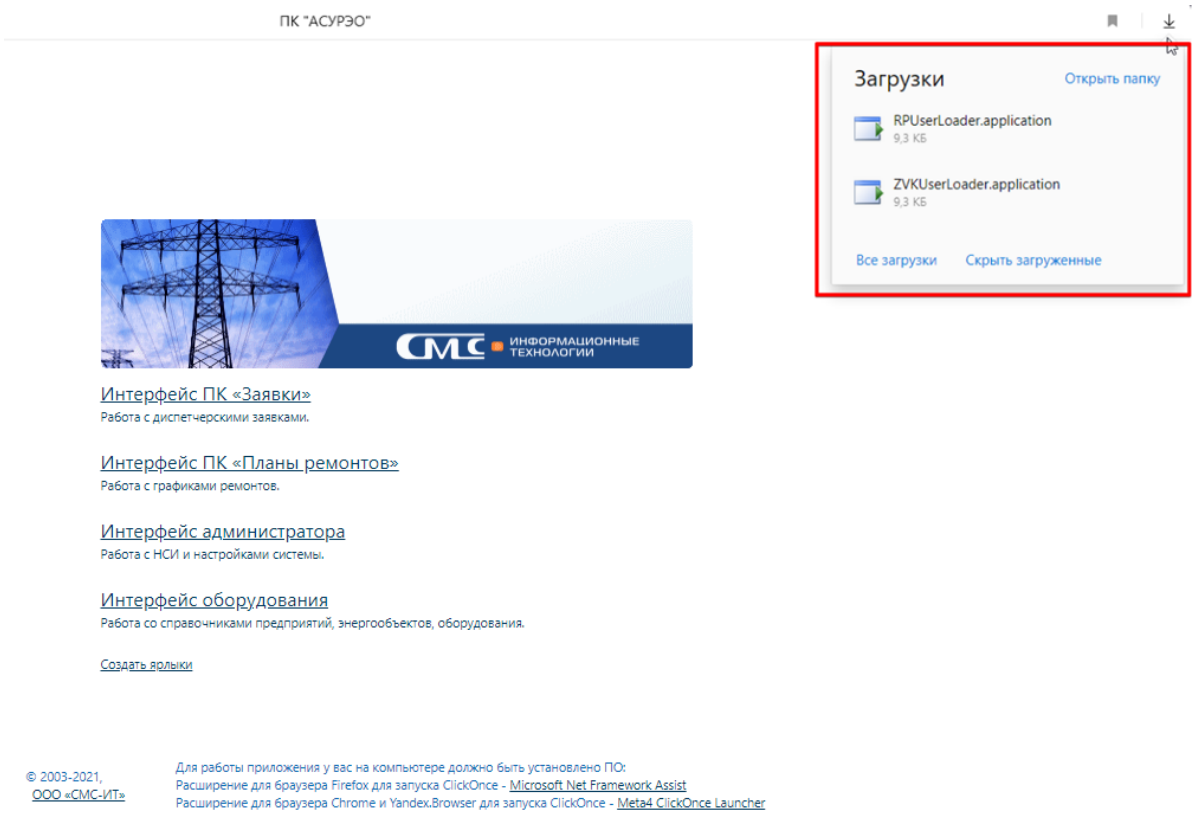

Рисунок 10.84 – Загрузки

При открытии файла загрузки открывается окно установки выбранного приложения (Рисунок 10.85).

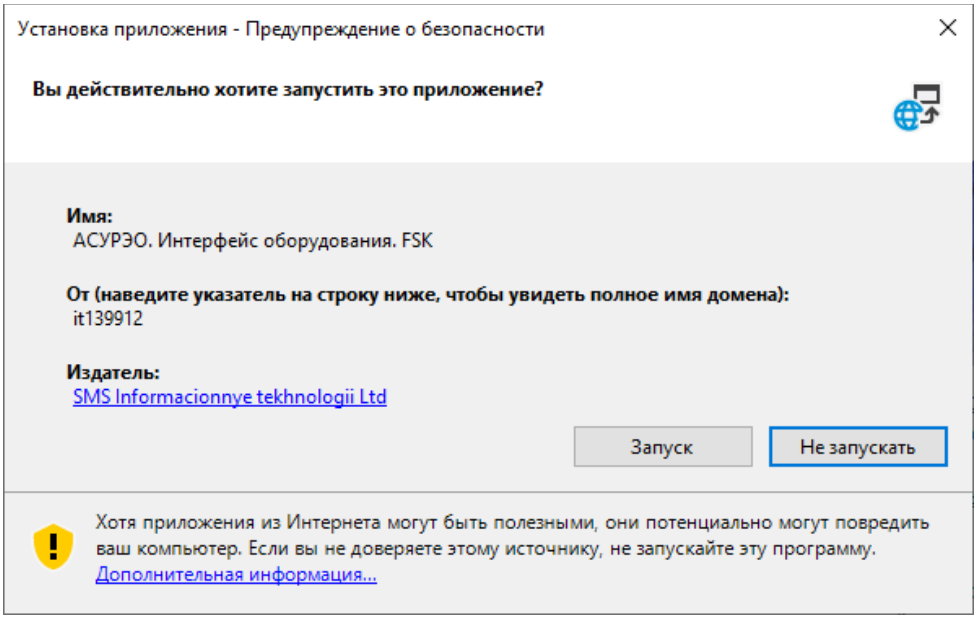

Рисунок 10.85 – Окно установки приложения

Для подтверждения запуска выбранного приложения необходимо нажать кнопку «Запуск». После подтверждения запуска начинается скачивание выбранного приложения (Рисунок 10.86).

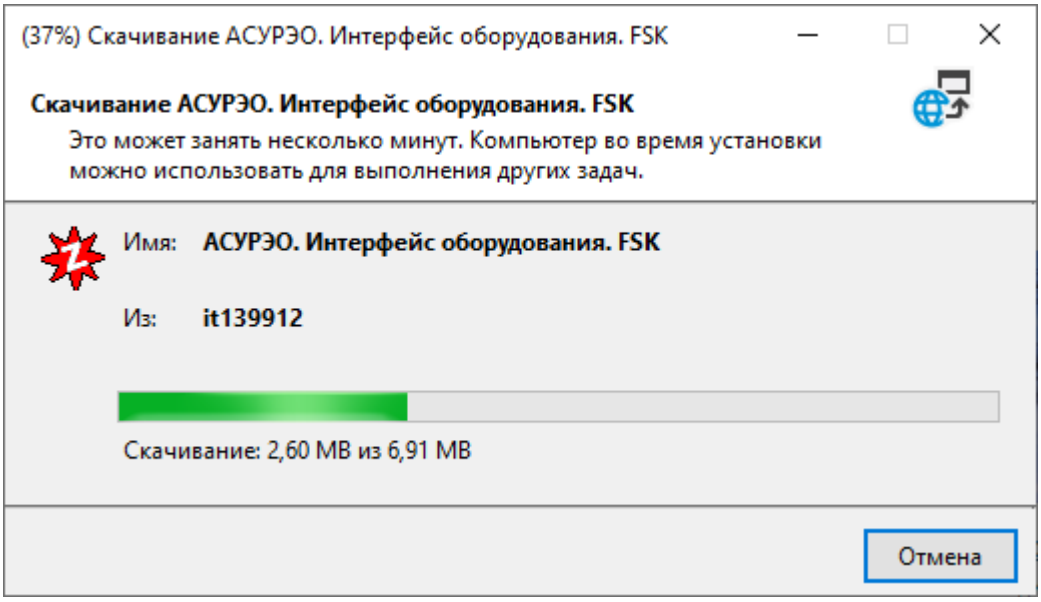

Рисунок 10.86 – Скачивание приложения

При скачивании клиентских интерфейсов ПК «АСУРЭО» ОС семейства Linux появляется предупреждение Windows о неопознанном приложении (Рисунок 10.87). Для успешного запуска приложения необходимо нажать кнопку *«Выполнить в любом случае»*. Отображение такого предупреждения является корректным для ОС семейства Linux.

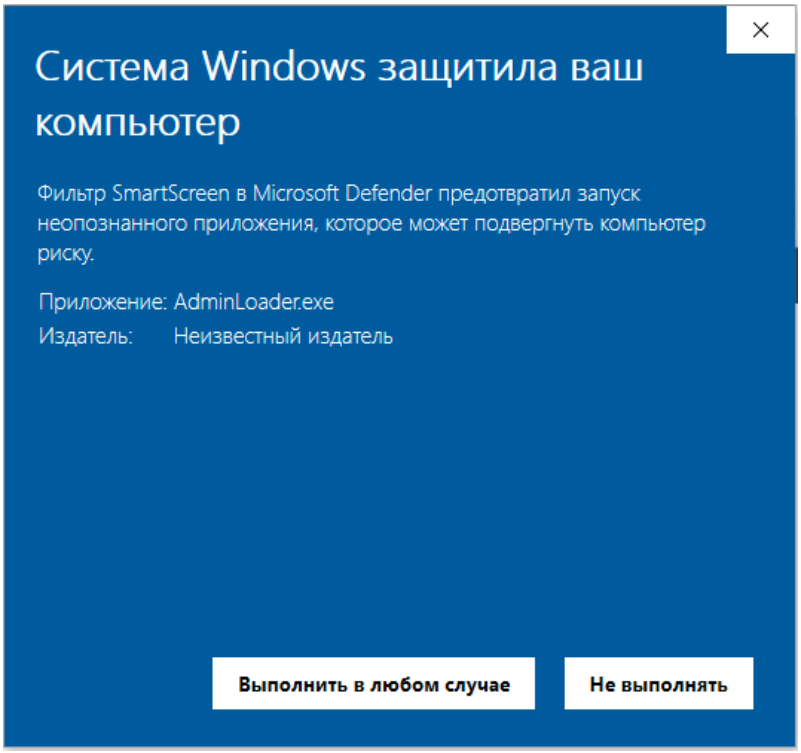

Рисунок 10.87 – Предупреждение Windows о неопознанном приложении

10.18.4Первый запуск ПК на рабочей станции

10.18.4.1 Общие сведения

При установке приложения инсталлятор создает ярлык на рабочем столе, который открывается браузером по умолчанию. Запуск приложения производится двойным щелчком мыши по ярлыку на рабочем столе.

При первом запуске ярлыка ПК пользователю предлагается установка компонентов программного комплекса на клиенте (Рисунок 10.88).

Внизу страницы отображаются ссылки со списком интерфейсов, они предназначены для запуска конкретного интерфейса.

Рисунок 10.88 – Установка ПК на клиенте

После перехода по ссылки открывается окно установки приложения (Рисунок 10.89).

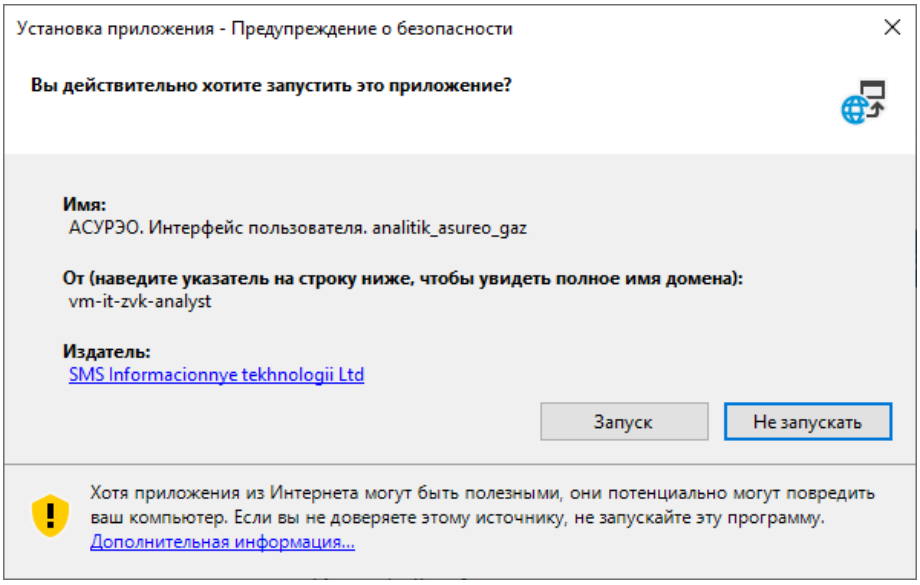

Рисунок 10.89 – Окно установки приложения

Для подтверждения запуска установки выбранного приложения необходимо нажать кнопку *«Запуск»*. После подтверждения запуска начинается скачивание выбранного приложения (Рисунок 10.90). Для отмены запуска установки выбранного приложения необходимо нажать на кнопку *«Не запускать»*.

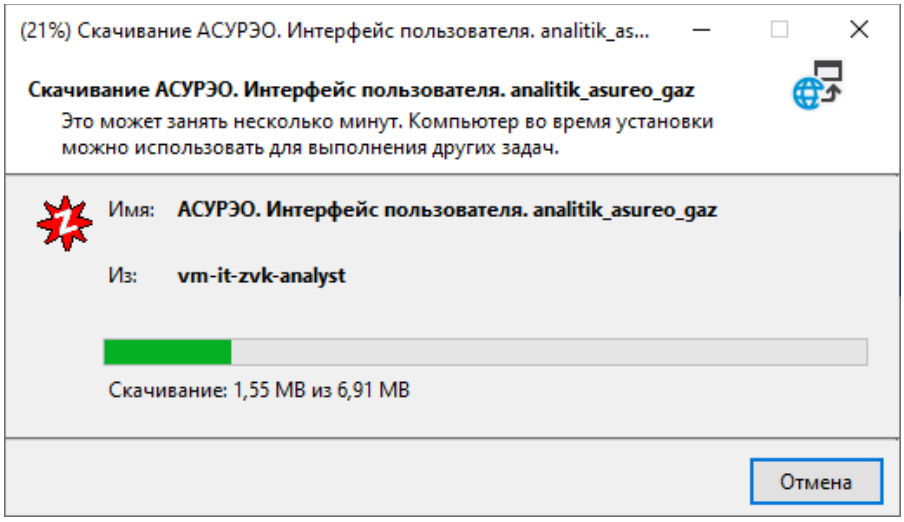

Рисунок 10.90 – Скачивание приложения

После чего запускается процесс установки приложения на рабочую станцию пользователя (Рисунок 10.91).

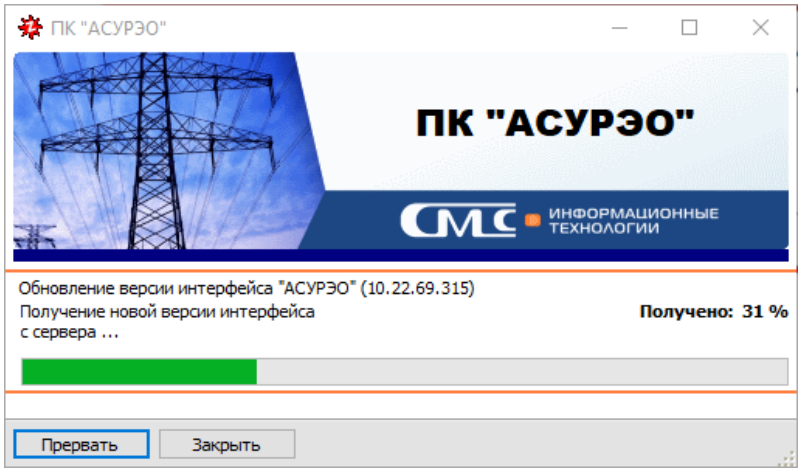

Рисунок 10.91 – Установка приложения

В процессе получения информации с сервера, если нажать на кнопку *«Прервать»*, то скачивание приостановится, кнопка изменится на *«Повторить»* (Рисунок 10.92).

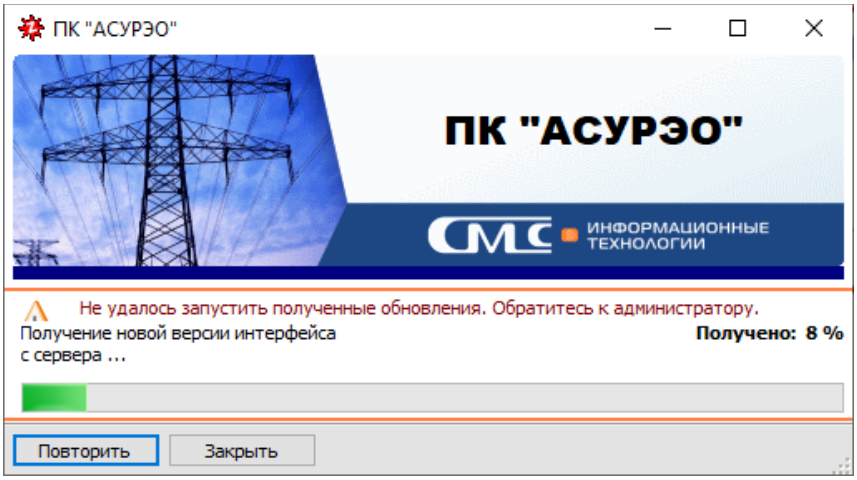

Рисунок 10.92 – Прерывание процесса загрузки обновлений

На данном шаге с сервера приложений запрашиваются и записываются на рабочую станцию пользователя файлы в директорию «C:\Program Files (x86)\ZVK».

Для стабильной работы пользовательских компонентов необходимо добавить директорию «C:\ProgramData\ZVK» в доверенную зону Kaspersky Security.

ZVK.exe	– загрузчик клиентских интерфейсов, обеспечивающий обновление исполняемых файлов интерфейсов на машине пользователя при их обновлении на сервере приложений.
ZVK.ini	– файл, автоматически создаваемый при первой загрузке, в котором хранятся параметры соединения с сервером приложений.

При обновлении ПК директория ZVK для ранних версий (5.X и ниже), расположенная по адресу «C:\Documents and Settings\<имя пользователя>\Application Data\», удаляется автоматически.

После успешного завершения процесса установки ПК на стороне клиента в папке «C:\ProgramData\ZVK» будет создан файл zvk.ini.

Пример:

[SERVER]
URL= http://192.168.7.8:0001

[Integration]
WAIT_TIMEOUT_MS=60000

[Session]
TimeZoneOffset=5

В секции [SERVER] указывается URL – адрес, по которому доступен сервер приложений.

В секции [Integration] указывается параметр WAIT_TIMEOUT_MS – время ожидания отклика ПК.

В секции [Session] указывается параметр TimeZoneOffset – использование заданного часового пояса:

- если параметр указан, то используется заданное значение часового пояса;
- если параметр отсутствует, то часовой пояс зависит от настройки Windows на клиентском ПК;
- если в качестве параметра не указано значение или указано некорректное значение (диапазон возможных значений -12…14), то отображается время UTC+0.

В случае возникновения ошибки при получении информации с сервера выдается соответствующее сообщение об ошибке (Рисунок 10.93).

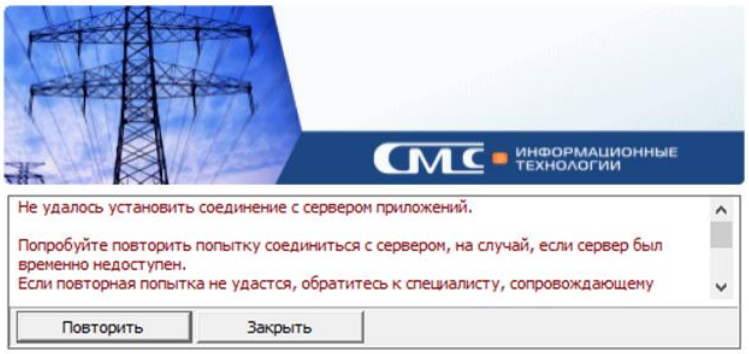

Рисунок 10.93 – Ошибка при получении пакета установки с сервера

После устранения причин ошибки необходимо запустить обновление версии приложения, нажав кнопку *«Повторить»*.

При загрузке с сервера приложений компонентов приложений на рабочей станции пользователя в директории «C:\ProgramData\ZVK» создается папка с номером версии ПК, соответствующая версии ПК на сервере. В папке содержатся файлы приложений, относящиеся к данной версии.

Пример:	
C:\ ProgramData \ZVK\10.20.115.0313\	– каталог, содержащий файлы интерфейсов ПК версии 10.20.115.0313.

DeviceDescr.exe ZVKAdmin.exe ZVKUser.exe	– файлы интерфейсов оборудования, администратора и пользователя для версии 10.20.115.0313.
alert.wav	- файл звукового оповещения о приходе новых заявок для рассмотрения (подгружается вместе с ZVKUser.exe).

После загрузки с сервера компонентов интерфейса на рабочую станцию пользователю открывается окно ПК с приглашением входа в приложение (Рисунок 10.94). В окне необходимо ввести имя и пароль пользователя.

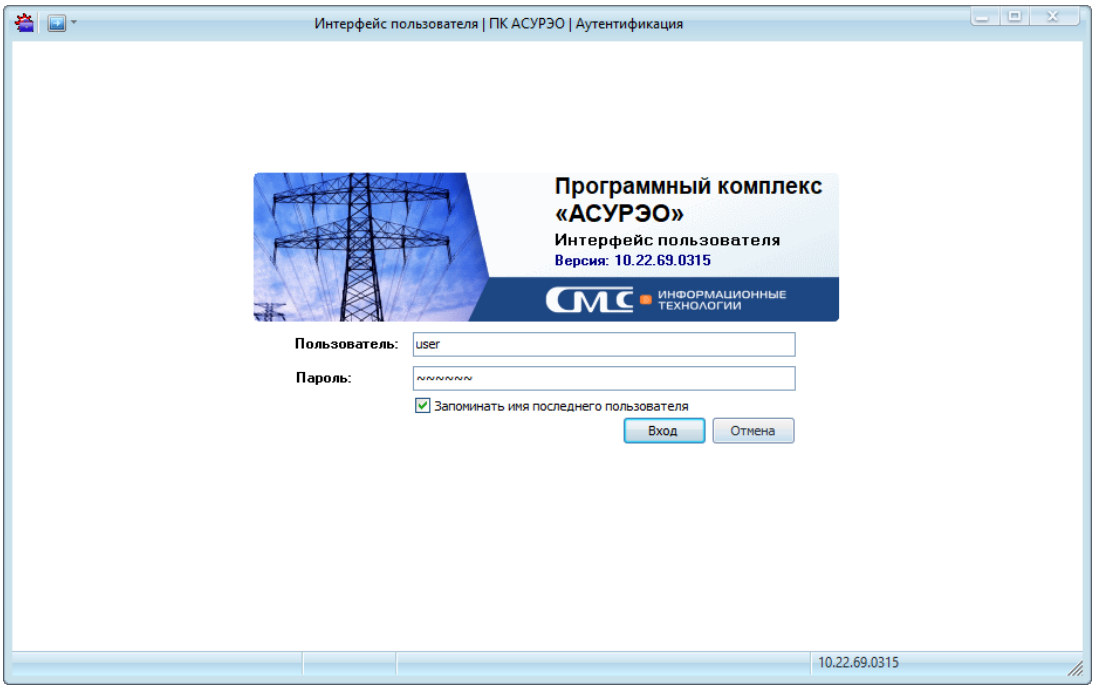

Рисунок 10.94 – Диалоговое окно входа в систему

В случае если пользователь успешно зарегистрирован в системе, то появится окно работы с выбранным интерфейсом со всеми доступными для данного пользователя функциями. Если пользователю установлен параметр *«Пользователь NT»*, то запуск интерфейса пользователя будет выполнен автоматически без ввода логина и пароля пользователя (подробнее о параметре «Пользователь NT» см. раздел «8.1.3.3 Настройки пользователя» руководства по работе с приложением «Интерфейс администратора»).

Внимание! Для корректной работы в заданном часовом поясе необходимо, чтобы настройки часового пояса операционной системы на клиентском рабочем месте совпадали с настройкой часового пояса в ПК (см. раздел «8.5.2 Общие настройки» руководства по работе с приложением «Интерфейс администратора»).

Внимание! При работе на одной машине с версиями 10.21.1025.0817 и предыдущими версиями АСУРЭО или экземпляром ИУС «СИМ-ЗРП» необходимо запускать интерфейсы из браузера (тогда стартер автоматически перезатягивается нужный). При запуске с созданных ярлыков могут наблюдаться проблемы. В случае возникновения проблем с запуском разных версий необходимо удалить стартер из папки «Program Data» вручную и заново запустить интерфейс.

10.18.5Создание ярлыка интерфейса пользователя на рабочей станции

При первоначальной установке компонентов, или в любой другой момент, пользователь создает себе на компьютере ярлыки для быстрого запуска интерфейса пользователя. На стартовой странице выбора интерфейсов по ссылке *«Создать ярлыки»* отображается панель с вариантами создания ярлыков (Рисунок 10.95).

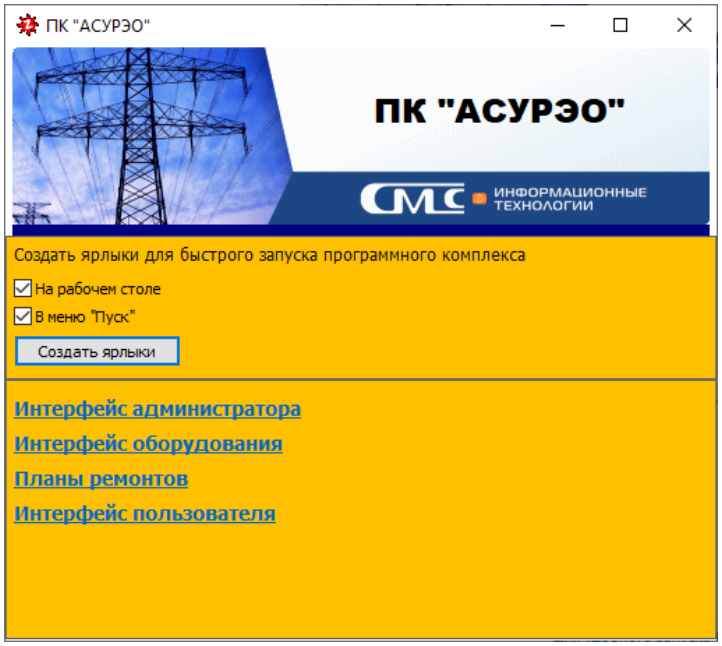

Рисунок 10.95 – Создание ярлыка

Ярлык для быстрого запуска интерфейса пользователя может быть создан:

– ***«На рабочем столе»*** – ярлык создается на рабочем столе пользователя.

– ***«В меню «Пуск»»*** – в меню «Программы» создается папка с именем «АСУРЭО» в ней создаются ярлыки для запуска интерфейса пользователя, администратора, оборудования и пользователя ремонтов.

Для создания ярлыков выбранные позиции помечаются флагом. По нажатию кнопки *«Создать ярлыки»*, создаются ярлыки в указанных местах. Название ярлыка состоит из имени приложения и названия текущего предприятия.

Автоматическое создание ярлыков на рабочем столе пользователя применяется только для интерфейса пользователя, как наиболее часто используемого. Создание отдельных ярлыков для запуска интерфейсов администратора, оборудования или пользователя ремонтов необходимо провести вручную. Для этого необходимо скопировать их из меню Пуск / Программы / АСУРЭО (Рисунок 10.96).

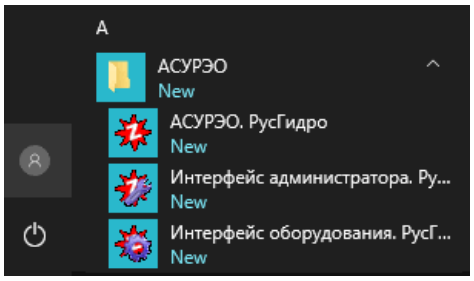

Рисунок 10.96 – Ярлыки интерфейсов в меню «Пуск»

10.18.6Обновление клиентской части ПК

При каждой загрузке интерфейса с рабочей станции на сервер запрашивается информация о соответствии версии компонентов интерфейса на клиенте с версией сервера. В случае, если на рабочей станции уже есть компоненты, соответствующие версии сервера (на клиенте есть папка C:\ProgramData\ZVK\<номер версии>\ с искомым интерфейсом, например пользователя - ZVKUser.exe), то производится запуск интерфейса. Если на рабочей станции компоненты, соответствующие версии сервера, не обнаружены (например, на сервере было выполнено обновление ПК до новой версии), то при запуске интерфейса на клиенте производится автоматическое обновление компонентов с сервера (Рисунок 10.97).

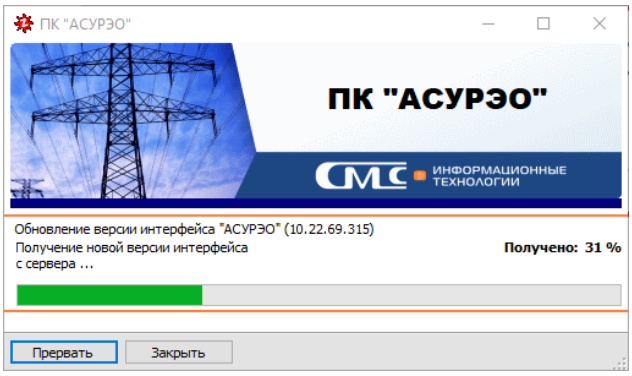

Рисунок 10.97 – Загрузка компонентов интерфейса пользователя с сервера

После обновления на рабочей станции пользователя в директории C:\ProgramData\ZVK» создается папка с новым номером версии ПК, соответствующая версии программного комплекса на сервере.

Таким образом, при каждом обновлении версии ПК на рабочей станции создается новая папка «C:\ProgramData\ZVK\<номер версии>\», содержащая компоненты приложений соответствующей версии, что позволяет пользователю работать одновременно с разными версиями программного комплекса без дополнительных манипуляций с компонентами.

Пример файловой структуры на рабочей станции:

C:\ProgramData\ZVK\ V10.20.115.0313	– каталог, содержащий файлы интерфейсов ПК версии 10.20.115.0313.
DeviceDescr.exe ZVKAdmin.exe ZVKUser.exe	– файлы интерфейсов оборудования, администратора и пользователя для версии 10.20.115.0313.
alert.wav	- файл звукового оповещения о приходе новых заявок для рассмотрения (подгружается вместе с ZVKUser.exe).
C:\ProgramData\ZVK\ V10.20.115.0313	– каталог, содержащий файлы интерфейсов ПК версии 10.20.115.0313.
DeviceDescr.exe ZVKAdmin.exe ZVKUser.exe	– файлы интерфейсов оборудования, администратора и пользователя для версии 10.20.115.0313.
alert.wav	- файл звукового оповещения о приходе новых заявок для рассмотрения (подгружается вместе с ZVKUser.exe).

10.18.7Хранимые версии

На рабочей станции пользователя в директории «C:\ProgramData\ZVK» хранятся папки с номером версии подсистемы (только для трех последних версий подсистемы), в которых хранятся файлы для работы с их клиентскими положениями:

- в случае, если в директории ZVK хранятся файлы только для одной/двух версий подсистемы (например, в папках «V7.XXXX.XX.XX», «V8.XXXX.XX.XX»), то при обновлении подсистемы файлы для работы с клиентским приложением новой версии записываются в директорию ZVK в автоматически созданную папку с номером версии подсистемы (например, «V9.XXXX.XX.XX»);

- в случае, если в директории ZVK хранятся файлы для трех версий подсистемы (например, в папках «V7.XXXX.XX.XX», «V8.XXXX.XX.XX» и «V9.XXXX.XX.XX»), то при обновлении подсистемы из директория ZVK автоматически удаляется папка с файлами для наиболее ранней версии (в данном примере папка «V7.XXXX.XX.XX»), а файлы для работы с клиентским приложением новой версии записываются в директорию ZVK в автоматически созданную папку с номером версии подсистемы (например, «V10.XXXX.XX.XX»).

Существует возможность настройки количества хранимых версий интерфейса.

Для этого необходимо в файл zvk.ini в секцию [Addition Functions] добавить параметр CachedClientVersionCount = <Необходимое количество хранимых версий> подробнее в разделе «10.10 Описание параметров файла zvk.ini». В качестве необходимого количества хранимых версий можно указать значения от 4 до 9. При указании других значений будут храниться по умолчанию файлы трех последних версий подсистемы.

На рабочей станции пользователя в директории «C:\ProgramData\ZVK» будут храниться папки с номером версии подсистемы (для указанного количества последних версий подсистемы), в которых будут содержаться файлы для работы с их клиентскими положениями.

Примечание. При загрузке экземпляра, у которого не подключен параметр CachedClientVersionCount, удаляются старые версии в директории «C:\ProgramData\ZVK» и по умолчанию остается 3 последние версии подсистемы.

10.18.8 Установка клиентской части Системы на ОС Astra Linux

Для установки клиентов ПК «АСУРЭО» с помощью средства эмуляции Wine в терминале необходимо выполнить следующие действия:

1. Установка Wine и Winetricks

   - **Alt Linux**
     - Обновить список пакетов: *sudo apt-get update*
     - Установить пакеты wine: *sudo apt-get install wine winetricks i586-wine –y*
   - **Astra Linux**
     - Обновить список пакетов: *sudo apt update*

– Установить пакеты wine: *sudo apt install wine*

– Установить пакеты Winetricks: *sudo apt install winetricks*

И обновить до новой версии: *sudo winetricks --self-update*

2. Установка компонент dotnet для запуска файлов application.

- Установить dotnet: *winetricks dotnet45*
- На всплывающем окне «Установка Wine Mono» нажать кнопку «Установить» (Рисунок 10.98).

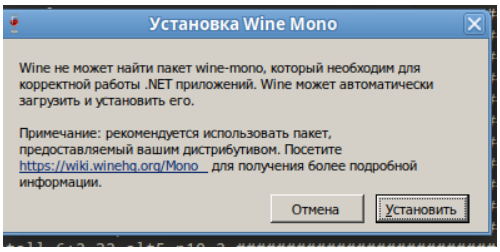

Рисунок 10.98 – Всплывающее окно «Wine Mono»

- Принять лицензионное соглашение и нажать кнопку «Установить» (Рисунок 10.99), после установки нажать копку «Готово» (Рисунок 10.100).

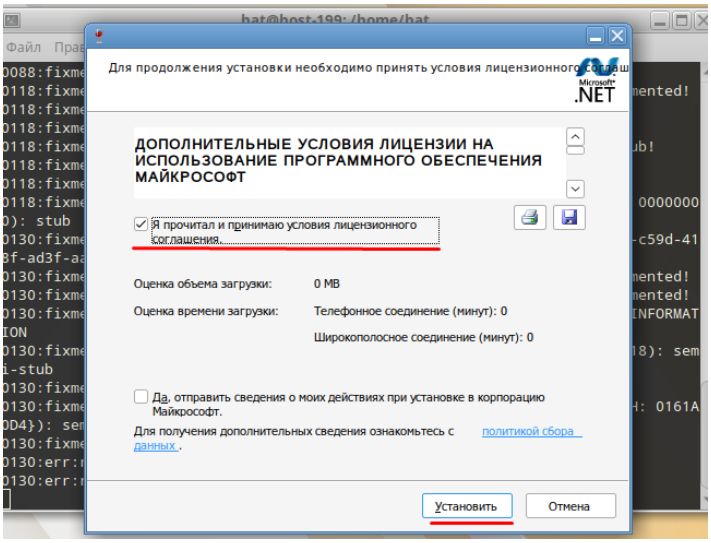

Рисунок 10.99 – Принятие лицензионного соглашения

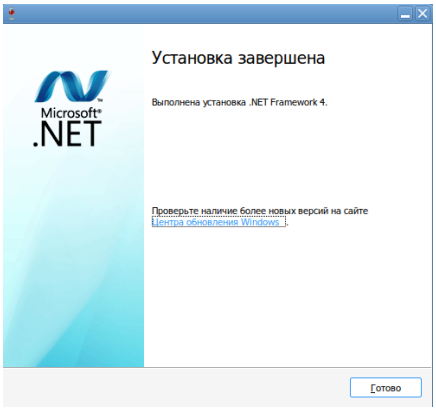

Рисунок 10.100 – Завершение установки

- Далее в окне «Майкрософт .NET Framework 4.5» нажать кнопку «Продолжить» (Рисунок 10.101).

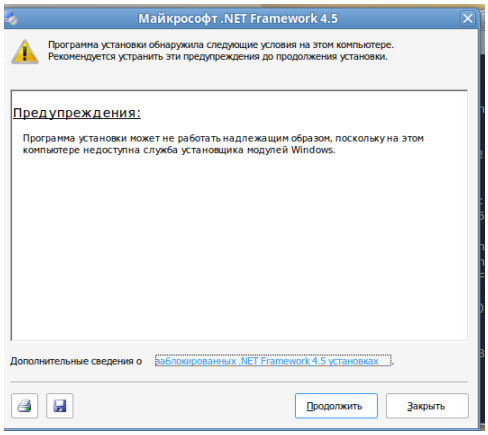

Рисунок 10.101 – Окно «Майкрософт .NET Framework 4.5»

- Принять лицензионное соглашение и нажать на кнопку «Установить» (Рисунок 10.102)

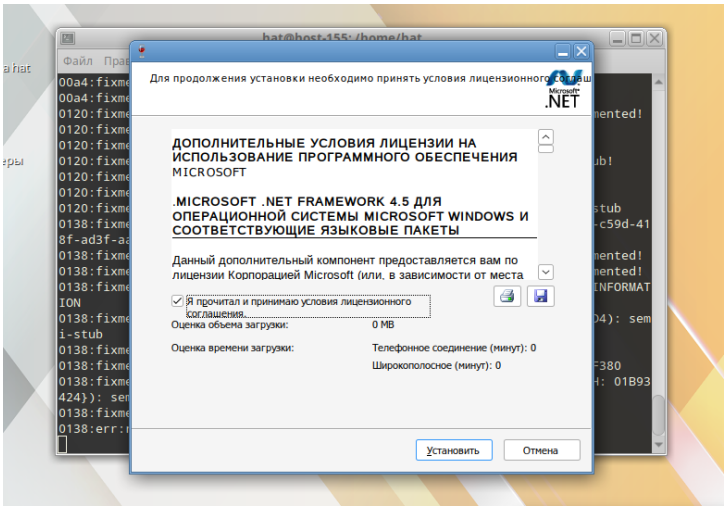

Рисунок 10.102 – Принятие лицензионного соглашения

- Скачать интерфейс ПК «Заявки» с индексовой страницы (Рисунок 10.103).

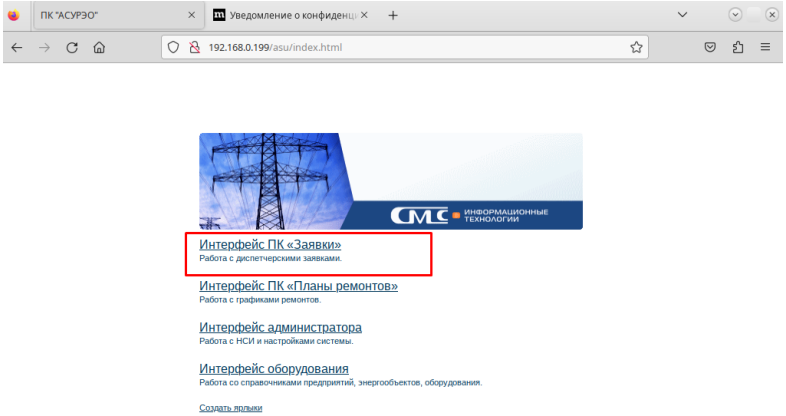

Рисунок 10.103 – Скачивание интерфейса

- Запустить приложение:

  wine /home/$USER/Загрузки/ZvkUserLoader.application

  Либо открыть проводник – ***wine explorer***, и запустить интерфейс двойным нажатием (Рисунок 10.104).

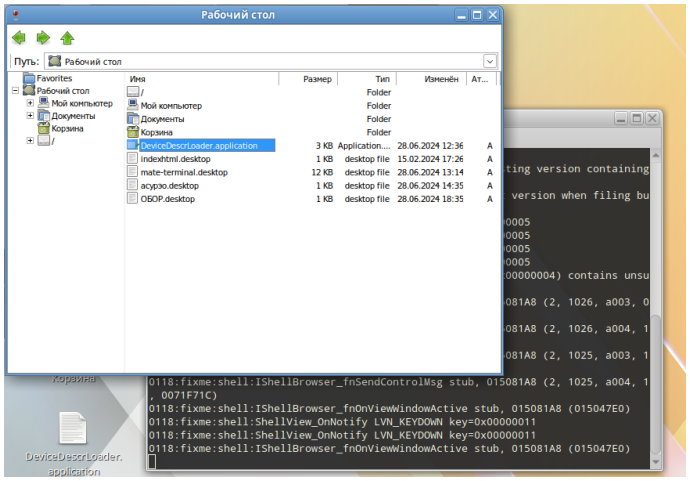

Рисунок 10.104 – Запуск интерфейса

- Zvk.exe создается по пути:

  /home/$USER/.wine/drive_c/ProgramData/ZVK/Zvk.exe

  Можно создать ярлык – ПКМ на рабочем столе ALT OS – Создать кнопку запуска – в поле указать команду (Рисунок 10.105):

  ***«wine /home/$USER/.wine/drive_c/ProgramData/ZVK/Zvk.exe»*** ($USER нужно заменить на имя пользователя, так как из ярлыка переменную не считывает).

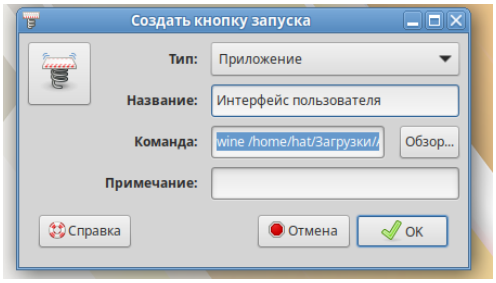

Рисунок 10.105 – Создание кнопки запуска

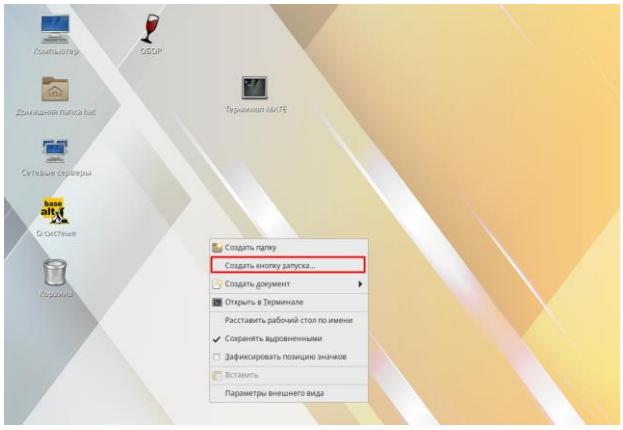

Рисунок 10.106 – Создание кнопки запуска

- Пользователь заходит в Интерфейс пользователя через ярлык (Рисунок 10.107).

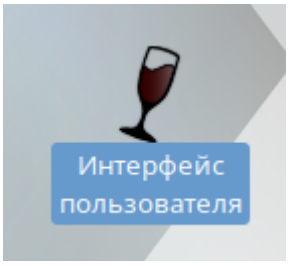

Рисунок 10.107 – Ярлык Интерфейса пользователя

10.18.8.1 Установка клиентской части Системы с самораспаковывающегося архива

Для удобства первичной установки Системы на рабочие места пользователей имеется возможность установки комплекса через самораспаковывающийся архив (makeself), предварительно сформированный администратором на своем рабочем месте. В данном способе не требуется установка компонента dotnet45 на рабочие места пользователей.

Для этого необходимо, на рабочем месте администратора:

1. Выполнить установку системы вручную, согласно рекомендациям раздела «10.18.8 Установка клиентской части Системы на ОС Astra Linux».
2. Скопировать все необходимые файлы клиентской части комплекса (каталог /home/$USER/.wine/drive_c/ProgramData/ZVK) в отдельный каталог, например: /home/$USER/asureo.
3. В этом же каталоге создать файл-ярлык, который будет размещаться на рабочих столах пользователей:

   nano ASUREO.desktop

   внести содержимое:

   [Desktop Entry]
   Name=АСУРЭО
   Type=Application
   NoDisplay=false
   Exec=bash -c 'wine /home/$USER/.wine/drive_c/ProgramData/ZVK/Zvk.exe URL=http://192.168.0.100:85/appsrv/proxy.dll INTF=ZVKUser.exe'
   Icon=application-x-executable
   Hidden=false

Terminal=false

StartupNotify=false

где,

- *Name* – имя ярлыка, можно задать любое;
- *Exec* – команда запуска интерфейса ПК «АСУРЭО», где:
  - *wine /home/$USER/.wine/drive_c/ProgramData/ZVK/Zvk.exe* – команда запуска. Указание обязательно;
  - *URL=http://**192.168.0.100:85**/appsrv/proxy.dll* – адрес сервера приложений ПК «АСУРЭО». Указание не обязательно. URL требуется если на клиенте планируется запуск комплекса АСУРЭО разных предприятий (комплекса с разных серверов приложений);
  - *INTF=DeviceDescr.exe* – интерфейс запуска. Указание не обязательно, по умолчанию запускается интерфейс пользователя ПК Заявки. Допустимо указание:
    - ZVKUser.exe – интерфейс пользователя ПК Заявки;
    - RPUser.exe – интерфейс ПК Планы ремонтов;
    - DeviceDescr.exe – интерфейс оборудования;
    - ZVKAdmin.exe – интерфейс администратора.

Допускается создание нескольких файлов для создания нескольких ярлыков с разным наименованием.

4. В том же каталоге /home/$USER/asureo создать скрипт распаковки клиентских файлов:

nano extract_ASUREO.sh

внести содержимое:

```
#!/bin/bash

# Проверяем, где находится папка рабочего стола
if [ -d "$HOME/Desktop" ]; then
   DESKTOP="$HOME/Desktop"
elif [ -d "$HOME/Рабочий стол" ]; then
   DESKTOP="$HOME/Рабочий стол"
else
   echo "Не удалось найти папку рабочего стола!"
```

```
    exit 1
fi

# Распаковываем ZVK в путь, соответствующий Wine
mkdir -p "$HOME/.wine/drive_c/ProgramData/ZVK"
cp -r ./ZVK/* "$HOME/.wine/drive_c/ProgramData/ZVK/"

# Копируем ASUREO.desktop на рабочий стол, если файлов-ярлыков было создано несколько – то скопировать все
cp ./ASUREO.desktop "$DESKTOP/"
```

сделать скрипт исполняемым: *chmod +x extract_ASUREO.sh*

5. Для формирования самораспаковывающего архива установить необходимое ПО **makeself** в любой удобный каталог, например */opt/*:

   Загрузить makeself:

   wget https://github.com/megastep/makeself/releases/download/release-2.5.0/makeself-2.5.0.run

   Сделать исполняемым: *chmod +x makeself-2.5.0.run*

   Запустить: *./makeself-2.5.0.run*

   Перейти в каталог: *cd /opt/makeself-2.5.0/*

   Сделать скрипт makeself.sh исполняемым: *chmod +x makeself.sh*

6. Сформировать архив с клиентской частью ПК АСУРЭО, для этого из каталога /opt/makeself-2.5.0/ выполнить команду:

   ./makeself.sh --gzip /home/$USER/asureo/ ASUREO_installer.run "ASUREO Installer" ./extract_ASUREO.sh, где

   - *--gzip* – указывает на использование сжатия;
   - */home/$USER/asureo/* – путь к директории, где находятся файлы, которые будут упакованы. Необходимо указать имя вашего пользователя;
   - *ASUREO_installer.run* – имя создаваемого архива;
   - *"ASUREO Installer"* – строка, которая будет отображаться при запуске архива;
   - *./extract_ASUREO.sh* – путь к скрипту, который будет выполняться при запуске (он будет находится в корне собранного архива).

Переместить полученный архив ASUREO_installer.run на рабочие места пользователей вручную или следовать рекомендациям из раздела «10.18.8.2 Размещение самораспаковывающегося архива на веб-сервере IIS».

На рабочих местах пользователей выполнить следующие действия:

1. Установка Wine и Winetricks
   - **Alt Linux**
     - Обновить список пакетов: *sudo apt-get update*
     - Установить пакеты wine: *sudo apt-get install wine winetricks i586-wine -y*
   - **Astra Linux**
     - Обновить список пакетов: *sudo apt update*
     - Установить пакеты wine: *sudo apt install wine*
     - Установить пакеты Winetricks: *sudo apt install winetricks*

   И обновить до новой версии: *sudo winetricks --self-update*
2. Для распаковки самораспаковывающегося архива выполнить с правами администратора:

   Сделать архив исполняемым: *chmod +x ASUREO_installer.zip*

   Запустить архив: *./ASUREO_installer.zip*

   На рабочем столе пользователя появится ярлык АСУРЭО, запустив, который начнётся установка клиентского приложения Системы. При необходимости в свойствах ярлыка возможно изменение адреса до сервера приложений.
3. При первом запуске комплекса на рабочем столе потребуется установка Wine Mono, на всплывающем окне «Установка Wine Mono» необходимо нажать кнопку «Установить» (Рисунок 10.108).

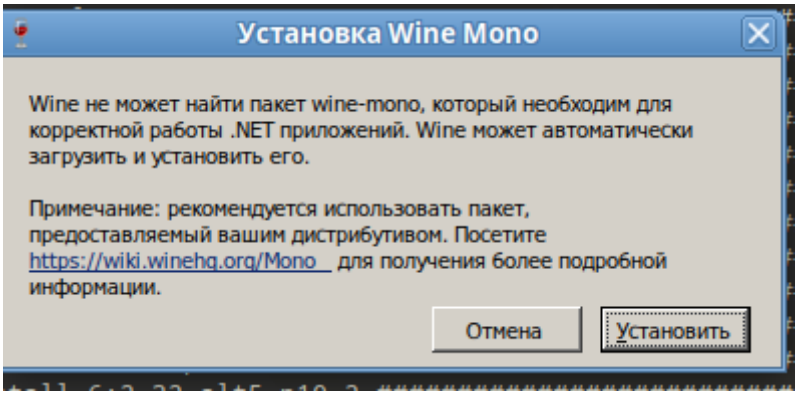

Рисунок 10.108 – Всплывающее окно «Wine Mono»

В дальнейшем, при обновлении версии ПК «АСУРЭО» на сервере, выше описанные действия по установке клиента на рабочих местах пользователей выполнять не потребуется.

На стороне клиента потребуется закрыть все запущенные интерфейсы предыдущей версии и повторно запустить клиент через ярлык – при этом автоматически на машину пользователя подгрузится обновлённая версия приложения.

Клиент Delphi необходимо запускать только на физическом хосте с ОС Linux.

10.18.8.2 Размещение самораспаковывающегося архива на веб-сервере IIS

Для возможности массового распространения среди пользователей ранее собранного самораспаковывающегося архива существует возможность создать виртуальный каталог на веб-сервере и получить доступ к архиву по единому URL.

Для этого на сервере в каталоге экземпляра АСУРЭО (по умолчанию C:\Program Files\Zvk\{имя_экземпляра}) необходимо создать новую папку, например, clientLin, и разместить в неё ранее сформированный самораспаковывающий архив ASUREO_installer.zip.

На веб-сервере IIS необходимо добавить новый виртуальный каталог и привязать его к ранее созданной папке C:\Program Files\Zvk\{имя_экземпляра}\clientLin (Рисунок 10.109).

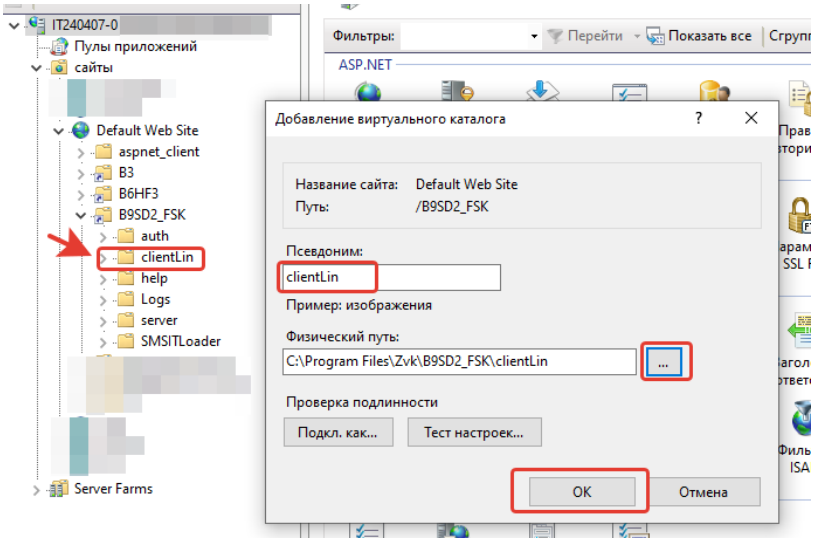

Рисунок 10.109 – Создание виртуального каталога в IIS

Для доступа к данному каталогу по URL необходимо в настройке редактора конфигураций IIS для раздела system.webServer/directoryBrowse указать значение «True» в атрибуте «enabled» и нажать кнопку «Применить» (Рисунок 10.110).

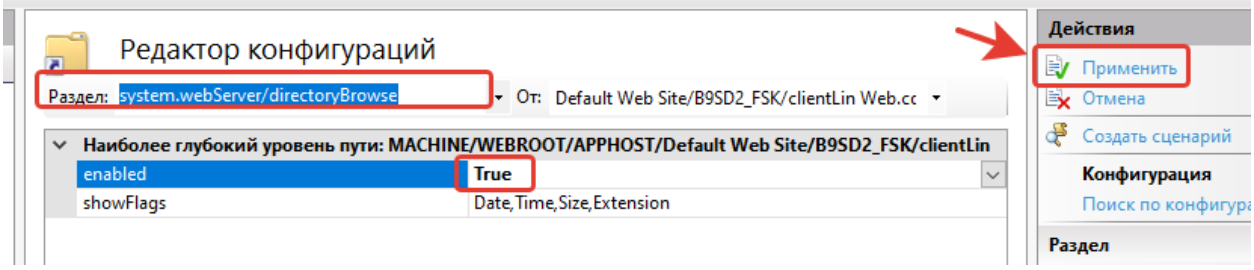

Рисунок 10.110 – Настройка редактора конфигураций IIS

После выполненных вышеуказанных действий самораспаковывающий архив ASUREO_installer.zip доступен к скачиванию по URL: http(s)://xx.xxx.xx.xxx/<имя экземпляра>/clientLin, где

- xx.xxx.xx.xxx – ip-адрес или полное имя сервера;
- <имя экземпляра> – название установленного экземпляра ПК АСУРЭО;
- clientLin – имя виртуального каталога, созданный ранее в IIS для размещения самораспаковывающего архива.

10.19 Проверка работоспособности ПК после установки

Для проверки работоспособности ПК после установки, администратору необходимо выполнить следующие действия.

1. Запустить и осуществить вход во все интерфейсы ПК, убедиться, что вход в интерфейсы осуществляется.

2. В интерфейсе администратора в разделе «Журналы», открыть вкладку «Системный журнал», далее выбрать «Пользовательский», убедиться, что вход в интерфейсы зафиксировался в журнале.

3. Перейти в Интерфейс пользователя ПК «АСУРЭО», открыть любую заявку на просмотр.

4. Перейти в Интерфейс пользователя ПК «Планы ремонтов», открыть любой график на просмотр.

10.20 Откат к предыдущей версии ПК

В случае, если обновление осуществить не удалось, либо не удаётся произвести проверку корректности работы ПК, необходимо произвести процедуру отката. Для этого необходимо выполнить следующие действия.

1. Создать резервную копию БД, хранить до установления причин неуспешного обновления;

2. Деинсталлировать ПК (см. раздел «10.21 Удаление ПК»), предварительно сохранив копию содержимого директории установки (папка установки экземпляра по умолчанию «C:\Program Files (x86)\ZVK\<название экземпляра>\»), хранить до установления причин неуспешного обновления;

3. Восстановить БД из резервной копии сделанной до обновления ПК (см. раздел «11.6 Восстановление БД»);

4. Установить ПК из дистрибутива предыдущей версии (см. раздел «10.6 Установка АСУРЭО на СУБД MSSQL/PostgreSQL»);

5. Проверить работоспособность установленного ПО.

10.21 Удаление ПК «АСУРЭО» на ОС MS Windows

Удаление ранее установленных экземпляров ПК «АСУРЭО» на ОС MS Windows может быть произведено с помощью программы установки ПК «*setup.exe*» (см. раздел «10.6 Установка АСУРЭО на СУБД MSSQL/PostgreSQL»).

С помощью программы установки ПК «*setup.exe*» для удаления экземпляров необходимо в окне мастера *«Выбор производных действий»* выбрать пункт *«Удалить экземпляры»* и в списке *«Установленные экземпляры»* выбрать нужные экземпляры (Рисунок 10.111). Выбор нескольких экземпляров производится с помощью клавиш *«Shift»* / *«Ctrl»*.

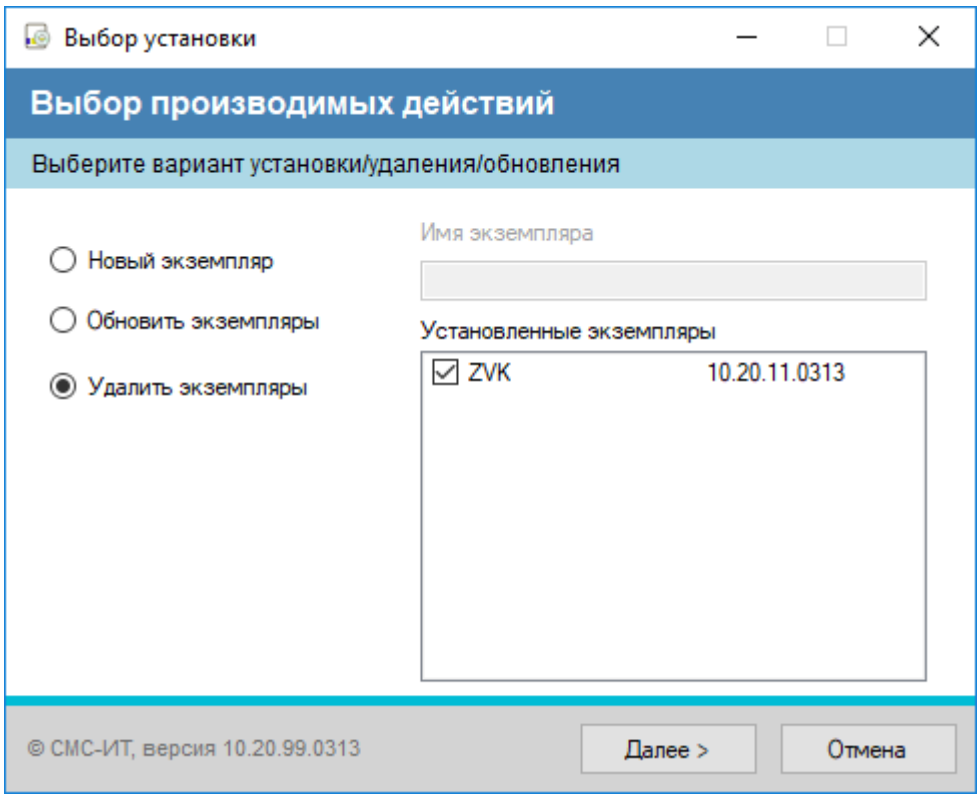

Рисунок 10.111 – Выбор экземпляра для удаления

На следующем шаге, если установить флаг *«Удалить файлы пользователя»* (по умолчанию – установлен), то производится удаление всех файлов из каталога установки экземпляра (Рисунок 10.112). Если флаг снят, то созданные пользователем файлы в директории экземпляра и журнала сервера приложений не удаляются. Удаление БД, с которой работал экземпляр, не производится.

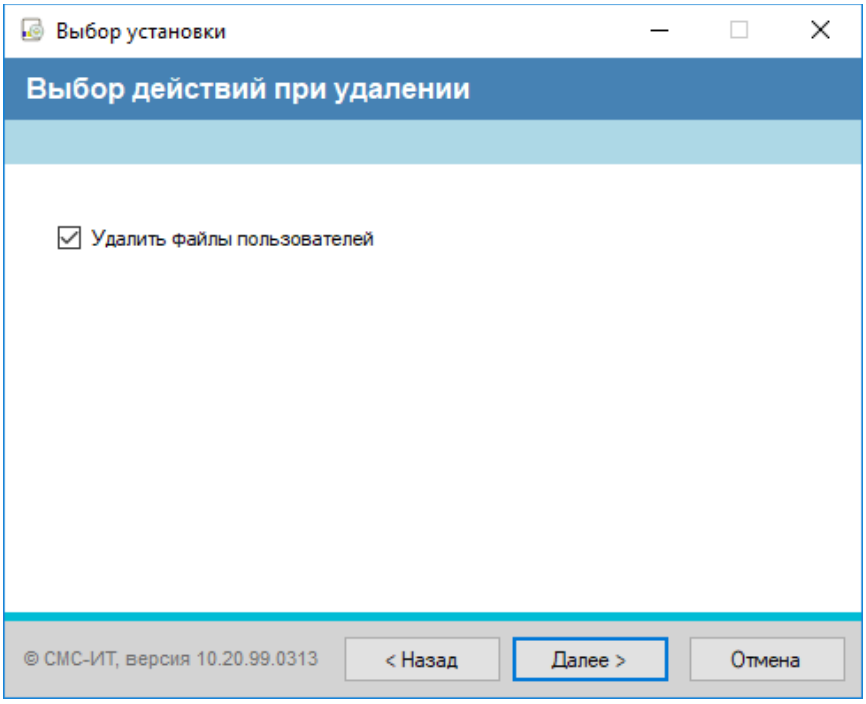

Рисунок 10.112 – Установка флага «Удалить файлы пользователей»

По окончанию процесса удаления выбранных экземпляров появляется окно завершения мастера установки (Рисунок 10.113).

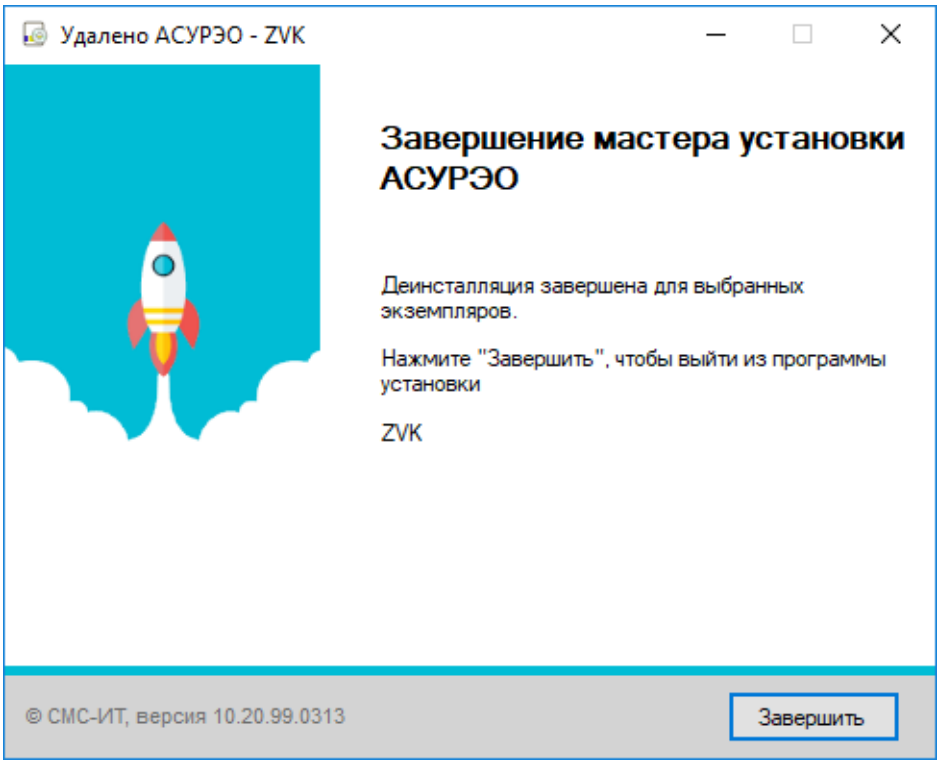

Рисунок 10.113 – Завершение удаления

Для выхода из программы удаления необходимо нажать на кнопку *«Завершить»*.

10.22 Удаление ПК «АСУРЭО» на ОС семейства Linux

Удаление ранее установленного ПК «АСУРЭО» на ОС семейства Linux может быть произведено путём удаления docker контейнера и docker образа. Для удаления необходимо выполнить следующие действия:

1. Вывести весь список docker контейнеров. Выполнить команду: *docker ps* (Рисунок 10.114).

```
root@astral:/opt/asureo# docker ps
CONTAINER ID        IMAGE                  COMMAND             CREATED             STATUS
            PORTS                                       NAMES
3d27b66245ef          asureo    :latest   "bash"              58 seconds ago      Up 30 se
conds       0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp   asureo
```

Рисунок 10.114 – Выполнение команды docker ps

2. Остановить docker контейнер asureo. Выполнить команду: *docker stop asureo* (Рисунок 10.115).

```
root@astral:/opt/asureo# docker stop asureo
asureo
```

Рисунок 10.115 – Выполнение команды docker stop asureo

3. Удалить docker контейнер asureo. Выполнить команду: *docker rm asureo* (Рисунок 10.116).

```
root@astral:/opt/asureo# docker rm asureo
asureo
```

Рисунок 10.116 – Выполнение команды docker rm asureo

4. Вывести список docker образов. Выполнить команду: *docker image ls* (Рисунок 10.117).

```
root@astral:/opt/asureo# docker image ls
REPOSITORY                          TAG                 IMAGE ID            CREATED
      SIZE
dpage/pgadmin4                      latest              94c0924749b6        13 days ago
      366MB
asureo                              latest              2a6f7883db56        2 weeks ago
      543MB
```

Рисунок 10.117 – Выполнение команды docker image ls

5. Удалить docker образ asureo. Выполнить команду: *docker rmi asureo* (Рисунок 10.118).

```
root@astral:/opt/asureo# docker rmi asureo
asureo
```

Рисунок 10.118 – Выполнение команды docker rmi asureo

6. Удалить папку /opt/asureo. Выполнить команду: *rm -r /opt/asureo* (Рисунок 10.119).

```
root@astral:/opt/asureo# rm -r /opt/asureo
```

Рисунок 10.119 – Выполнение команды rm -r /opt/asureo

11 Резервное копирование данных ПК на СУБД MS SQL

11.1 Общие сведения

Под резервированием данных ПК понимается создание резервной копии базы данных текущего экземпляра программного комплекса на сервере базы данных.

Резервирование выполняется на СУБД MS SQL 2016 / 2019. Для проведения процедуры резервного копирования необходимо выполнить следующие действия:

1) Определить место хранения будущей резервной копии.

2) Создать устройство / псевдоним для SQL Server, указывающий место хранения резервной копии.

3) Настроить опции процесса резервного копирования, в том числе установить расписание, по которому в дальнейшем будет проводиться резервирование.

4) Запустить процедуру резервного копирования.

11.2 Создание устройства

В приложении *Server Management Studio Express* для сервера нужно выбрать узел *Server Objects*, а в нем элемент *Backup Devices*. Щелкнув правой кнопкой мыши на нем, выберите пункт *New Backup Device*. В открывшемся диалоговом окне нужно указать псевдоним для будущей резервной копии (Name) и выбрать ее место расположения (*File name*) (Рисунок 11.1).

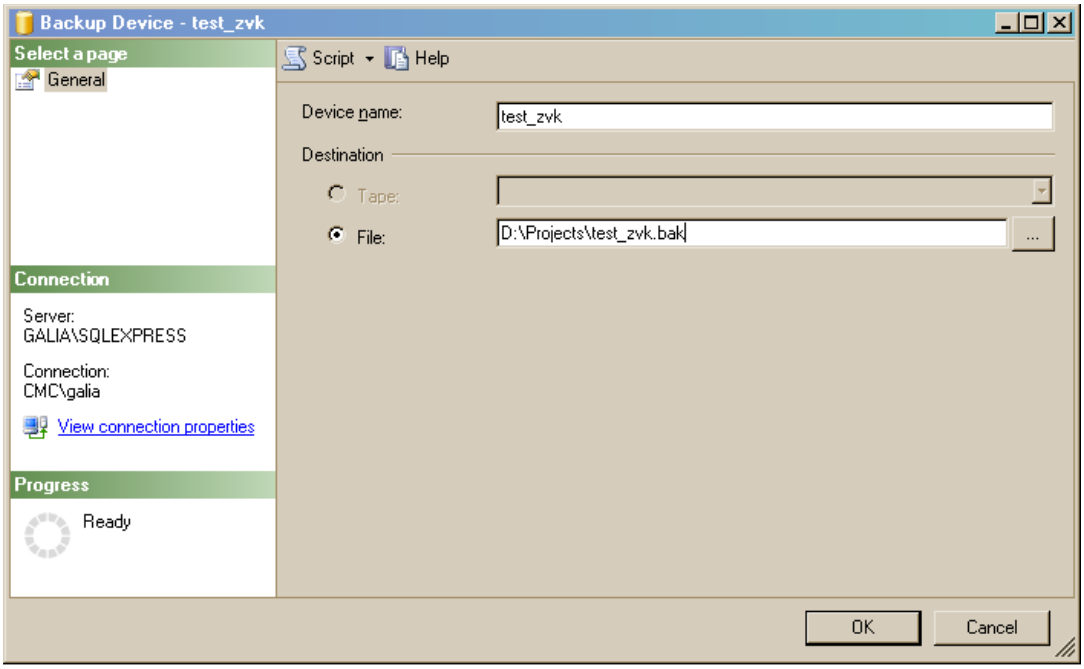

Рисунок 11.1 – Создание устройства для хранения резервной копии

11.3 Предварительные условия

Если в БД используется «full» модель восстановления или восстановления с неполным протоколированием, то необходимо регулярно создавать резервную копию журнала транзакций, чтобы защитить данные и предотвратить переполнение журнала транзакций. При этом журнал усекается с помощью компонента «Компонент Database Engine» и поддерживает восстановление БД на определенный момент времени.

Если резервная копия журнала транзакций создается первый раз, то для того, чтобы разрешить компоненту «Компонент Database Engine» усечение журнала транзакций до контрольной точки, необходимо создать вторую резервную копию журнала транзакций.

Для корректной работы ПК, необходимо предотвратить переполнение журнала транзакций и заполнения физического диска, выполнив настройку плана обслуживания БД, а именно полное резервное копирование и резервное копирование журнала транзакций (см. раздел «11.4 Последовательность действий по настройке плана обслуживания БД»).

В данном разделе указаны рекомендуемые параметры настройки задач резервного копирования базы данных и лога транзакций, а также задача очистки данных после обслуживания. Т.к. полная резервная копия служит основным источником данных в случае сбоя системы рекомендуемая периодичность создания резервных копий раз в сутки. При этом размер резервной копии не будет резко увеличиваться и восстановление системы будет

занимать прогнозируемое время. Для обеспечения надежности системы и возможности восстановления на любой момент времени рекомендуется выполнять резервное копирование журнала транзакций раз в час. Данные рекомендации носят общий характер и могут быть скорректированы в частном случае.

Настройка плана обслуживания возможна на редакции SQL Server Standard и выше.

11.4 Последовательность действий по настройке плана обслуживания БД

Для настройки плана обслуживания БД необходимо выполнить следующие действия:

1) Открыть «MS SQL Management Studio».

2) В Object Explorer раскрыть папку *«Management»*, кликнуть правой кнопкой мыши по папке *«Maintenance Plans»* и из контекстного меню выбрать пункт *«Maintenance Plan Wizard»* (Рисунок 11.2).

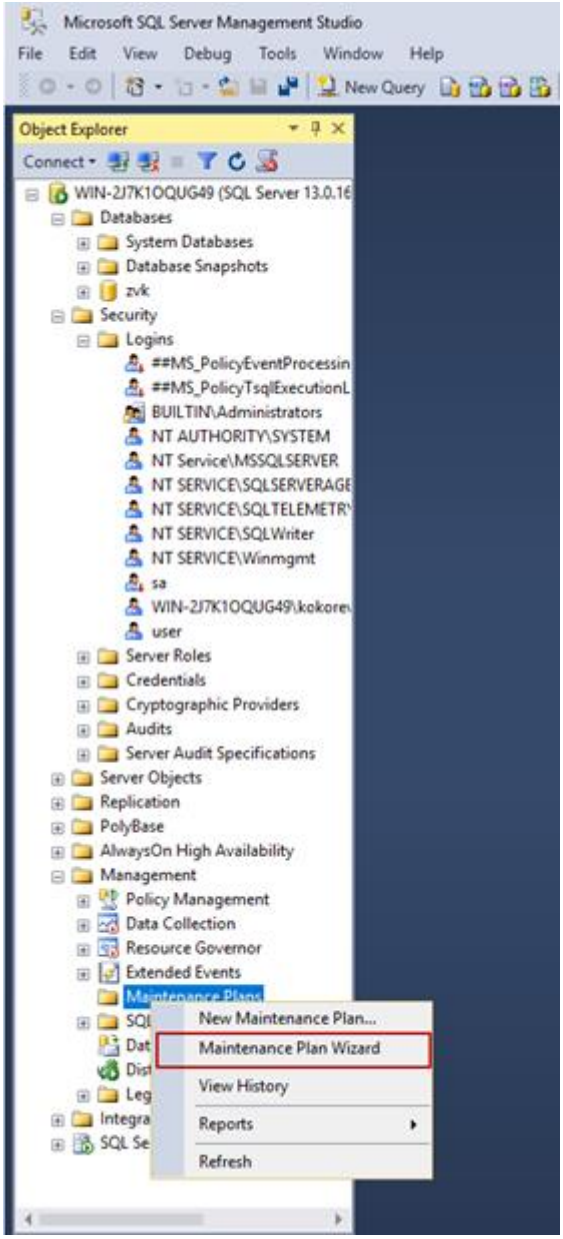

Рисунок 11.2 – Выбор пункта «Maintenance Plan Wizard»

3) В запустившемся *Maintenance Plan Wizard* на странице приветствие нажать кнопку «*Next*».
4) На шаге *«Select Plan Properties»* выполнить следующие действия (Рисунок 11.3):
   - указать имя и описание нового плана;
   - установить опцию *«Separate schedule for each task»*;
   - нажать кнопку *«Next»*.

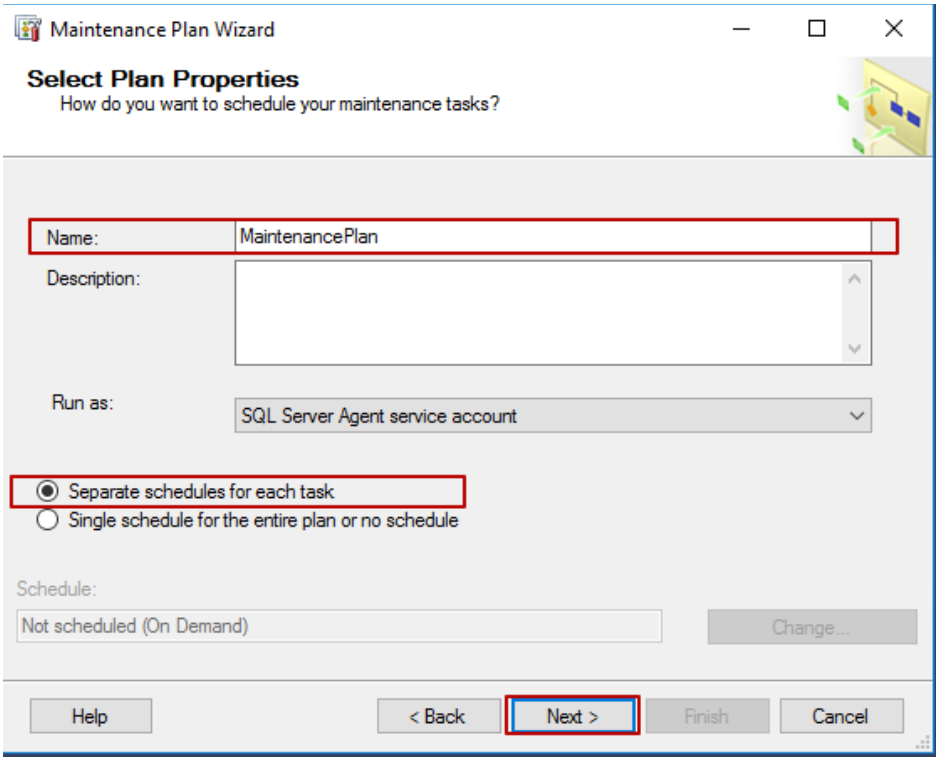

Рисунок 11.3 – Шаг «Select Plan Properties»

5) На шаге *«Select Maintenance Tasks»* выбрать задачи: *«The Back Up Database (Full)»*, *«The Back Up Database (Transaction Log)»*, *«Maintenance Cleanup Task»* и нажать кнопку *«Next»* (Рисунок 11.4).

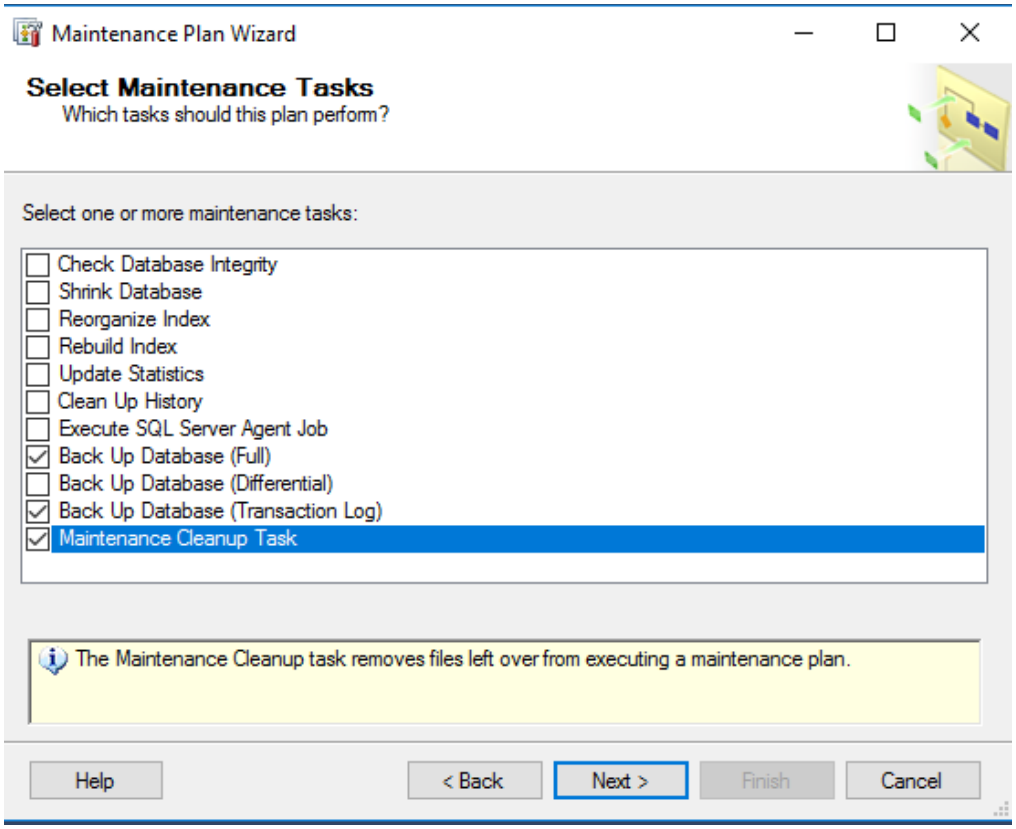

Рисунок 11.4 – Шаг «Select Maintenance Tasks»

6) На шаге *«Select Maintenance Task Order»* задать порядок выполнения задач, используя кнопки *«Move Up»*, *«Move Down»* и нажать кнопку *«Next»* (Рисунок 11.5).

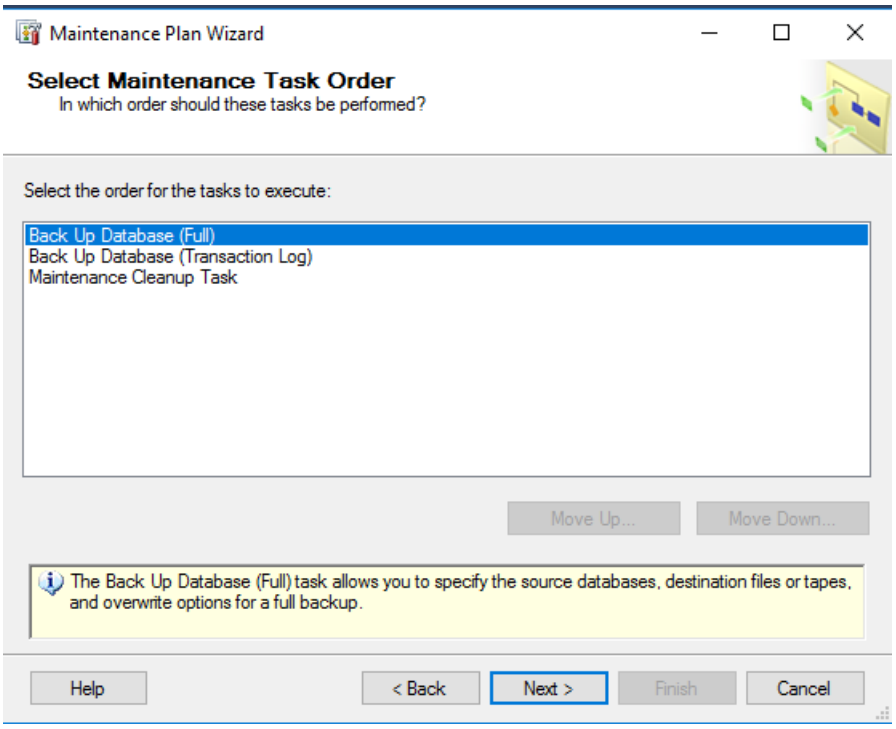

Рисунок 11.5 – Шаг «Select Maintenance Task Order»

7) На шаге «Define Backup Database (Full) Task» вкладка *«General»* в раскрывающей форме поля *«Database»* установить опцию *«These databases»*, выбрать необходимые для резервного копирования БД и нажать кнопку *«OK»* (Рисунок 11.6).

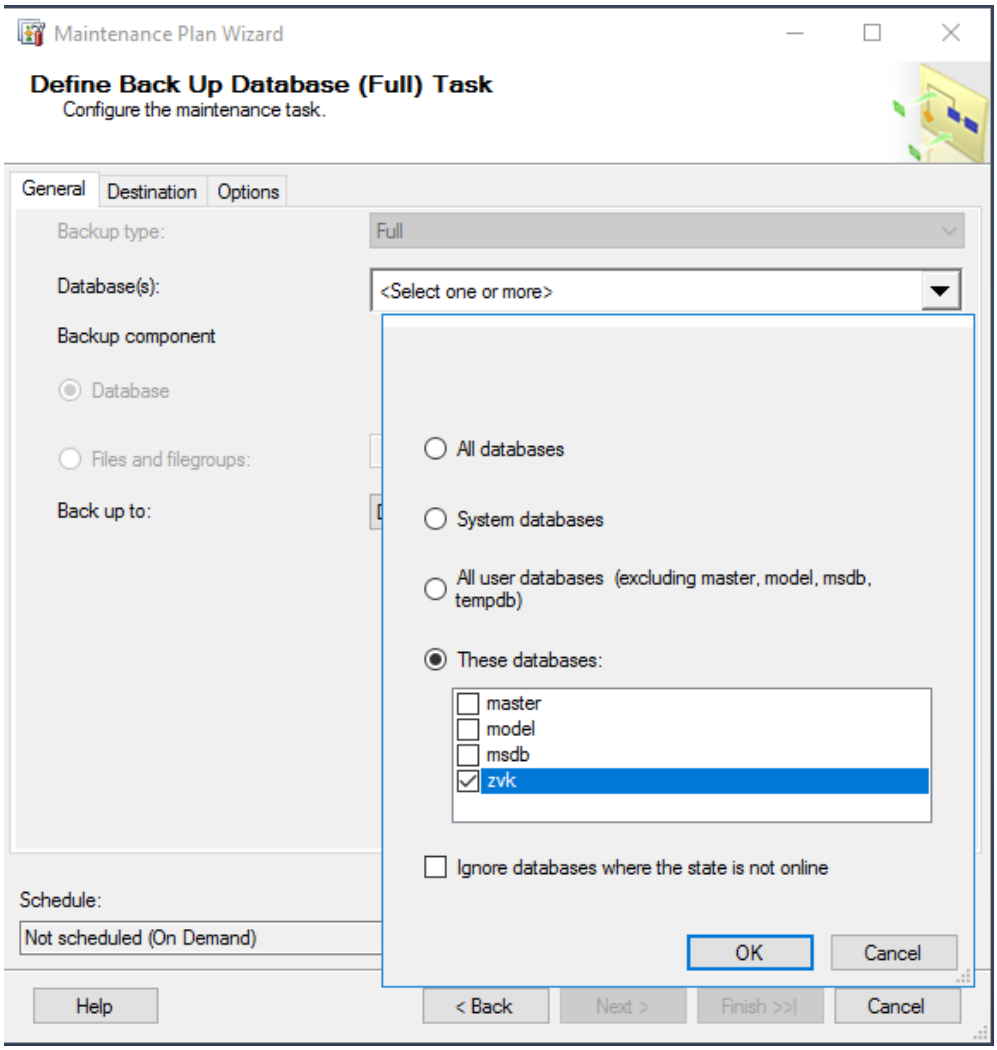

Рисунок 11.6 – Шаг «Define Backup Database (Full) Task» вкладка *«General»*

8) Задать следующие настройки (Рисунок 11.7):
   - Backup component – Database;
   - Back up to: Disk.

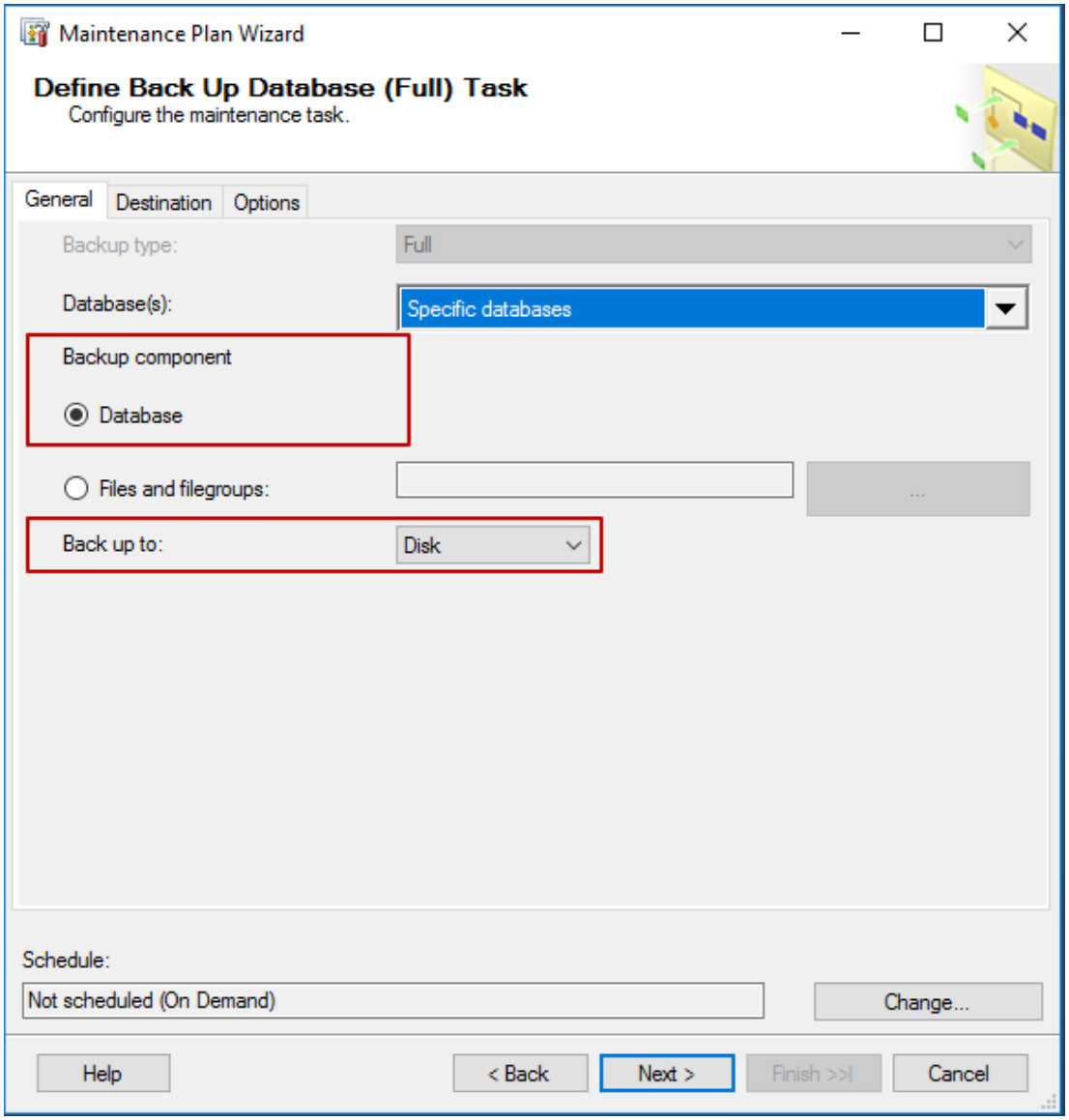

Рисунок 11.7 – Шаг «Define Backup Database (Full) Task» вкладка *«General»*

9) На вкладке *«Destination»* выбрать пункт *«Create a backup file for every database»* – при выполнении задания в выбранной директории будет создаваться несколько файлов резервных копий с именами, соответствующими названиям баз данных. Далее необходимо установить опцию *«Create a sub-directory for each database»* – расположение файлов по отдельным папкам (Рисунок 11.8).

   Обратите внимание, что необходимо оставить заполненным расширение файла резервной копии.

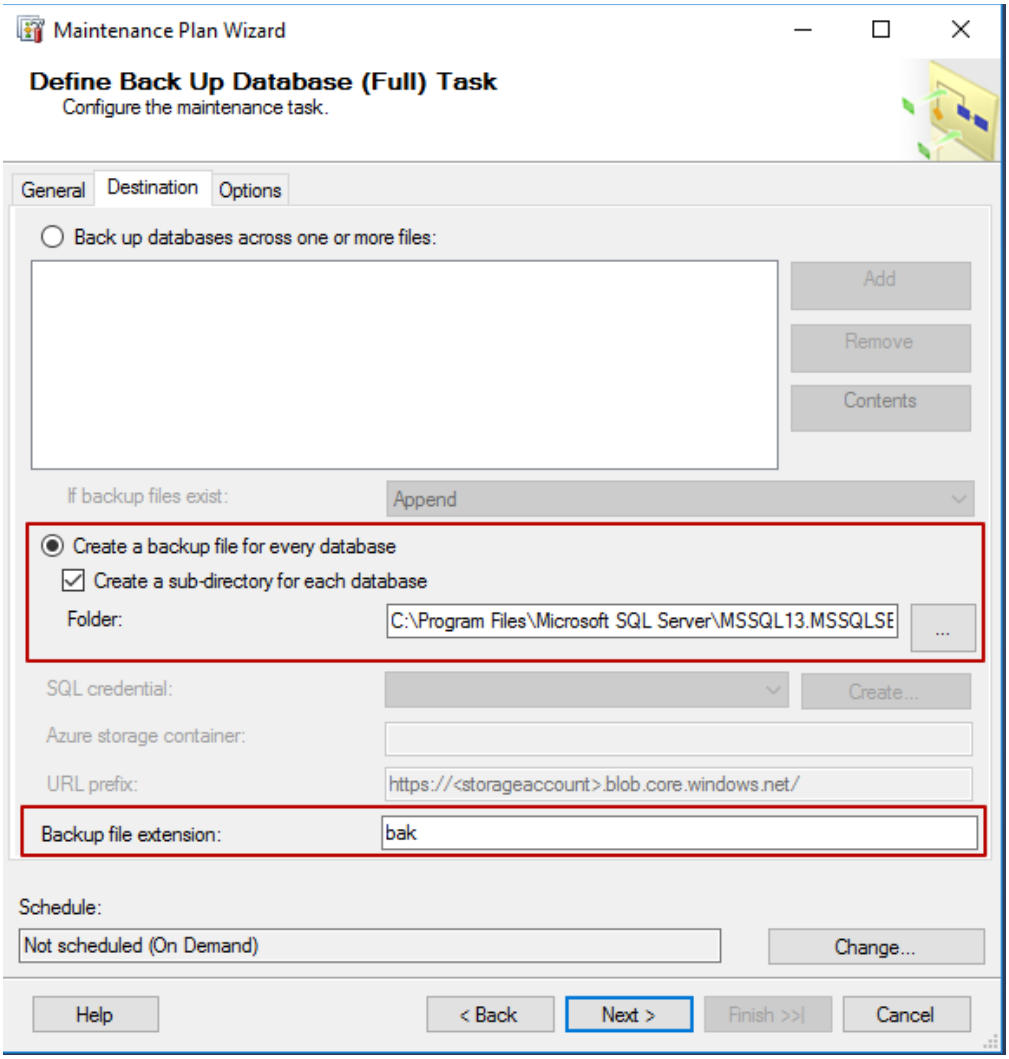

Рисунок 11.8 – Шаг «Define Backup Database (Full) Task» вкладка «Destination»

10) На вкладке «Options» из раскрывающегося списка поля *«Set backup compression»* рекомендуется выбрать пункт *«Compress backup»* для экономии дискового пространства, если используемая версия SQL Server поддерживает данную функцию. Для наибольшей надежности необходимо установить опцию *«Verify backup integrity»* (Рисунок 11.9). В случае использования групп доступности AlwaysOn на вкладке «Options» не должен быть установлен флаг в опции «For availability databases, ignore replica priority for backup and backup on primary setting».

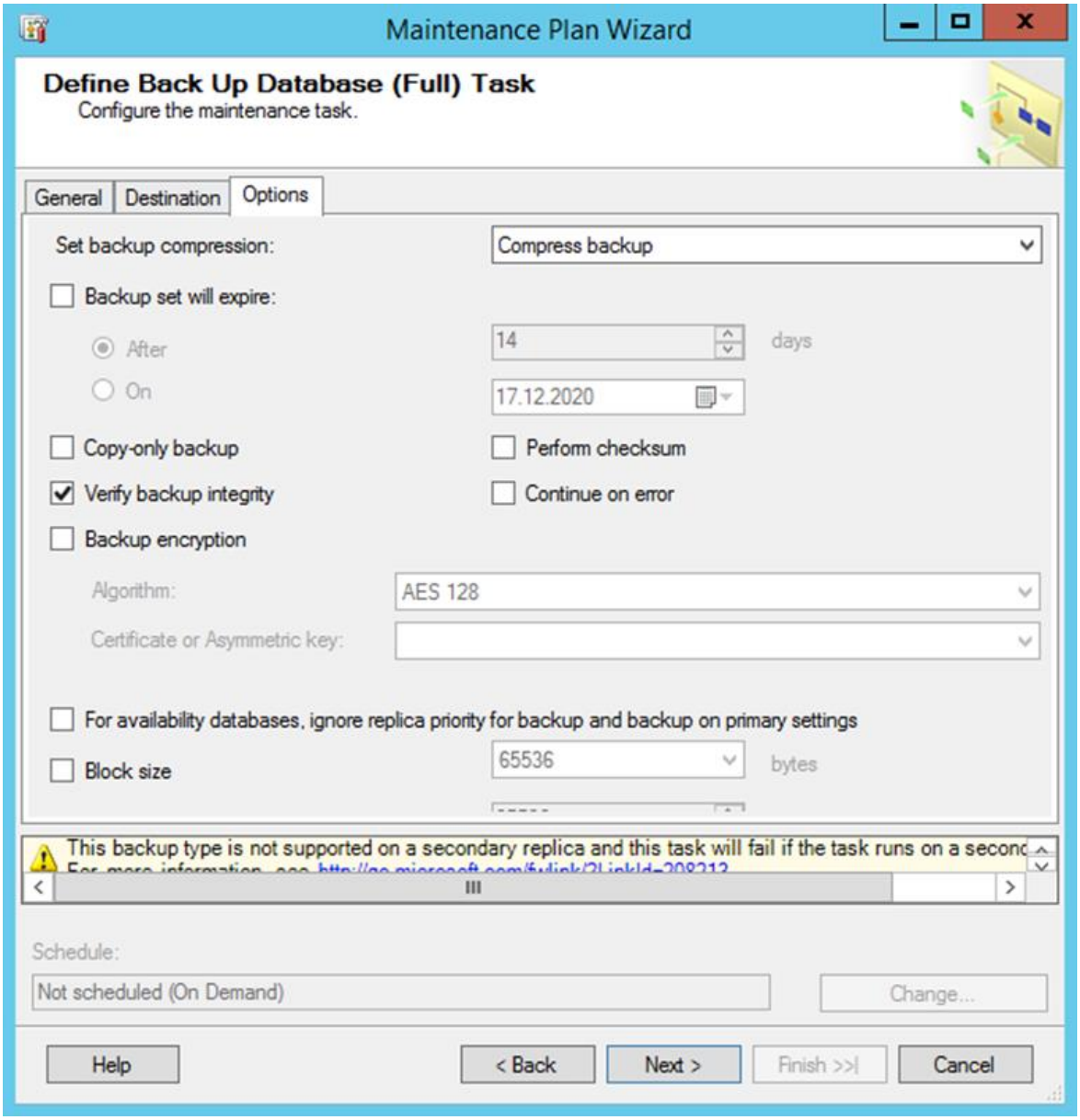

Рисунок 11.9 – Шаг «Define Backup Database (Full) Task» вкладка «Options»

11) Перейти на вкладку *«General»* в области настройки *«Schedule»* нажать кнопку *«Change»* (Рисунок 11.10).

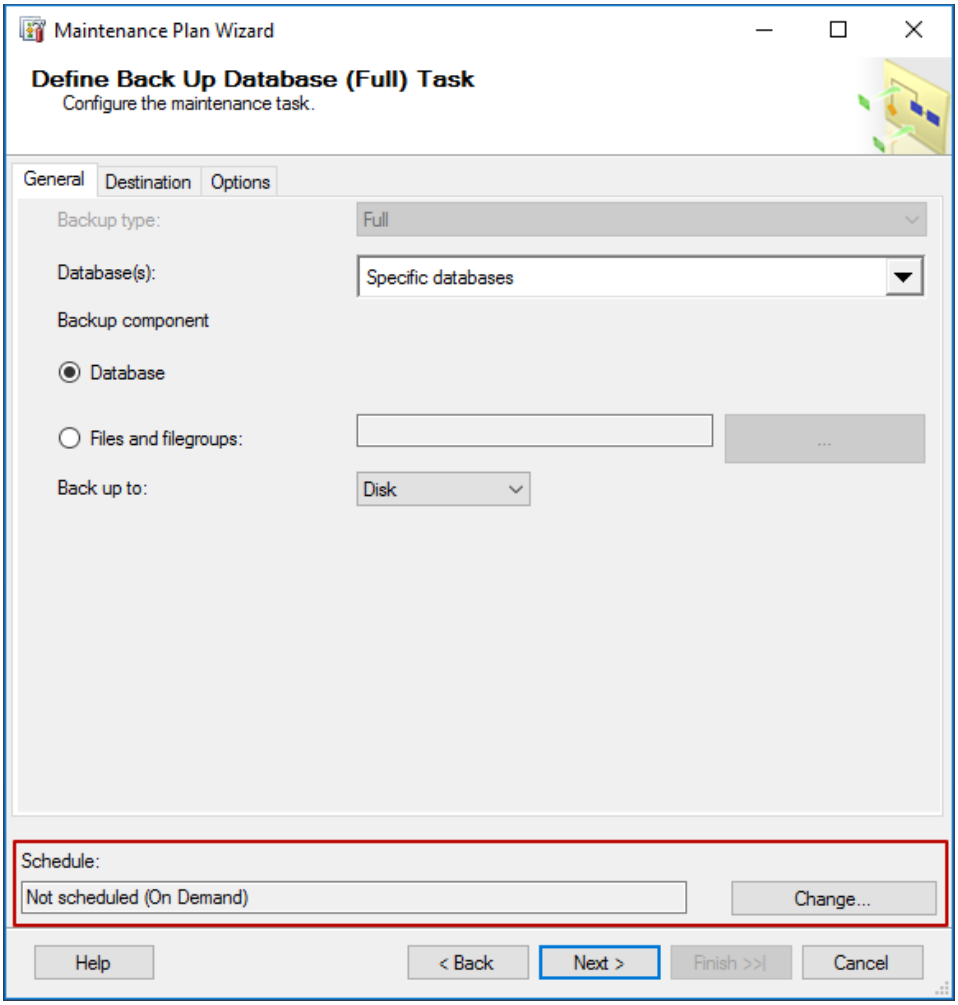

Рисунок 11.10 – Шаг «Define Backup Database (Full) Task» вкладка *«General»*

12) В диалоговом окне *«New Job Schedule»* в поле *«Name»* указать имя расписания задания и рекомендуется выполнить следующие настройки:

- из раскрывающегося списка поля *«Schedule type»* выбрать пункт *«Recuming»* и установить опцию *«Enabled»*;
- в области *«Frequency»* из раскрывающегося списка поля *«Occurs»* выбрать пункт «Daily»;
- в поле *«Recurs every»* указать значение *«1 дн.»*;
- в области *«Daily frequency»* выбрать значение *«Occurs once at»*. Для уменьшения нагрузки на сервер, выполнение задачи рекомендуется настроить в ночное время, например, 0:01:00.

После настройки расписания необходимо нажать кнопку *«OK»* (Рисунок 11.11).

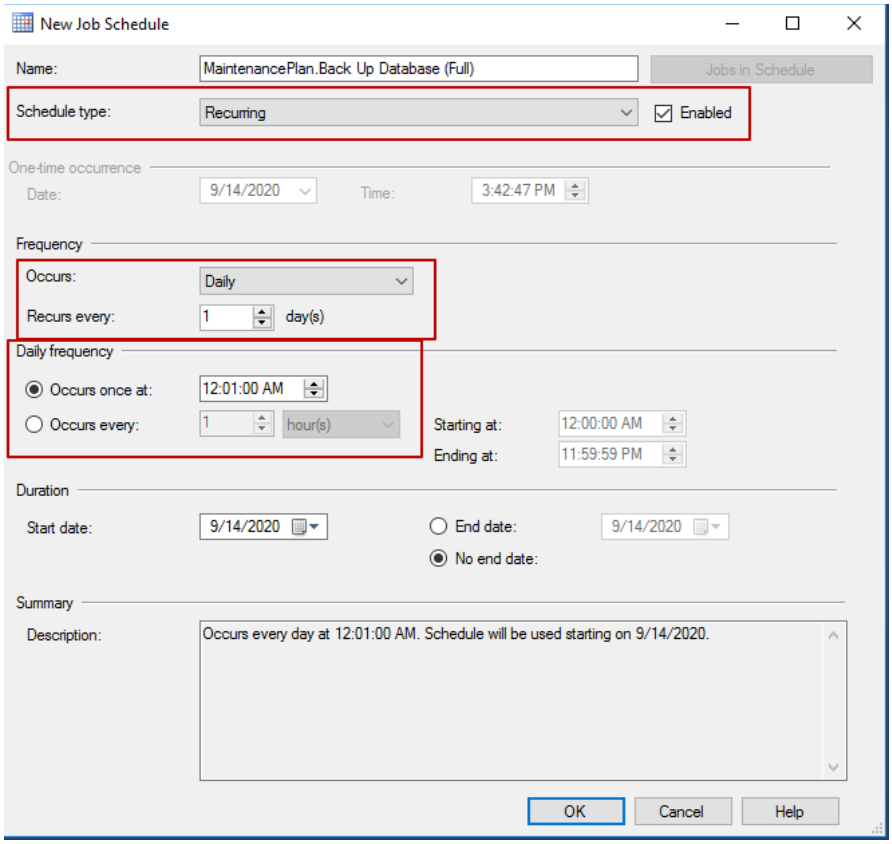

Рисунок 11.11 – Диалоговое окно «New Job Schedule»

13) На шаге *«Define Backup Database (Full) Task»* вкладка *«General»* нажать кнопку *«Next»* (Рисунок 11.12).

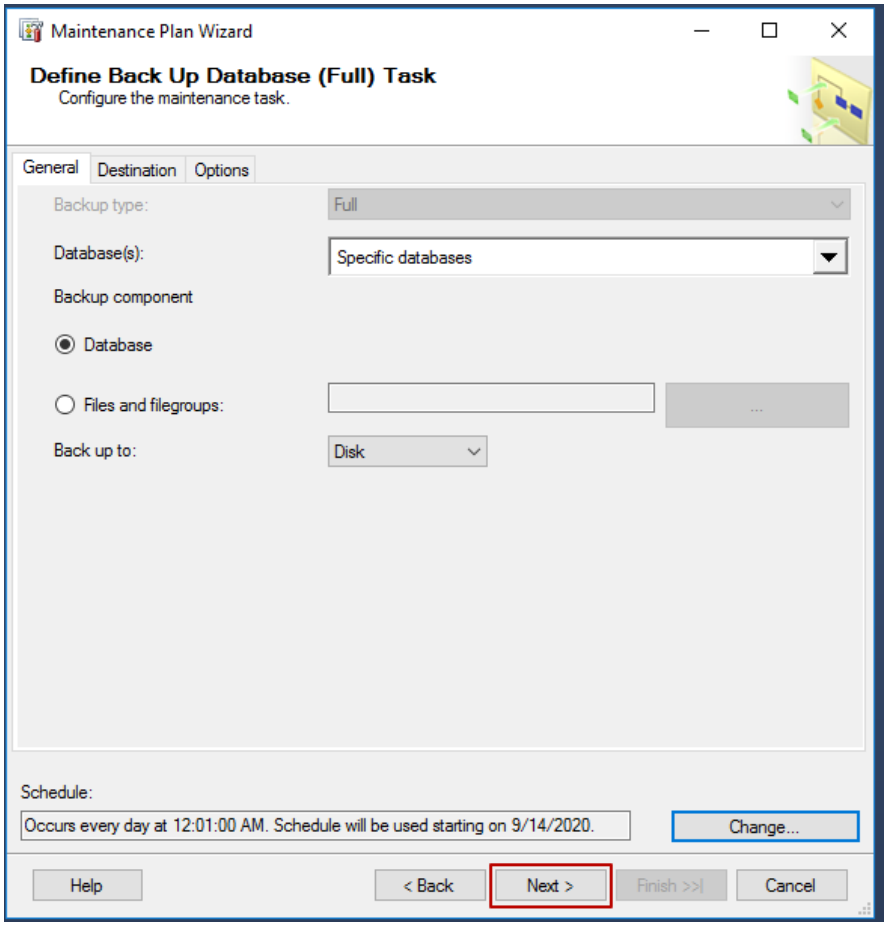

Рисунок 11.12 – Завершение настройки задачи «Define Backup Database (Full) Task»

14) Перейти к настройке задачи резервного копирования журнала транзакций. На шаге *«Define Backup Database (Transaction Log) Task»* вкладка *«General»* в раскрывающей форме поля *«Database»* установить опцию *«Specific databases»*, выбрать необходимые для резервного копирования БД и нажать кнопку *«OK»*.
15) На вкладках *Destination»* и *«Options»* задать настройки, аналогичные настройкам для задачи *«Define Backup Database (Full) Task»* (пункты 9-10 данного раздела).
16) На вкладке *«General»* в области настройки *«Schedule»* нажать кнопку *«Change»* (Рисунок 11.13).

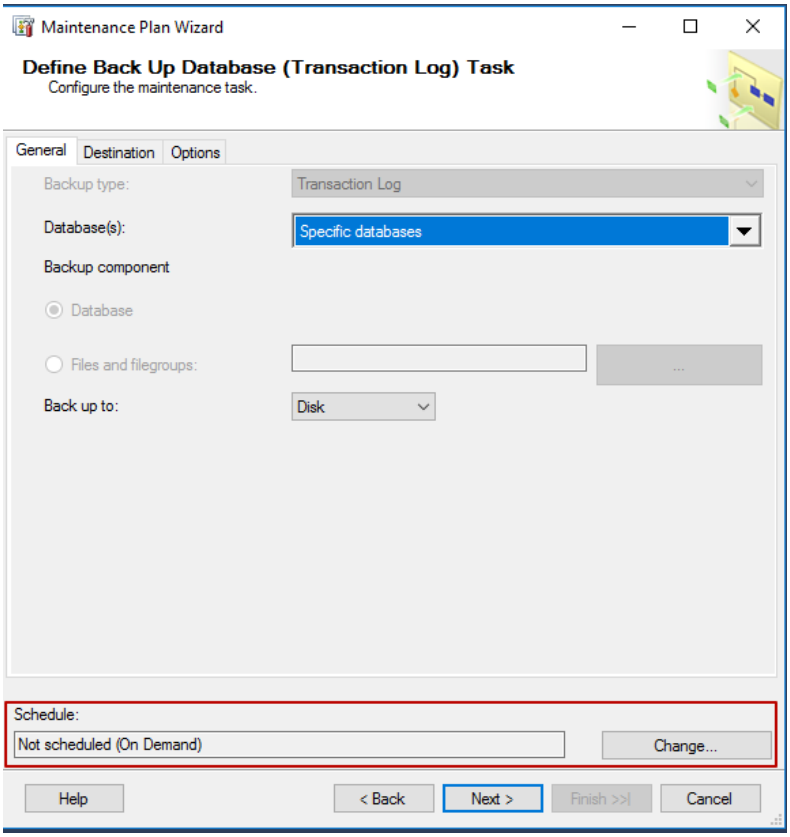

Рисунок 11.13 – Шаг «Define Backup Database (Transaction Log) Task» вкладка *«General»*

17) В диалоговом окне *«New Job Schedule»* в поле *«Name»* указать имя расписания задания и рекомендуется выполнить следующие настройки:

- из раскрывающегося списка поля *«Schedule type»* выбрать пункт *«Recuming»* и установить опцию *«Enabled»*;
- в области *«Frequency»* из раскрывающегося списка поля *«Occurs»* выбрать пункт *«Daily»*;
- в поле *«Recurs every»* для уменьшения нагрузки на сервер выполнение задачи настроить в ночное время, например, 0:01:00;
- в области *«Daily frequency»* выбрать значение *«Occurs every»*. Рекомендуемая частота – каждый час.

После настройки расписания необходимо нажать кнопку *«OK»* (Рисунок 11.4).

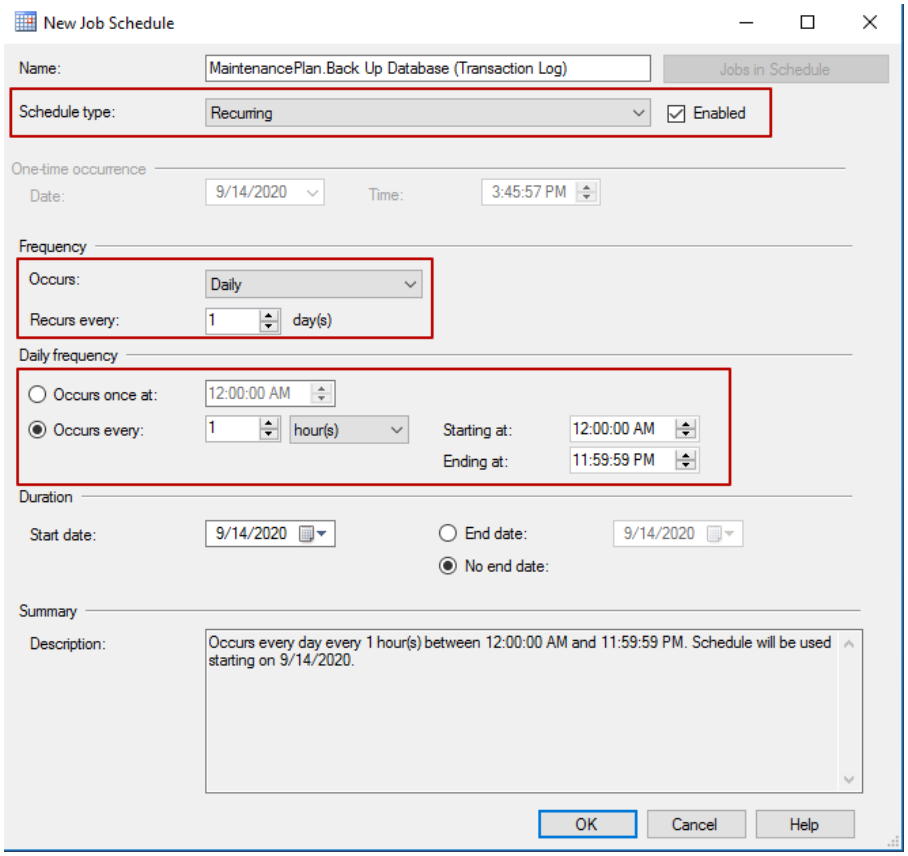

Рисунок 11.14 – Диалоговое окно «New Job Schedule»

18) На шаге *«Define Backup Database (Transaction Log) Task»* вкладка «*General*» нажать кнопку *«Next»* (Рисунок 11.15).

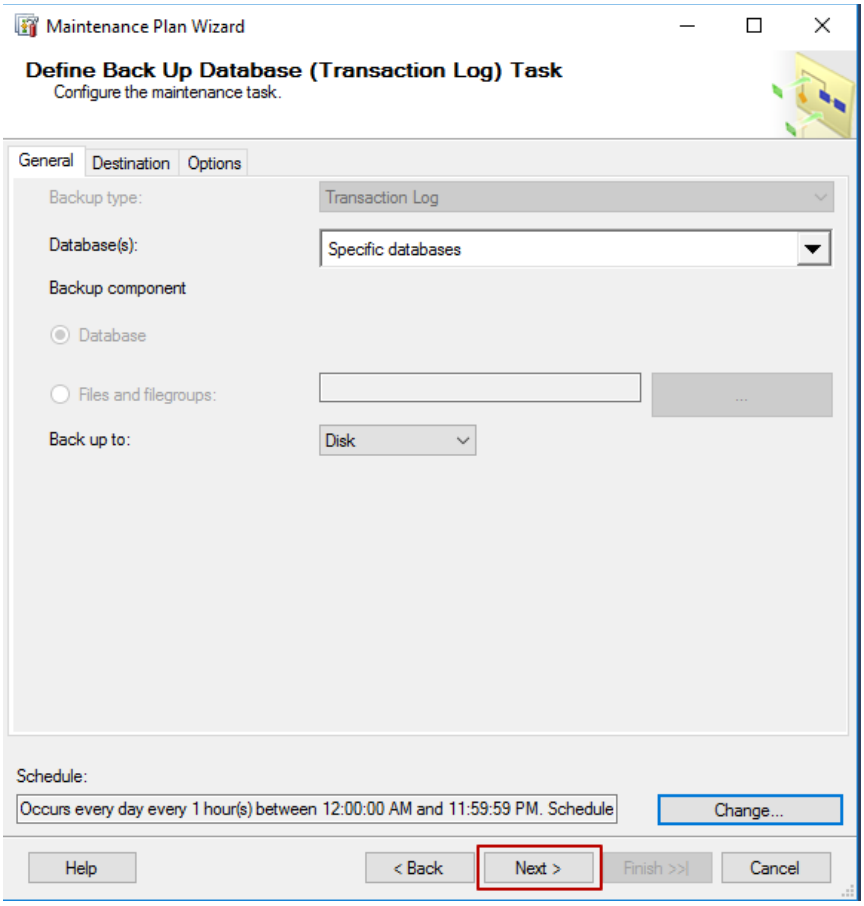

Рисунок 11.15 – Шаг «Define Backup Database (Transaction Log) Task» вкладка «General»

19) Перейти к настройке задачи очистки данных после обслуживания. На шаге *«Define Maintenance Cleanup Task»* в поле *«Folder»* раздела «*Search folder and delete files based on an extension*» указать директорию хранения резервных копий. В поле *«File extension»* указать расширение «bak». Установить флаг *«Delete files based on the age of the file at task run time»* и указать необходимое время хранения резервных копий (Рисунок 11.16).

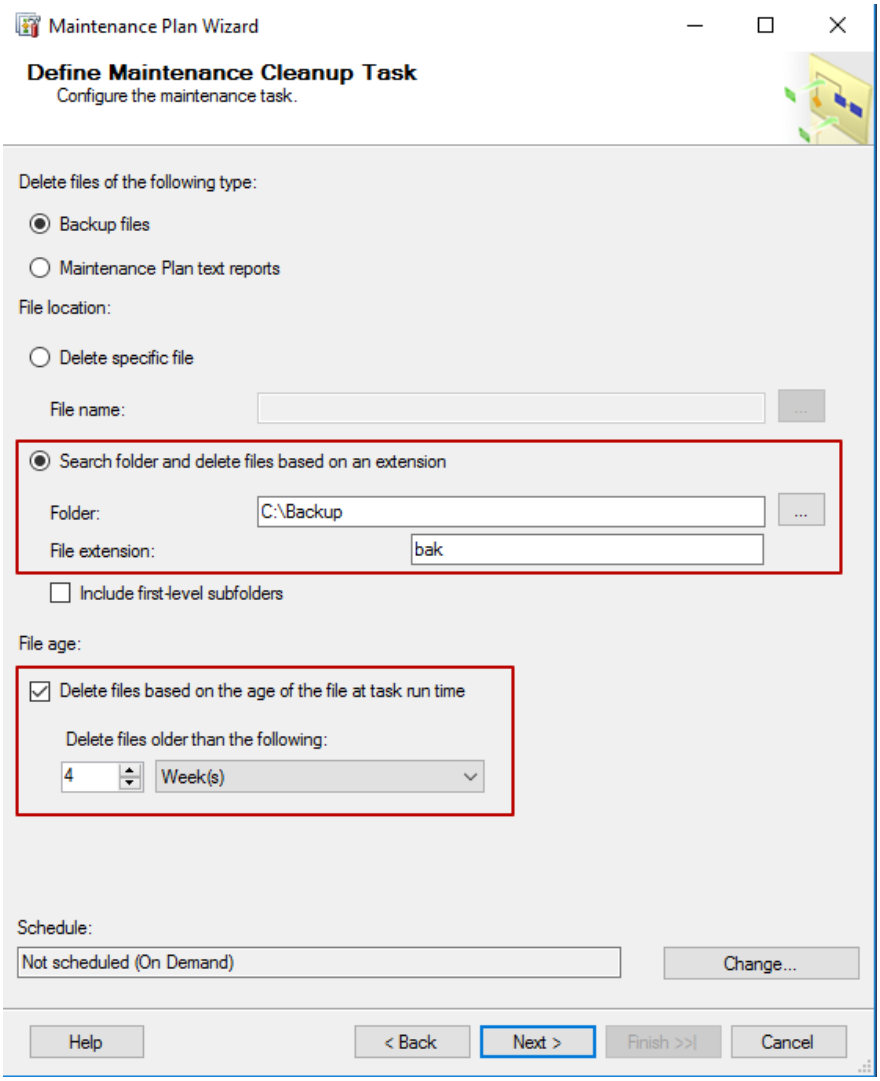

Рисунок 11.16 – Шаг *«Define Maintenance Cleanup Task»*

20) В диалоговом окне «New Job Schedule» необходимо задать расписание выполнения задачи. После настройки расписания необходимо нажать кнопку *«OK»* (Рисунок 11.17).

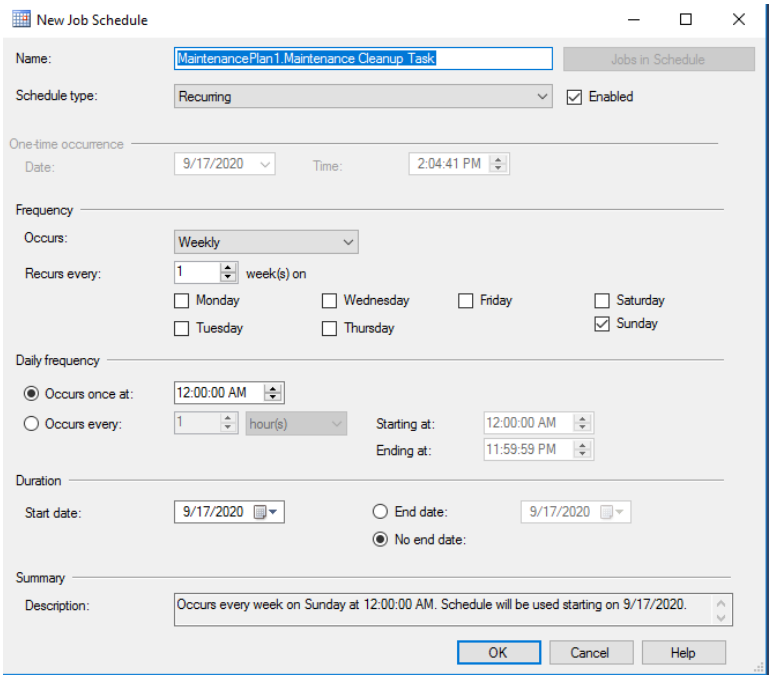

Рисунок 11.17 – Диалоговое окно «New Job Schedule»

21) На шаге *«Define Maintenance Cleanup Task»* нажать кнопку *«Next»* (Рисунок 11.18).

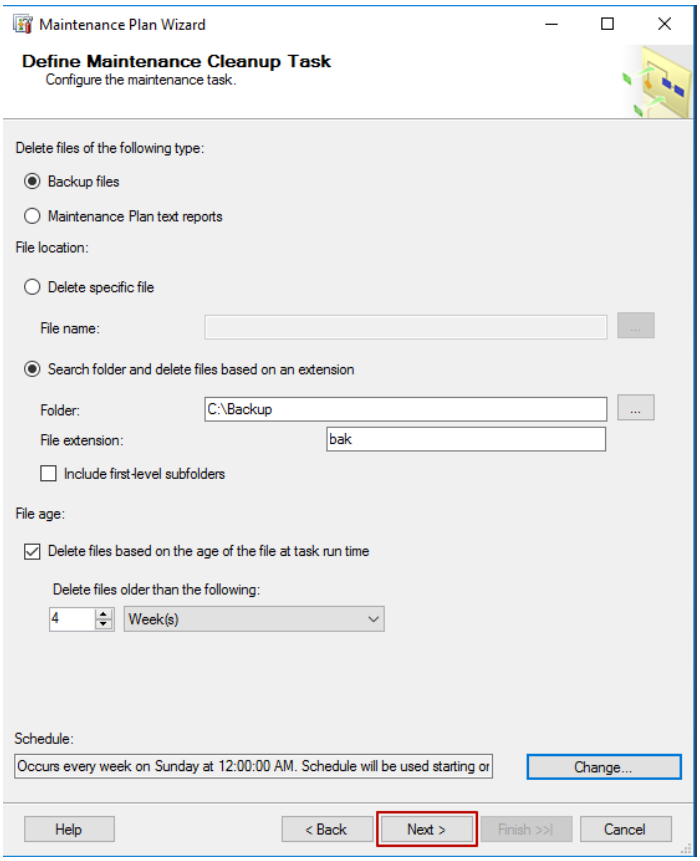

Рисунок 11.18 – Шаг «Define Maintenance Cleanup Task»

22) На шаге *«Select Report Options»* выбрать директорию, куда будет сохраняться файл журнала выполнения задания (Рисунок 11.19).

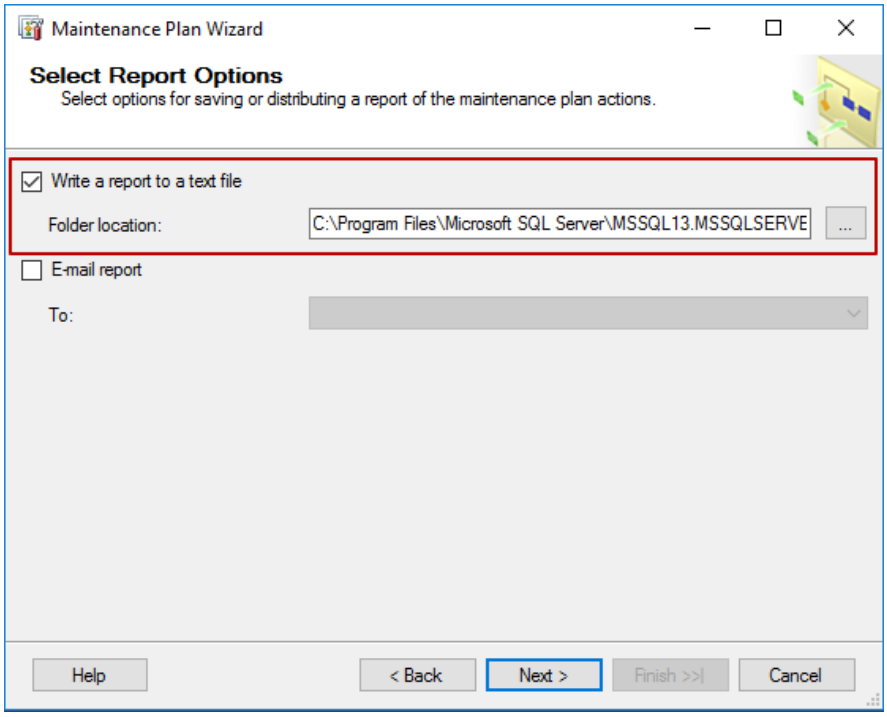

Рисунок 11.19 – Шаг «Select Report Options»

23) Проверить еще раз все настройки плана обслуживания и нажать кнопку *«Finish»* (Рисунок 11.20).

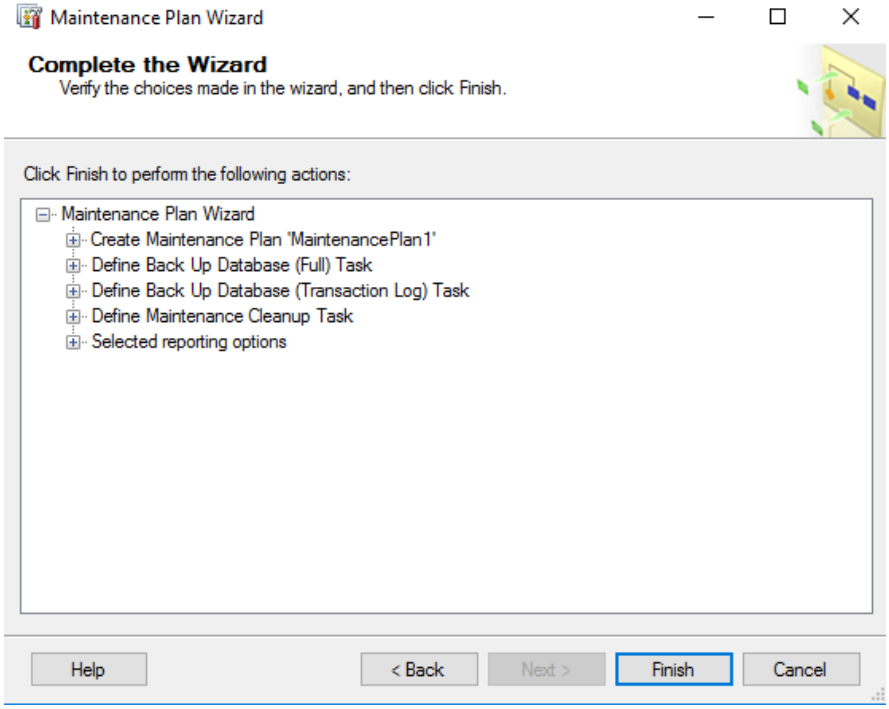

Рисунок 11.20 – Завершение работы мастера

Если мастер не обнаружит ошибок, то отобразится сообщение об успешном построении плана (Рисунок 11.21). В противном случае необходимо устранить ошибки и повторить процедуру снова.

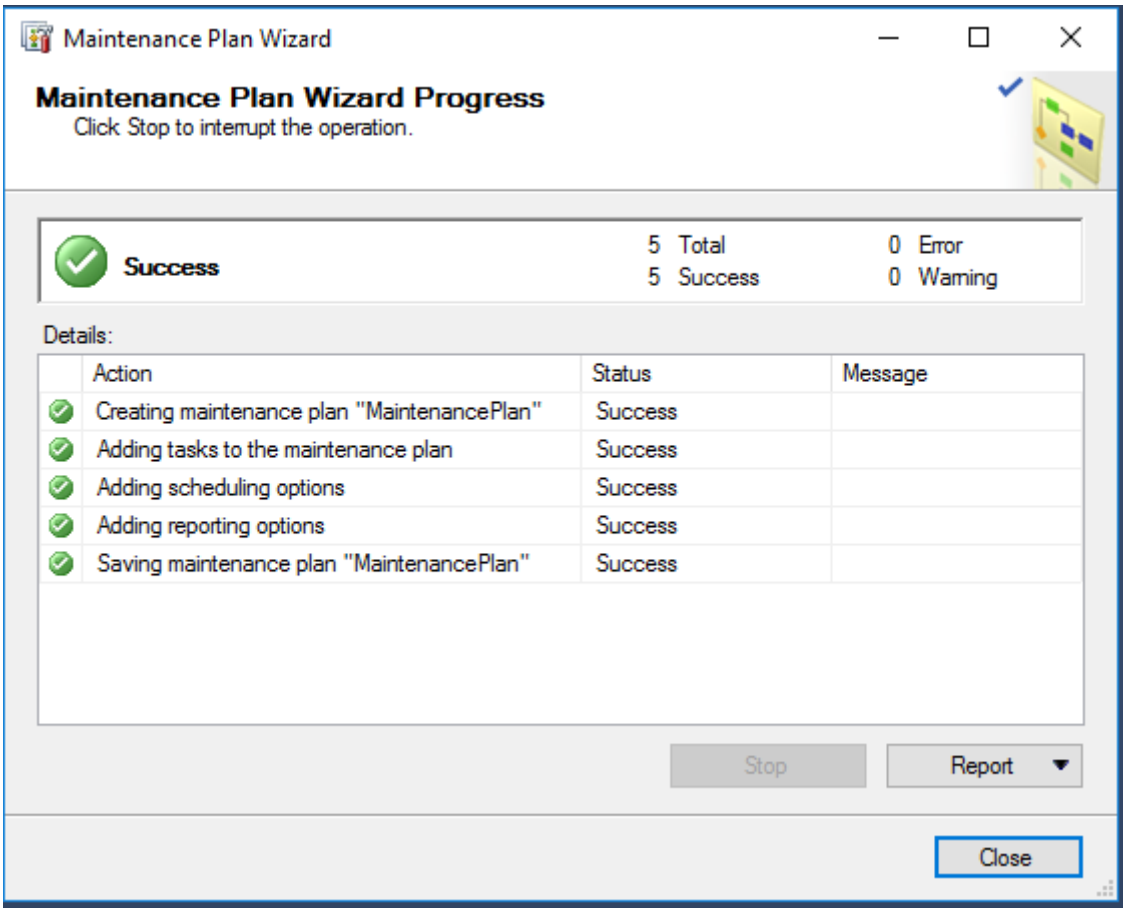

Рисунок 11.21 – Ход работы мастера планов обслуживания

24) Далее необходимо нажать кнопку «Close».

25) Чтобы проверить работу задания, необходимо перейти в программу «Microsoft SQL Server Management Studio». Раскрыть папку *«Jobs»*, в разделе *«SQL Server Agent»* будут отображаться созданные планы. Далее необходимо кликнуть правой кнопкой мыши по необходимому заданию агента SQL Server, и в контекстном меню выбрать пункт *«Start job at Step»* (Рисунок 11.22).

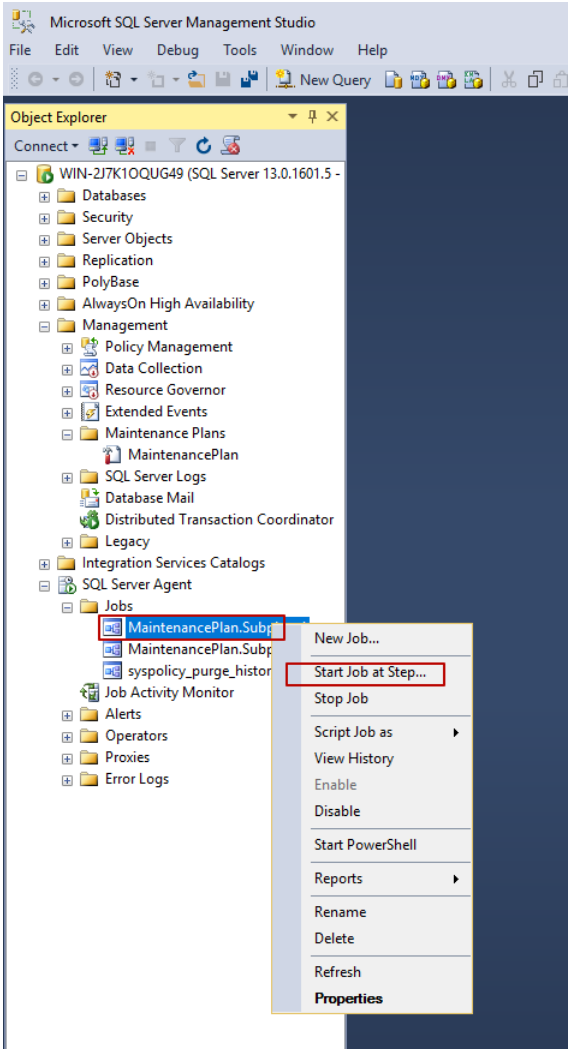

Рисунок 11.22 – Start job at Step

Запустится окно выполнения задания, в котором, должно появиться сообщение об успешном выполнении (Рисунок 11.23). Обязательно проверьте наличие файлов резервных копий в настроенном для их сохранения месте.

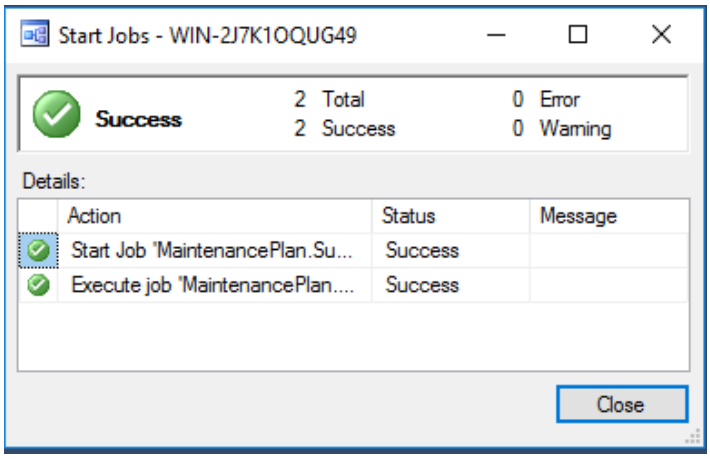

Рисунок 11.23 – Проверка запуска задания на шаге

11.5 Настройки процедуры резервного копирования

Для запуска процесса резервного копирования нужно щелкнуть правой кнопкой мыши на БД, содержащей данные текущего экземпляра ПК. В контекстном меню выбрать пункт *Tasks (Задачи)* | *Back Up*. После этого на экране появится диалоговое окно «Back Up Database» (Рисунок 11.24).

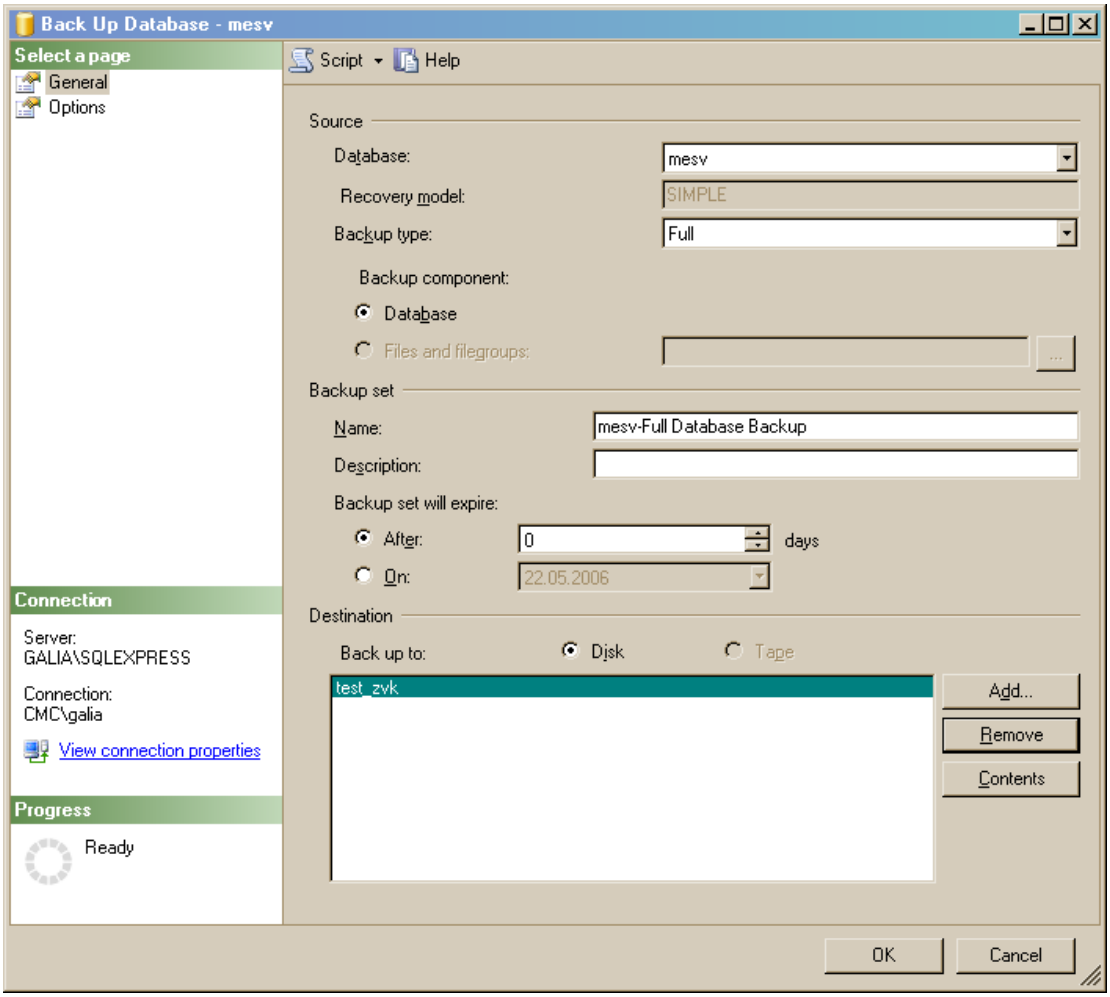

Рисунок 11.24 – Диалоговое окно «Back Up Database»

В пункте *Destination* (место назначения) указывается устройство, либо имя файла, в котором будет сохраняться резервная копия БД. Нажатие кнопки «*Add* (добавить)» дает возможность выбрать ранее созданное пользователем устройство.

11.6 Восстановление БД

В случае непредвиденных обстоятельств возможна ситуация, которая потребует восстановления БД экземпляра ПК и, в редких случаях, восстановления работы интерфейсов.

Восстановление работы ПК выполняется на СУБД MS SQL 2016 / 2019.

Восстановление данных средствами *Server Management Studio Express* происходит аналогично процессу резервирования. В дереве объектов нужно выбрать базу данных установленного экземпляра ПК (или при необходимости новую БД). Щелкнув правую кнопку мыши выбрать пункт меню *Tasks (Задачи)* | *Restore* | *Database*…(Рисунок 11.25).

В нижней части открывшегося окна можно видеть все существующие резервные копии, из которых можно проводить восстановление.

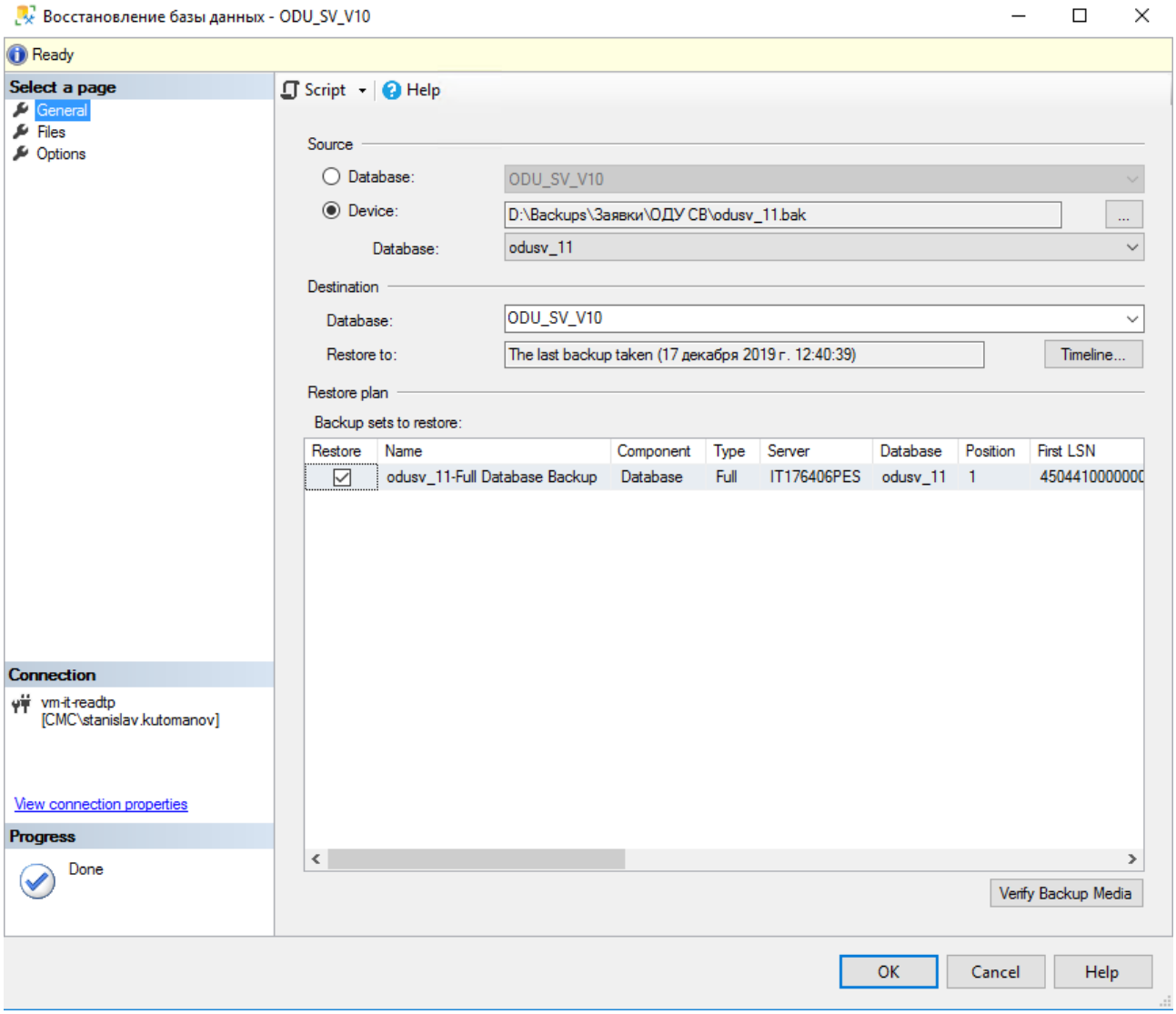

Рисунок 11.25 – Восстановление данных

11.7 Восстановление работы интерфейсов

Восстановление работы интерфейсов проводится путем удаления установленного экземпляра ПК и его инсталляции заново. Для этого необходимо выполнить следующие действия:

1) В случае установки экземпляра с восстановленной базой данных необходимо во время установки в качестве названия предприятия указать название предприятия, которое было использовано до этого.

2) Из списка баз данных выбрать базу данных предприятия, в которую производилась предыдущая установка.

3) При возникновении сообщения «The data type Ident already exists in the current database…» ответить «Да» и продолжить установку. При этом будет произведена только установка новых файлов серверной и клиентской части ПК и выполнена настройка веб-сервера. Сами данные в базе данных затронуты и потеряны не будут.

12 Резервное копирование данных ПК на СУБД PostgreSQL

12.1 Создание резервной копии базы данных средствами pg_dump

Под резервированием данных ПК понимается создание резервной копии базы данных текущего экземпляра программного комплекса на сервере базы данных.

Резервирование выполняется на СУБД PostgreSQL. Для проведения процедуры резервного копирования необходимо выполнить следующие действия:

1) Определить место хранения будущей резервной копии.

2) Создать bat-файл, который будет вызывать утилиту pg_dump.

3) Создать задание планировщика Windows, который будет запускать bat файл по расписанию.

4) Запустить задание планировщика Windows.

12.1.1 Создание bat-файла

В PostgreSQL есть утилита pg_dump, предназначенная для создания резервной копии БД. Чтобы автоматизировать процесс создания резервных копий баз PostgreSQL, необходимо создать bat-файл для вызова утилиты pg_dump.

Для создания bat-файла необходимо выполните следующие действия:

1. Запустить блокнот и указать команду:

```
@echo off
  :: Параметры
  :: хост БД
  set host=localhost
  :: порт БД
  set port=5432
  :: Пользователь - создатель бекапа
  set user=postgres
  :: Пароль пользователя
```

```
set password=sa
:: Наименование базы для бекапа
set databaseName=ASUREOTEST
:: Директория, куда будет помещен бекап (полный путь)
set outputDirectoryPath="D:\PostgresqlBack"
:: Директория, установленного экземпляра PostgreSQL
set scriptDirectoryFullPath="C:\Program Files\PostgreSQL\12"
set backupFileName=%databaseName%_%date%.backup
echo backup file name is %backupFileName%
SET PGPASSWORD=%password%

echo on

%scriptDirectoryFullPath%\bin\pg_dump -h %host% -p %port% -U %user% -E "UTF8" -F c -b -v -f %outputDirectoryPath%\%backupFileName% %databaseName%
```

Пример команды, в которой создается резервная копия базы данных ASUREO СУБД PostgreSQL на Localhost представлен на рисунке 12.1.

postgresqlBackup.bat — Блокнот

Файл Правка Формат Вид Справка

```
@echo off

:: Параметры
:: хост БД
set host=localhost
:: порт БД
set port=5432
:: Пользователь - создатель бекапа
set user=postgres
:: Пароль пользователя
set password=sa
:: Наименование базы для бекапа
set databaseName=ASUREOTEST
:: Директория, куда будет помещен бекап (полный путь)
set outputDirectoryPath=D:\PostgresqlBack
:: Директория, со скриптом (полный путь)
set scriptDirectoryFullPath=C:\Program Files\PostgreSQL\11

set backupFileName=%databaseName%_%date%.backup
echo backup file name is %backupFileName%
SET PGPASSWORD=%password%

echo on

%scriptDirectoryFullPath%\bin\pg_dump -h %host% -p %port% -U %user% -E "UTF8" -F c -b -v -f %outputDirectoryPath%\
%backupFileName% %databaseName%
```

Рисунок 12.1 – Пример команды

2. Сохранить файл с расширением .bat (например, postgresqlBackup.bat).

12.1.2 Создание задания планировщика Windows

Для создания задания планировщика Windows необходимо выполнить следующие действия:

1. Открыть планировщик заданий Windows: *«Пуск-Панель управления-Администрирование-Планировщик заданий»* (Рисунок 12.2).

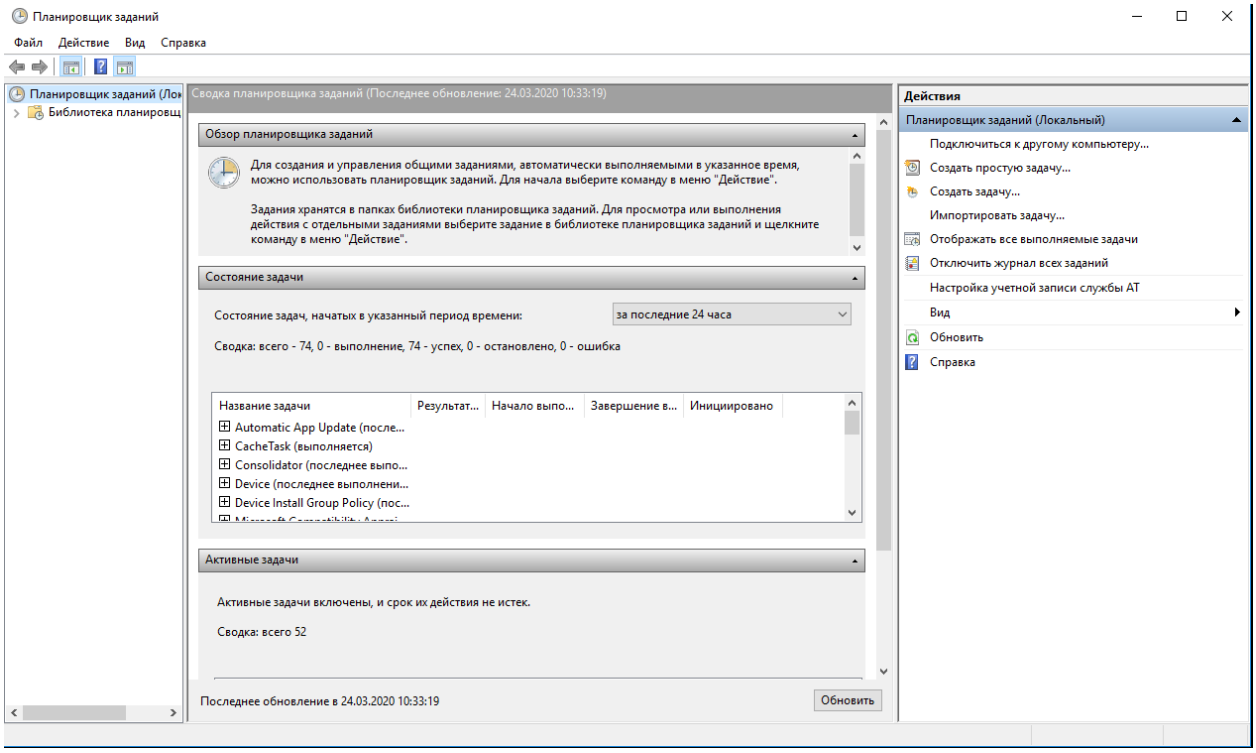

Рисунок 12.2 – Планировщик заданий

2. В Планировщике заданий (Task Scheduler) из раскрывающегося списка пункта меню *«Действие»* (Action) выбрать пункт *«Создать задачу»* (Create Task) (Рисунок 12.3).

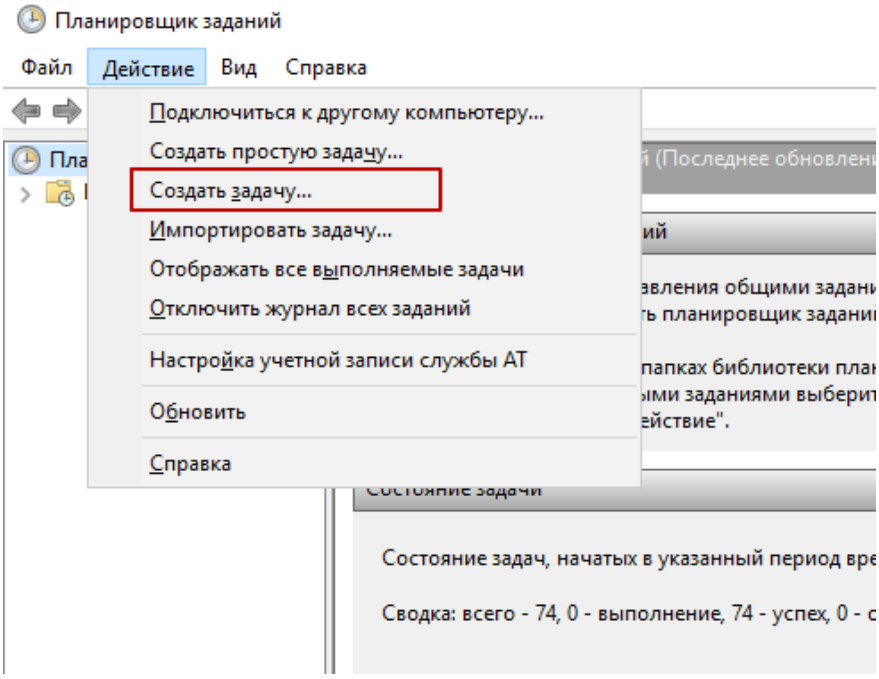

Рисунок 12.3 – Выбор пункта «Создать задачу»

3. В открывшейся форме *«Создание задачи»* (Create Task) на вкладке *«Общее»* (Genral) указать *«Имя задачи»* (Name), например, Создание бэкапов PostgreSQL (Рисунок 12.4).

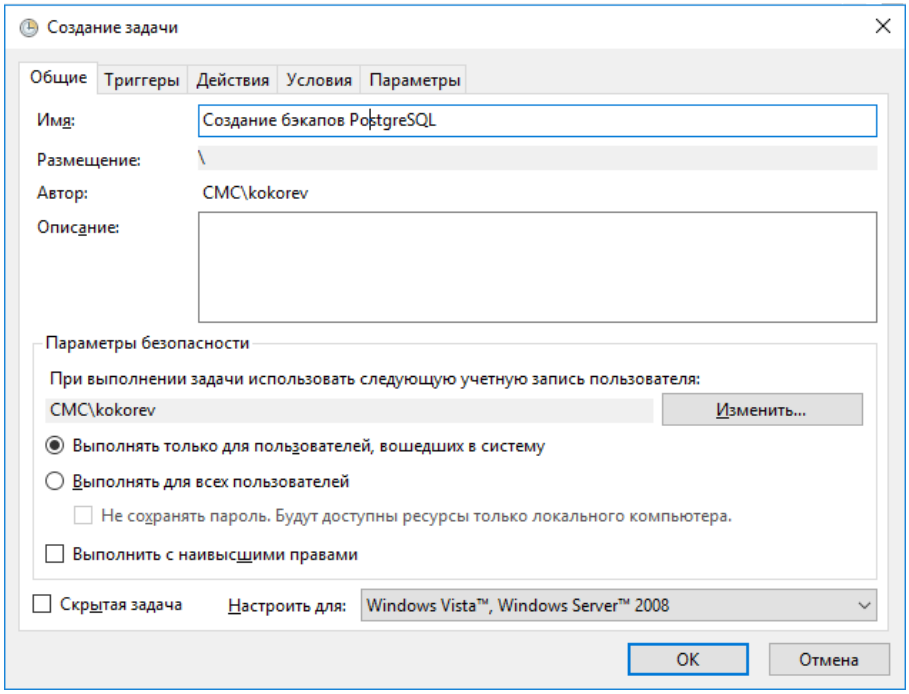

Рисунок 12.4 – Ввод имени задачи

4. Далее необходимо перейти на вкладку *«Триггеры»* (Triggers) и нажать кнопку *«Создать»* (New) (Рисунок 12.5).

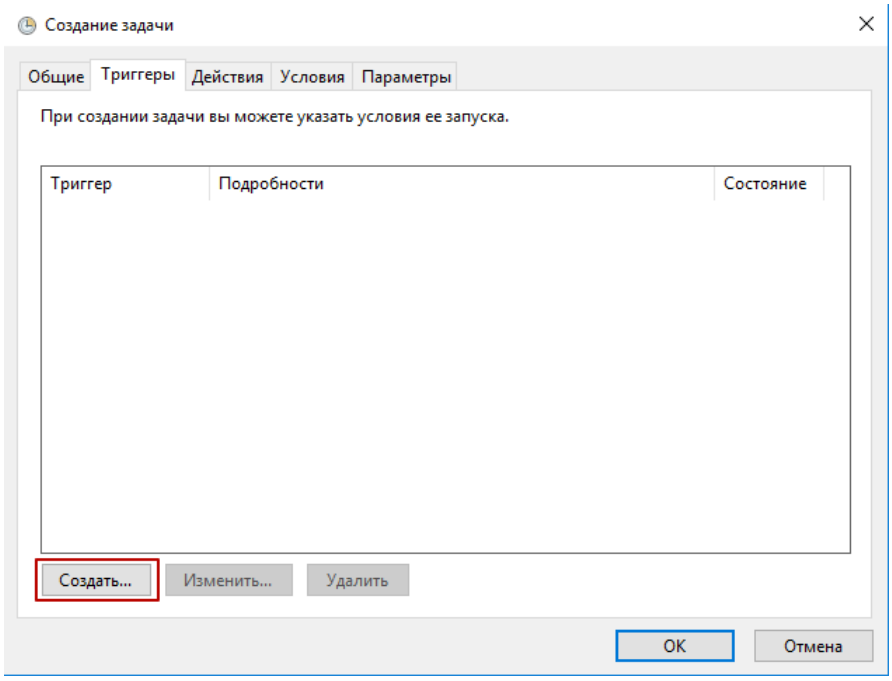

Рисунок 12.5 – Создание триггера

5. В открывшейся форме *«Создание триггера»* (New Trigger) настроить расписание запуска задания (в данном случае задание будет запускаться каждый день в 01-00) (Рисунок 12.6).

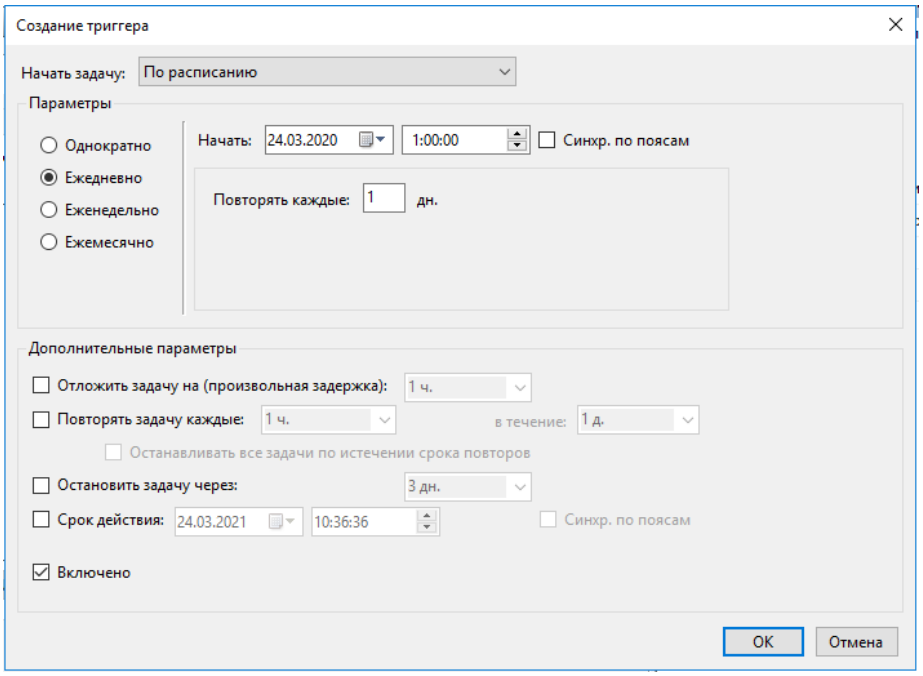

Рисунок 12.6 – Настройка расписания запуска задания

6. На вкладке *«Действия»* (Actions) необходимо указать действие нашего задания, для этого необходимо нажать кнопку «Создать» (New) (Рисунок 12.7).

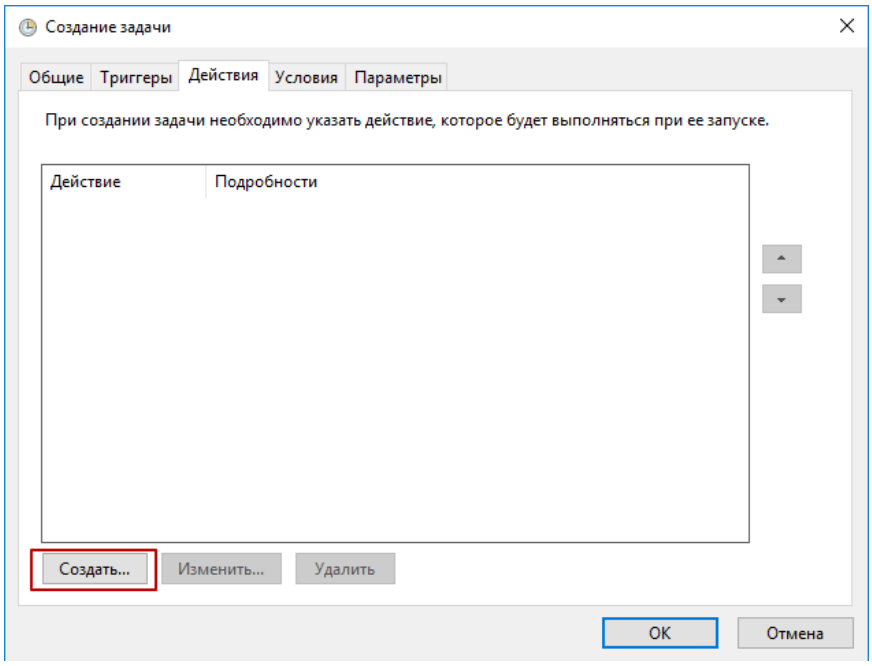

Рисунок 12.7 – Создание действия

7. В открывшейся форме *«Создание действия»* (New Action) указать действие – запуск файла *«postgresqlBackup.bat»* с локального диска D (Рисунок 12.8).

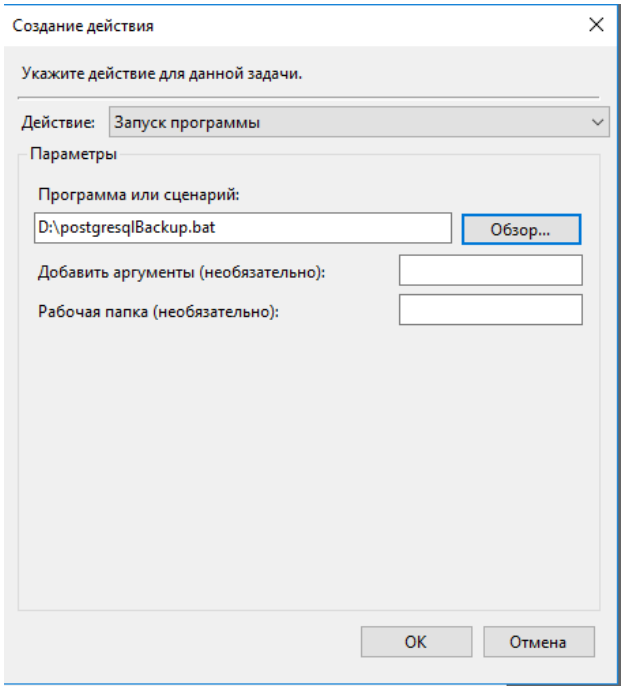

Рисунок 12.8 – Указание действия

8. На форме «Создание задачи» (Great Task) нажать кнопку «ОК» (Рисунок 12.9), в результате чего будут созданы: .bat файл с командой создания резервной копии БД АСУРЭО на СУБД PostgreSQL и задания планировщика Windows на запуск этого .bat файла.

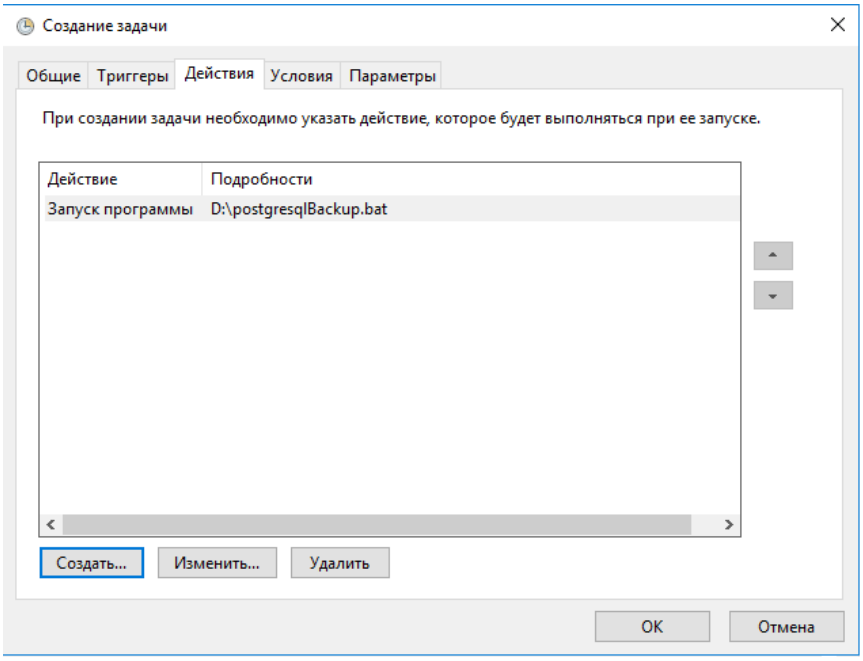

Рисунок 12.9 – Завершение создания

12.2 Создание резервной копии базы данных в инструментарии PGAdmin

Для создания резервной копии базы данных экземпляра ПК «АСУРЭО» в инструментарии PGAdmin необходимо выполнить следующие действия:

1. Правым кликом мыши вызвать контекстное меню БД, содержащей данные текущего экземпляра ПК. В контекстном меню выбрать пункт «Резервная копия» (Tasks) (Рисунок 12.10).

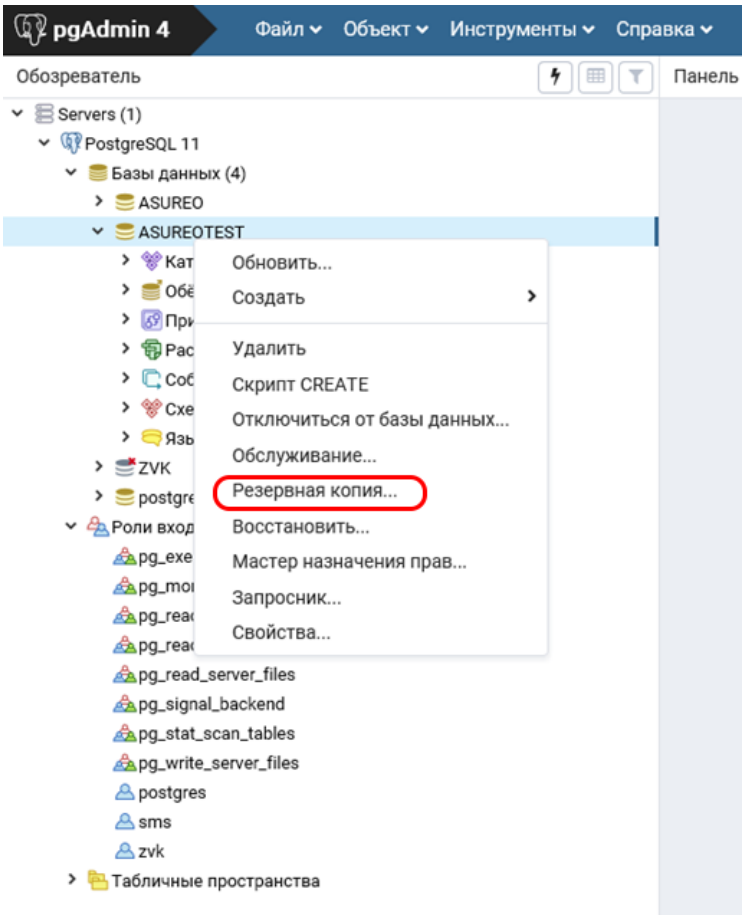

Рисунок 12.10 – Выбор пункта «Резервная копия»

2. В появившемся диалоговом окне необходимо указать путь и имя файла резервной копии, а также указать формат «Tar» (Рисунок 12.11).

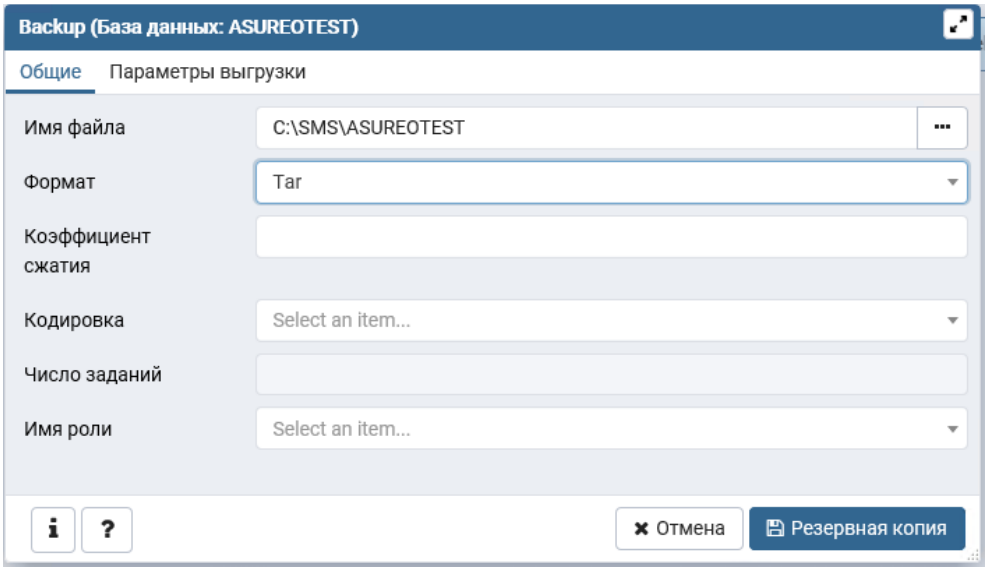

Рисунок 12.11 – Диалоговое окно «Backup (База данных: ASUREOTEST)»

3. Нажать кнопку «Резервная копия» и дождаться завершения процесса создания копии базы данных (Рисунок 12.12).

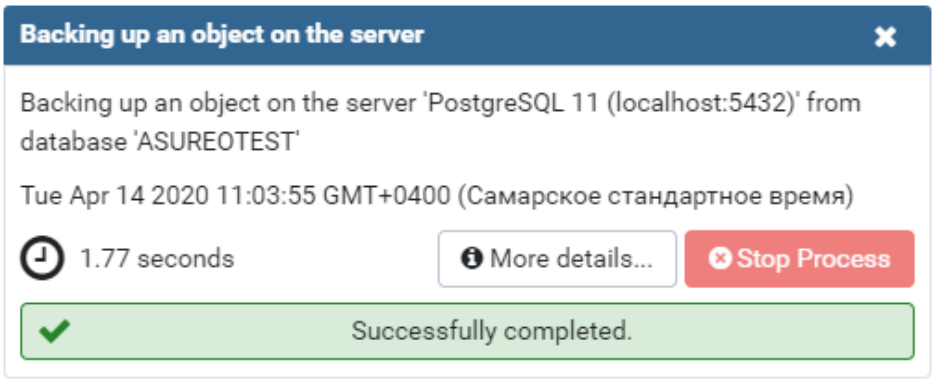

Рисунок 12.12 – Завершение процесса создания копии базы данных

12.3 Восстановление БД из резервной копии средствами pg_restore

Для восстановления базы данных из резервной копии экземпляра ПК «АСУРЭО» можно использовать утилиту pg_restore.exe.

Перед восстановлением необходимо создать базу данных.

Для выполнения команды восстановления базы данных необходимо выполнить следующие действия:

1. Запустить командную строку – на клавиатуре нажать клавиши «Win+R», в открывшемся окне «Выполнить» ввести команду «cmd» и нажать кнопку [OK].

2. В командной строке ввести и выполнить команду (Рисунок 12.13):

pg_restore -C --clean -d postgres -U postgres -W – "D:\Backup\test.sql"

где:

– «-C» – указание создать базу данных, прежде чем восстанавливать данные;

– «--clean» – указание удалить и пересоздать целевую базу данных перед подключением к ней;

– «-d» – указание системной базы PostgreSQL, от имени которой будет происходить создание новой базы данных;

– «-U» – указание пользователя PostgreSQL;

– «-W» – указание принудительно запрашивать пароль перед подключением к базе данных;

– "D:\Backup\test.sql" – указать путь хранения резервной копии.

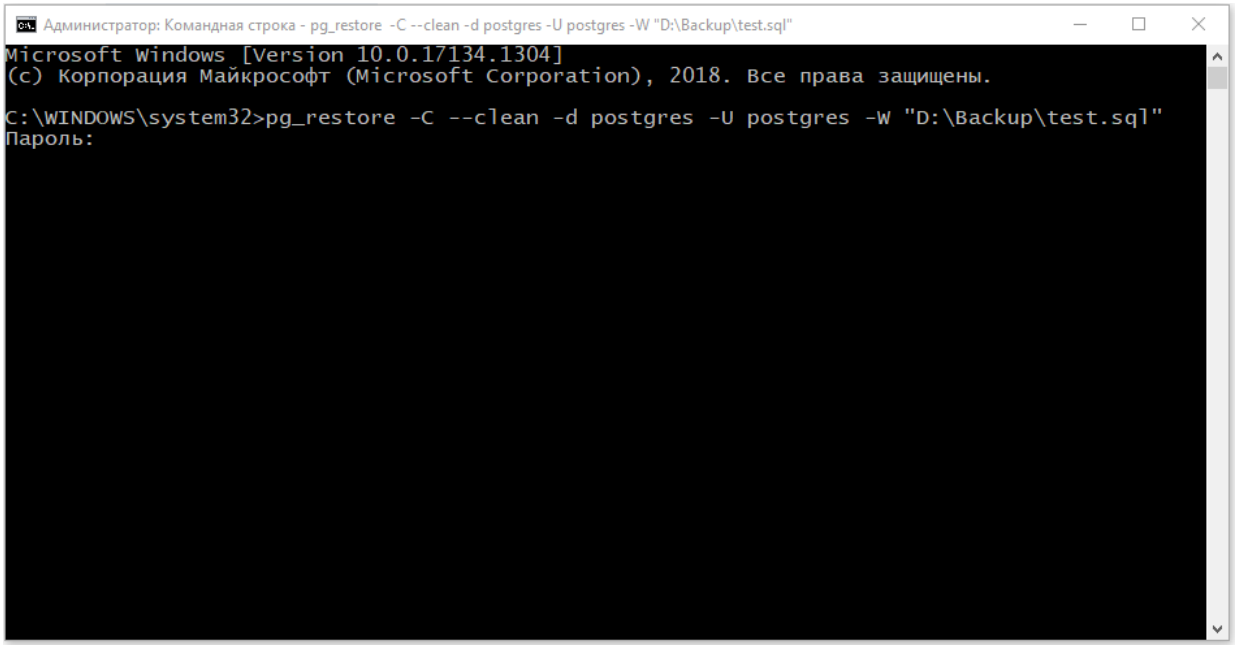

Рисунок 12.13 – Пример команды

12.4 Восстановление БД из резервной копии в инструментарии PGAdmin

Для восстановления базы данных из резервной копии экземпляра ПК «АСУРЭО» в инструментарии PGAdmin необходимо выполнить следующие действия:

1. Правым кликом мыши вызвать контекстное меню БД и в контекстном меню выбрать пункт «Восстановить» (Рисунок 12.14Рисунок 12.4).

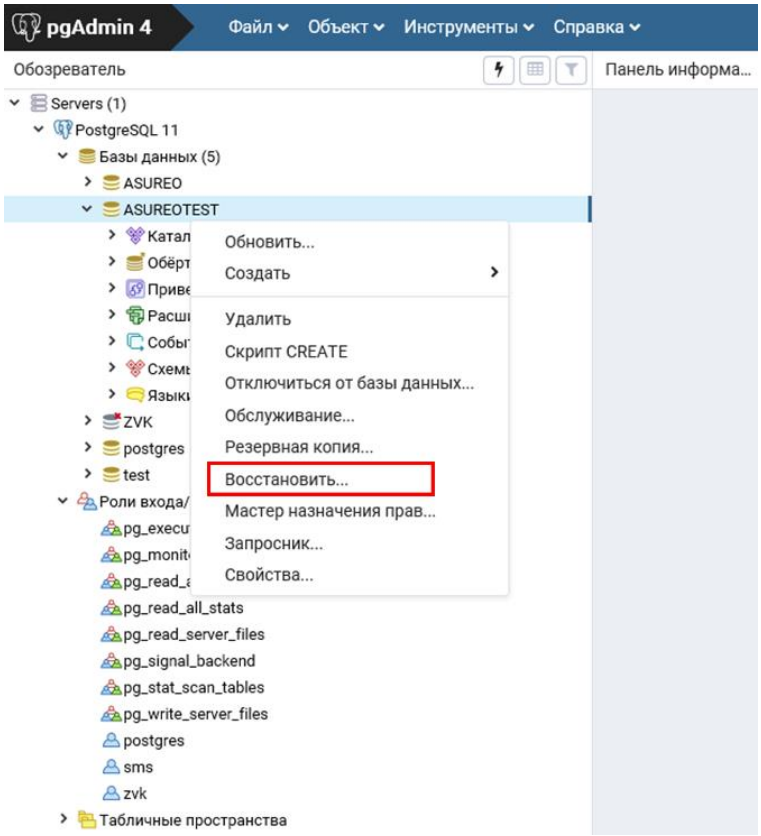

Рисунок 12.14 – Выбор пункта «Восстановить»

2. В появившемся диалоговом окне необходимо указать формат «Специальный или tar», а также путь и имя файла резервной копии (Рисунок 12.15).

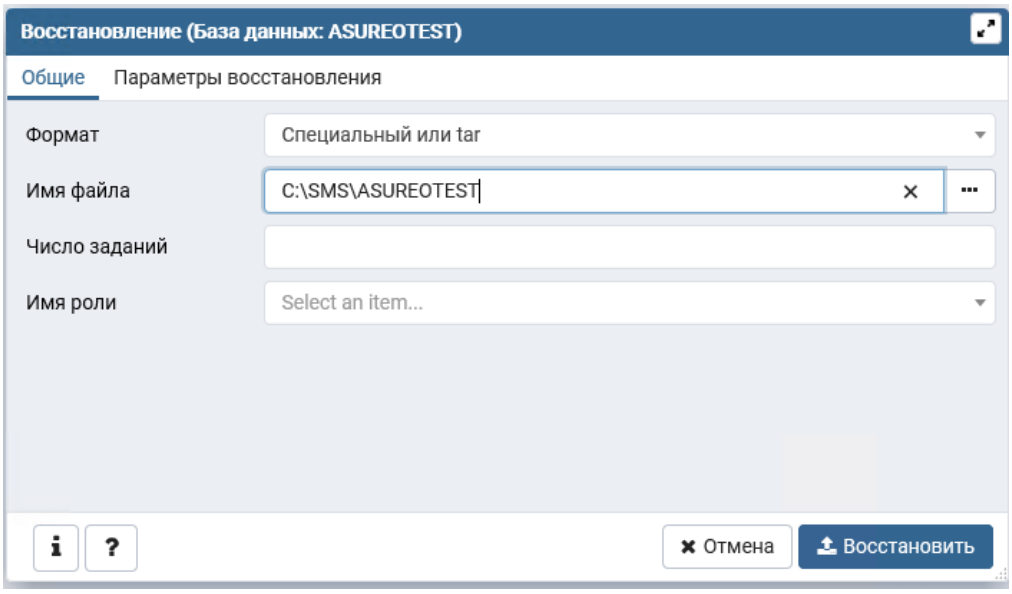

Рисунок 12.15 – Диалоговое окно «Восстановление (База данных: ASUREOTEST)»

3. Нажать кнопку «Восстановить» и дождаться завершения процесса восстановления базы данных (Рисунок 12.16).

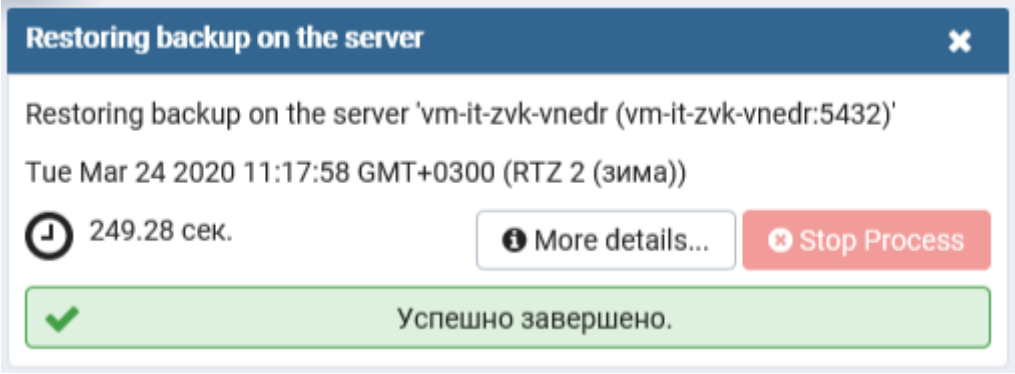

Рисунок 12.16 – Завершение процесса восстановления базы данных

13 Настройка карты многоэкземплярной конфигурации

13.1 Использование карты

Если пользователь работает с несколькими экземплярами приложения ПК, то для быстрого запуска требуемого экземпляра можно использовать карту многоэкземплярной конфигурации (Рисунок 13.1).

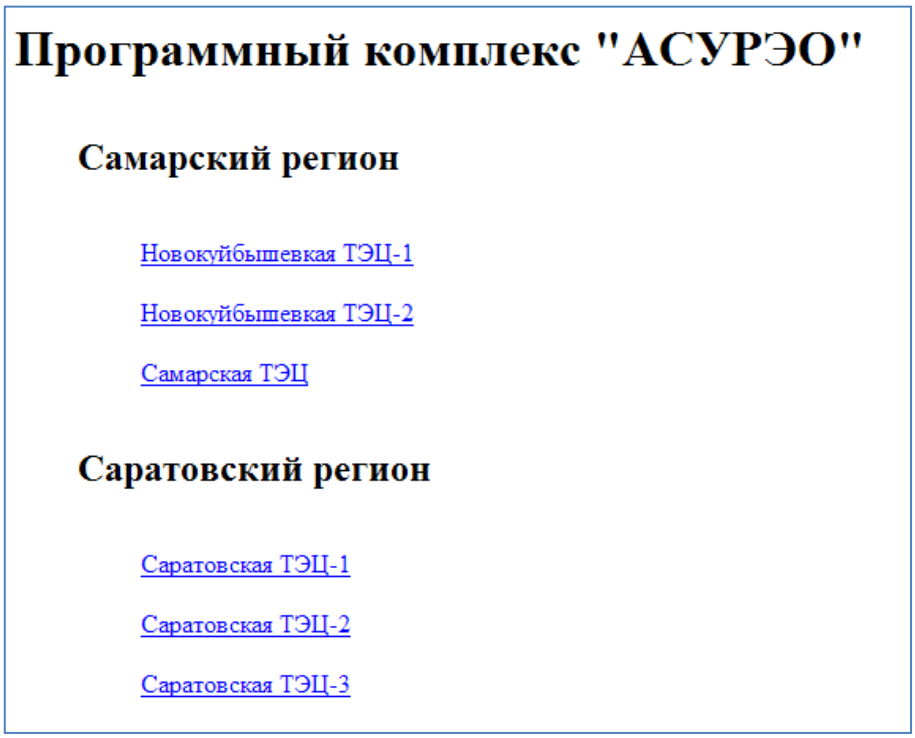

Рисунок 13.1 – Пример карты многоэкземплярной конфигурации

Карта многоэкземплярной конфигурации представляет собой HTML-страницу с набором ссылок на экземпляры приложения. По нажатию на ссылку появляется окно выбора интерфейсов приложения выбранного экземпляра ПК.

13.2 Создание карты

Пользователи, знающие язык разметки гипертекстов (html), могут создать карту многоэкземплярной конфигурации с помощью любого редактора HTML (Рисунок 13.2).

```
1  <H1>Программный комплекс "АСУРЭО"</H1>
2  <br>
3  <dd><H2>Самарский регион</H2>
4  <br>
5  <dd><dd><a href="http://server1/NovTEC-1/">Новокуйбышевкая ТЭЦ-1 </a><br> <br>
6  <dd><dd><a href="http://server1/NovTEC-2/">Новокуйбышевкая ТЭЦ-2 </a><br> <br>
7  <dd><dd><a href="http://server2/SamTEC/">Самарская ТЭЦ </a><br> <br>
8  <br>
9  <dd><H2>Саратовский регион</H2>
10 <br>
11 <dd><dd><a href="http://server3/SarTEC-1/">Саратовская ТЭЦ-1 </a><br> <br>
12 <dd><dd><a href="http://server3/SarTEC-2/">Саратовская ТЭЦ-2 </a><br> <br>
13 <dd><dd><a href="http://server3/SarTEC-3/">Саратовская ТЭЦ-3 </a><br> <br>
```

Рисунок 13.2 – Создание карты с помощью редактора HTML

Пользователи, не обладающие навыками работы с языком разметки гипертекстов (html), могут создать карту многоэкземплярной конфигурации с помощью текстового редактора MS Word.

Для создания карты многоэкземплярной конфигурации необходимо создать новый документ MS Word. В данном документе необходимо прописать названия экземпляров, которые требуются пользователю для работы (Рисунок 13.3).

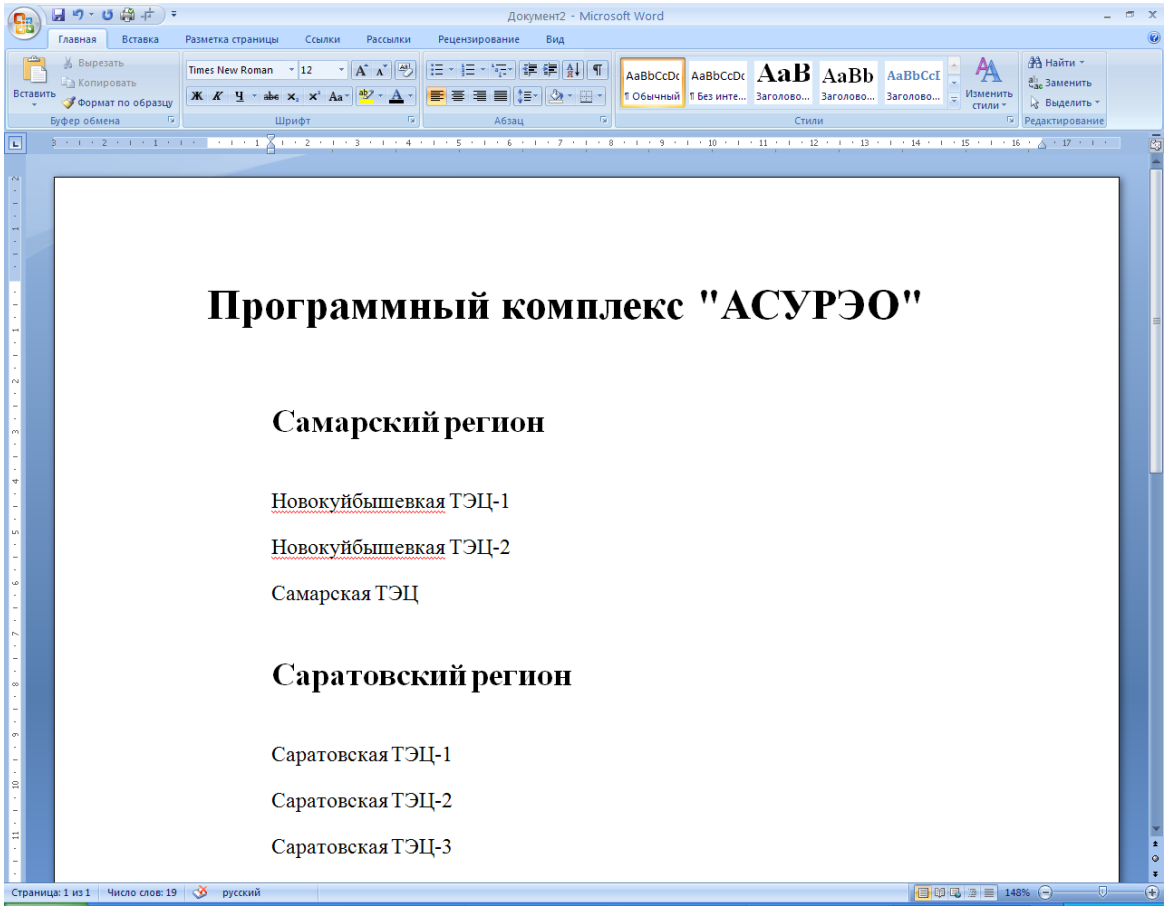

Рисунок 13.3 – Названия экземпляров в документ MS Word

Названия экземпляров должны представлять собой гиперссылки на соответствующие экземпляры ПК. Для этого необходимо выполнить следующие действия:

1) Выделить текст (в данном случае, название экземпляра).

2) На выделенном тексте нажать правой кнопкой мыши и в контекстном меню выбрать пункт «*Гиперссылка*» (Рисунок 13.4).

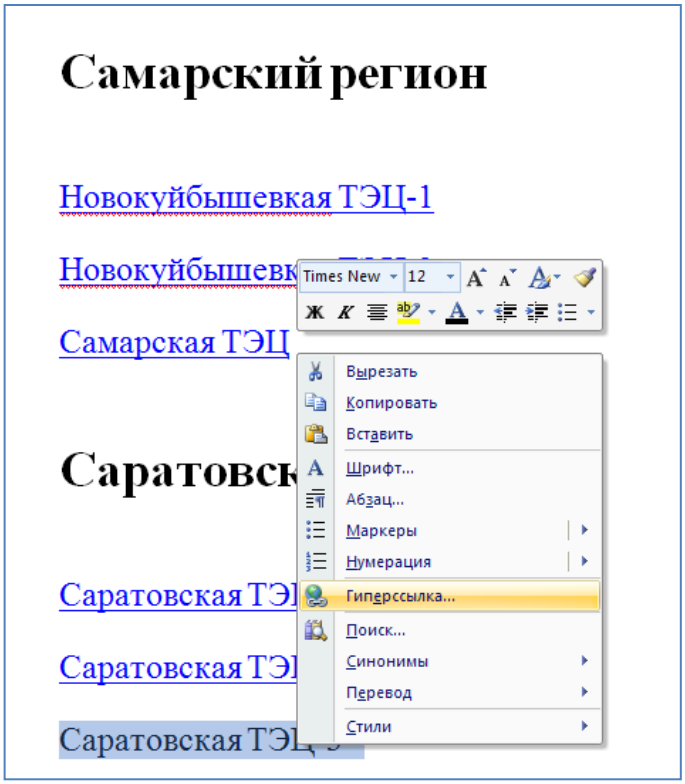

Рисунок 13.4 – Выделение названия экземпляра для вставки гиперссылки

3) В открывшемся диалоговом окне «*Гиперссылка*» в поле «*Адрес*» необходимо указать адрес к странице выбора интерфейсов соответствующего экземпляра (параметры запуска). Параметры запуска указываются в соответствии с установленным форматом (см. раздел «10.18 Настройка клиентского рабочего места»).

4) Нажать на кнопку «*ОК*» (Рисунок 13.5).

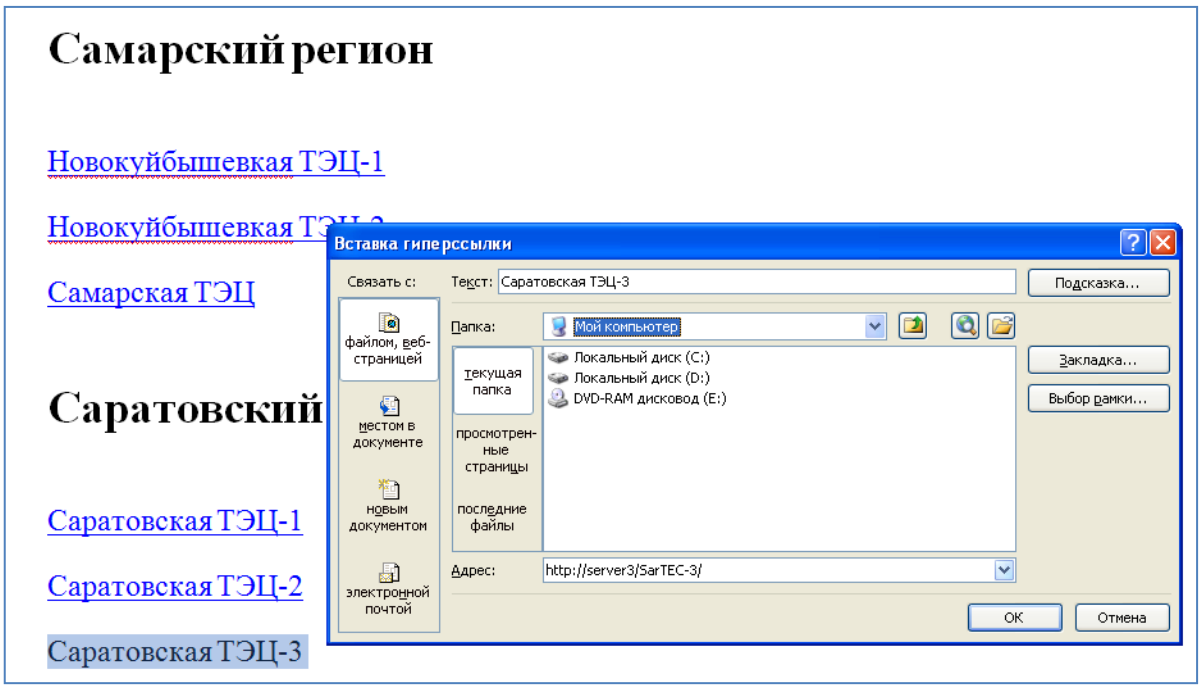

Рисунок 13.5 – Окно вставки адреса гиперссылки

5) Для каждого названия экземпляра повторить шаги 1-4.

Отформатированный текст документа представлен на рисунке 13.6.

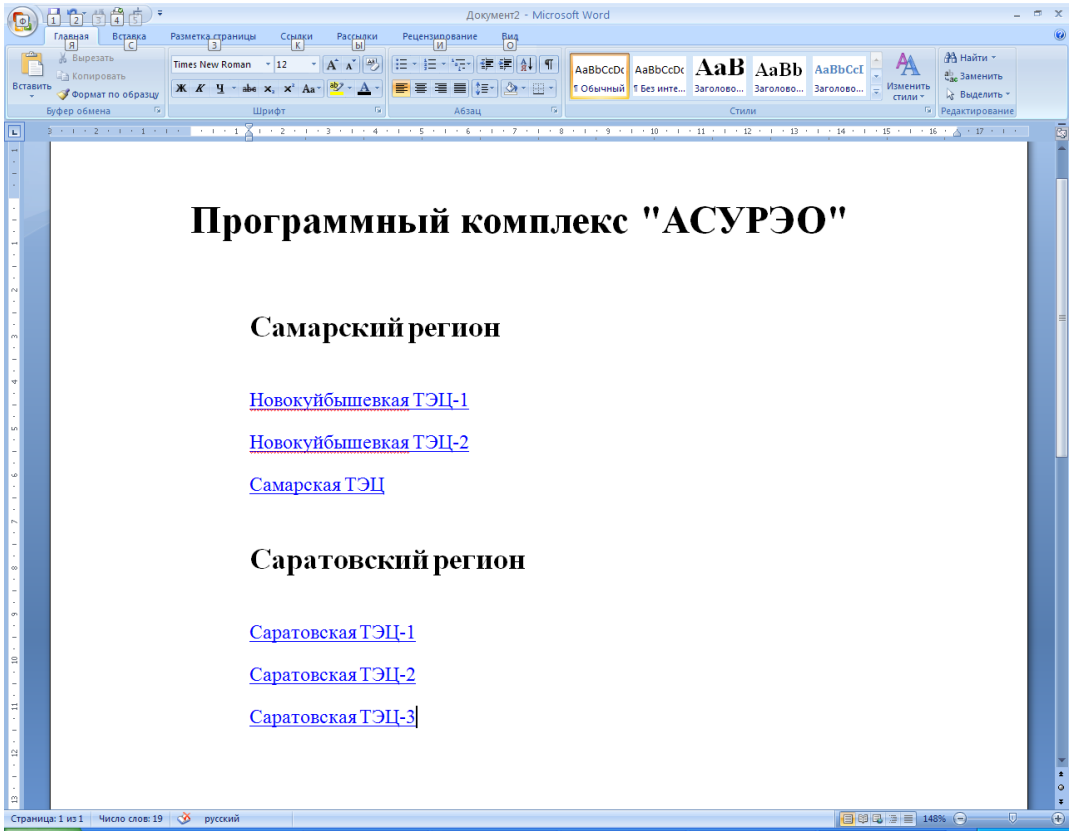

Рисунок 13.6 – Создание карты с помощью текстового редактора MS Word

По завершению форматирования документа его необходимо сохранить в формате HTML:

1) В раскрывающемся меню *«Сохранить как»* необходимо выбрать раздел *«Другие форматы»* (Рисунок 13.7).

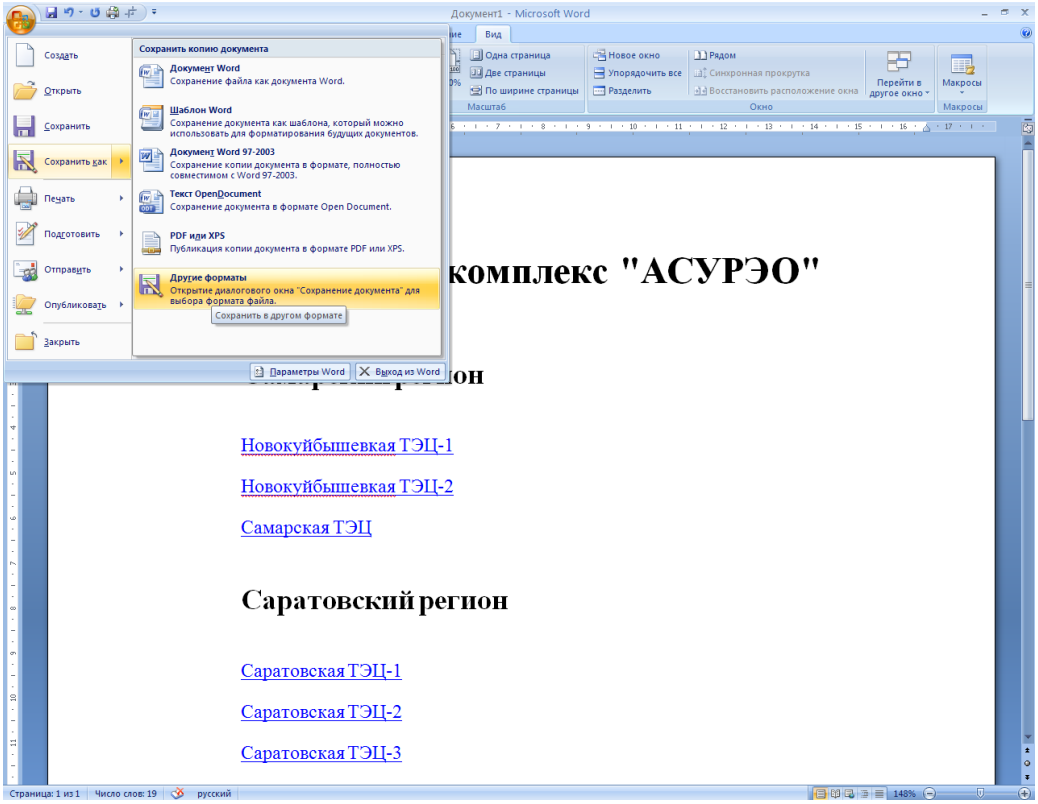

Рисунок 13.7 – Сохранение документа в формате HTML

2) В появившемся диалоговом окне «*Сохранение документа*» указать параметры сохранения: имя файла - index, тип файла - Веб-страница (Рисунок 13.8).

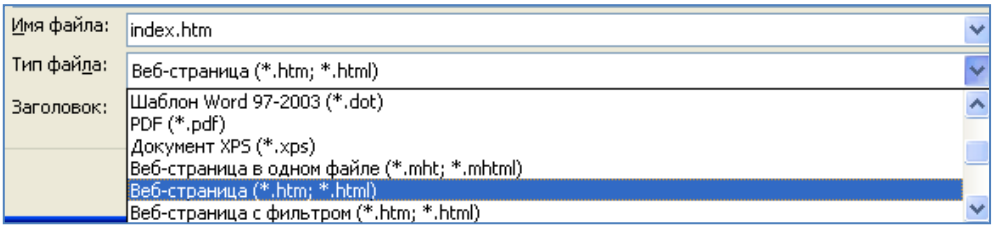

Рисунок 13.8 – Параметры сохранения

3) Нажать на кнопку «*Сохранить*».

13.3 Настройка карты многоэкземплярной конфигурации на сервере

Сохраненный файл «*index.html*» необходимо поместить в виртуальный каталог интернет сервиса. Путь к корневому виртуальному каталогу зависит от используемого веб-сервера:

для IIS: C:\Inetpub\wwwroot.

Ссылка на данную страничку будет иметь адрес: *http://<имя сервера>:<порт>/index.html* (по умолчанию порт 80).

Далее необходимо создать ярлыки, хранящие ссылку на созданную страничку, на клиентских машинах. Для этого необходимо выполнить следующие действия:

1) На рабочем столе вызвать правой кнопкой мыши контекстное меню и выбрать пункты: «*Создать*» => «*Ярлык*» (Рисунок 13.9).

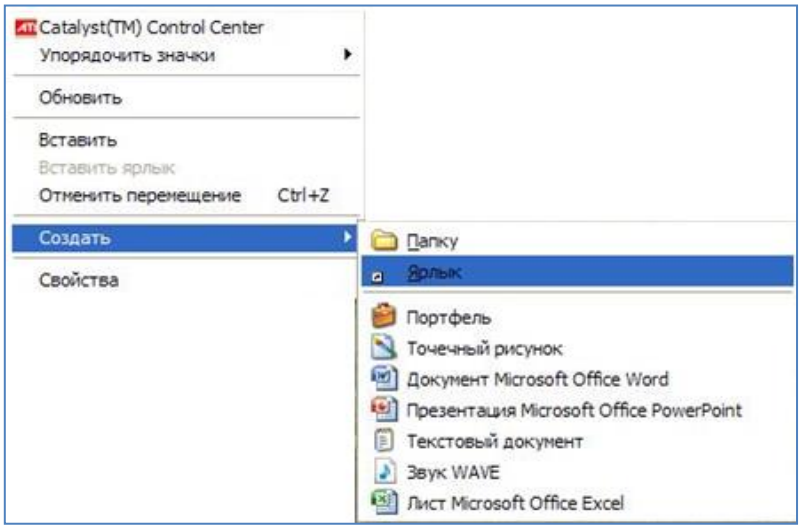

Рисунок 13.9 – Создание ярлыка

2) Указать размещение объекта (Рисунок 13.10):

- в окне «*Создание ярлыка*» нажать на кнопку «*Обзор…*»;
- в окне «*Обзор папок*» указать объект для ярлыка: «iexplorer.exe» (по умолчанию C:\Program Files\Internet Explorer).

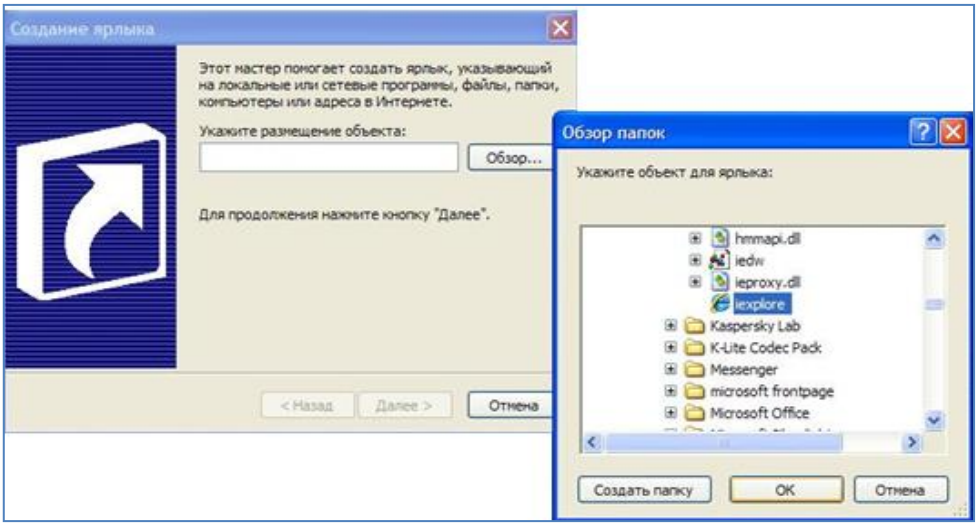

Рисунок 13.10 – Указание размещения объекта

3) В поле с адресом размещения объекта через пробел прописать: -new «адрес страницы», т.е. -new http://<имя сервера>:<порт>/index.html (Рисунок 13.11).

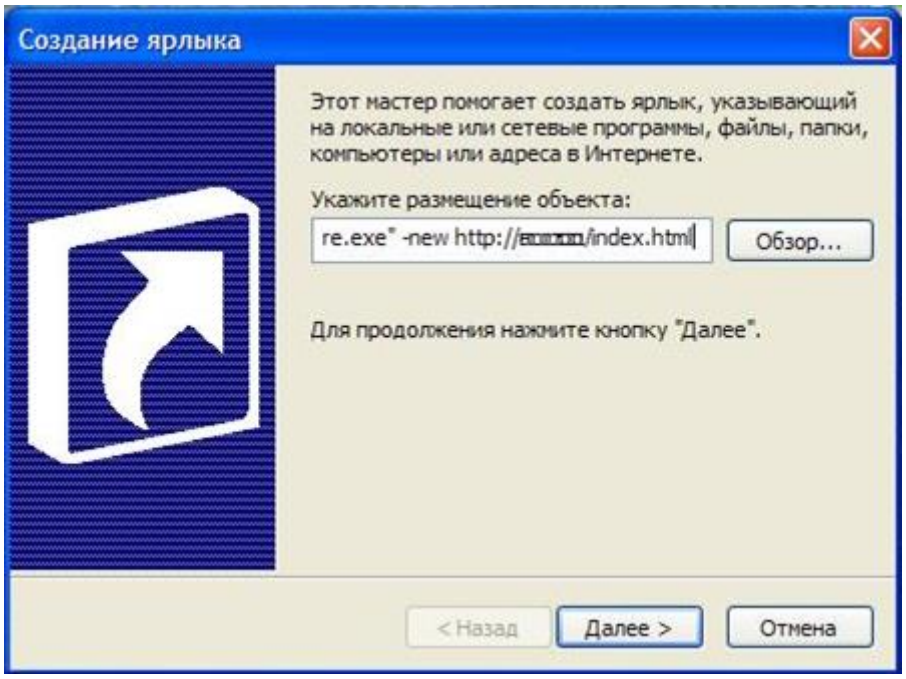

Рисунок 13.11 – Указание адреса страницы

4) Нажать на кнопку «*Далее*».

5) Ввести имя ярлыка и нажать на кнопку «*Готово*» (Рисунок 13.12).

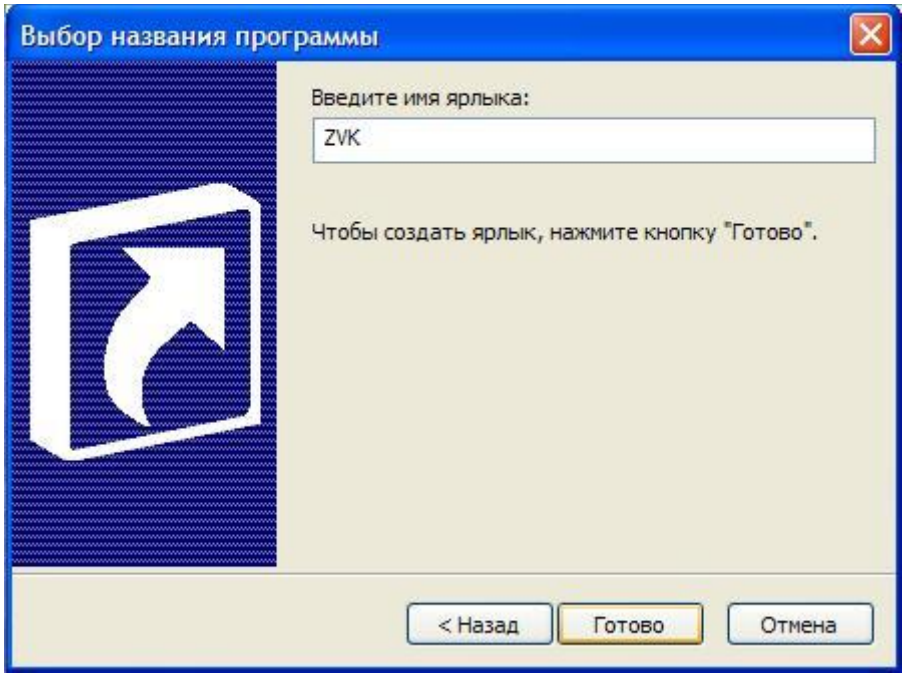

Рисунок 13.12 – Указание названия ярлыка

14 Логирование ПК

При принудительном останове сервера приложений в логе могут фиксироваться исключения типа Fatal, Access violation, ошибки или тексты невыполненных запросов. Текст ошибки представлен на рисунке 14.1.

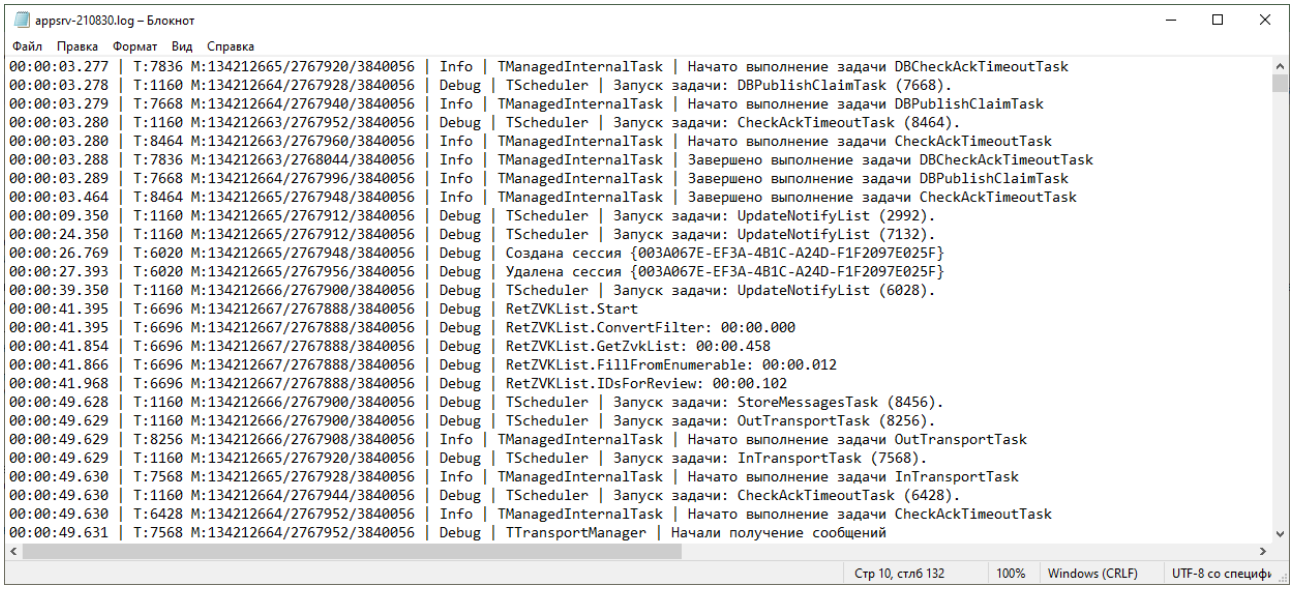

Рисунок 14.1 – Исключения типа Fatal и Access violation

Во избежание ошибок, рекомендуется:

1. Для оперативного анализа работы АСУРЭО просматривать текущие лог-файлы appsrv, FatalErr при помощи приложения Notepad++.
2. Избегать копирования файлов быстроизменяющихся текущих логов большего размера: WebCalls, ShedulerTasks.
3. При необходимости отправки файлов логов и их архивирования – производить архивирование в иную папку, отличную от папки с текущим логами.
4. При необходимости анализа или отправки файлов логов за текущие сутки (при работающем сервисе приложений АСУРЭО, особенно с высокой нагрузкой) – открывать в приложении Notepad++ и копировать содержимого файла лога в другой файл, расположенный вне папки с текущим логами.

При работе сервера приложения ПК «АСУРЭО» на ОС семейства Linux формируются логи сервера приложения. Файлы логов сервера приложения ПК «АСУРЭО» на ОС семейства Linux монтируются из docker контейнера на хост и расположены в каталоге /opt/asureo/Logs.

Файлы имеют расширение *.log. Каждый день записывается свой лог-файл и в имени прописывается дата создания файла.

Если удалить лог файлы в каталоге /opt/zvk/zrpNet/Logs во время работы сервера приложений ЗРП.Net, то лог файл не будет создаваться до перезапуска сервера приложений. Это нормальная работа сервера приложений.

В случае некорректной работы приложения рекомендуется просматривать лог файлы на наличие ошибок.

14.1 Удаление старых логов

При длительной работе ПК «АСУРЭО» накапливается много логов и их необходимо чистить, чтобы избежать поломки сервера – переполнением дискового пространства системы.

В Linux можно настроить Cron на ежедневую автоматическую очистку логов.

Для этого необходимо написать bash скрипт с именем «del_logs.sh»:

```
#!/bin/bash
# del Logs if > 30 days
find /opt/asureo/Logs/ -type f -mtime +30 -exec rm -rf {} \;
```

Сохранить скрипт и сделать его исполняемым.

Далее необходимо настроить Cron - sudo crontab -u root –e

И добавить в конец файла расписание запуска и путь до скрипта:

```
#Запуск скрипта очистки логов старше 30 дней каждый день в час ночи
0 1 * * * /opt/asureo/del_logs.sh # delete logs if > 30 days
```

15 Рекомендации для администраторов

15.1 Рекомендации по обновлению PostgreSQL версии 12 до 15

Обновлении версии PostgreSQL необходимо производить только после обновления АСУРЭО до версии не ниже 10.20.35.XX.XX, т.к. версии ниже не работают с версией PostgreSQL15.

15.2 Рекомендации о периодическом ребилдинге индексов в базе ПК

В процессе работы АСУРЭО в БД MS SQL Server происходит фрагментация индексов, что замедляет работу БД. Данное замедление сказывается на производительности ПК.

Реорганизация (reorganize) индексов проводится, если степень фрагментации составляет до 30%, иначе для повышения производительности необходимо использовать перестроение индексов (rebuild).

Определить степень фрагментации БД возможно с помощью встроенного в MS SQL Server отчета – Index-Physical Statistics. Его запуск: нажатием правой кнопкой мыши на требуемой БД – *Отчеты (Reports) – Стандартный отчет (Standard Reports) – Физическая статистика индекса (Index Physical Statistics)* (Рисунок 15.1).

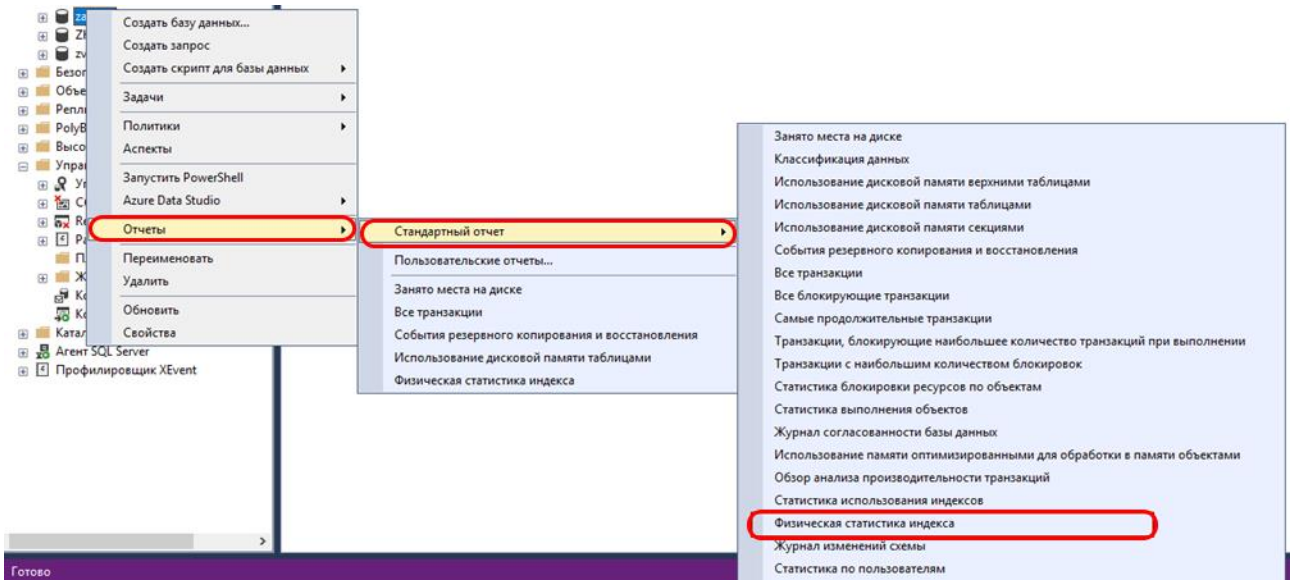

Рисунок 15.1 – Запуск отчета

После запуска отчета будет выведена информация о фрагментации (Рисунок 15.2).

dbo.WorkState

Index Name	Index Type	# Partitions	Depth	Operation Recommended
PK__WorkState__60725 1E5	NONCLUSTERED INDEX	1	1	-
UniqueIdentWS	NONCLUSTERED INDEX	1	1	-

dbo.ZVKBody

Index Name	Index Type	# Partitions	Depth	Operation Recommended
Index_ZVKBody_ForRev iew	NONCLUSTERED INDEX	1	3	Rebuild

Partition No.	Avg. Fragmentation (%)	# Fragments	Avg. Pages Per Fragment	# Pages
1	73	1 187	1	1 622

Рисунок 15.2 – Информация о фрагментации

По итогам отчета надо выбрать, каким способом выполнить оптимизацию БД.

Оптимизацию рекомендуется запускать периодически. Для этого можно создать план обслуживания БД. Maintenance Plan Wizard присутствует в выпусках Standard и Enterprise. Для запуска мастера необходимо:

1) Подключиться к необходимой базе.

2) Выбрать Management.

3) Выбрать Maintenance Plan.

4) На Maintenance Plan нажать правой кнопкой мыши и в контекстном меню выбрать Maintenance Plan Wizard.

С помощью данного мастера можно создать нужный план обслуживания:

1. Для запуска мастера создания плана обслуживания надо в контекстном меню Планы обслуживания (Maintenance Plan) выбрать *Мастер планов обслуживания (Maintenance Plan Wizard)* (Рисунок 15.3).

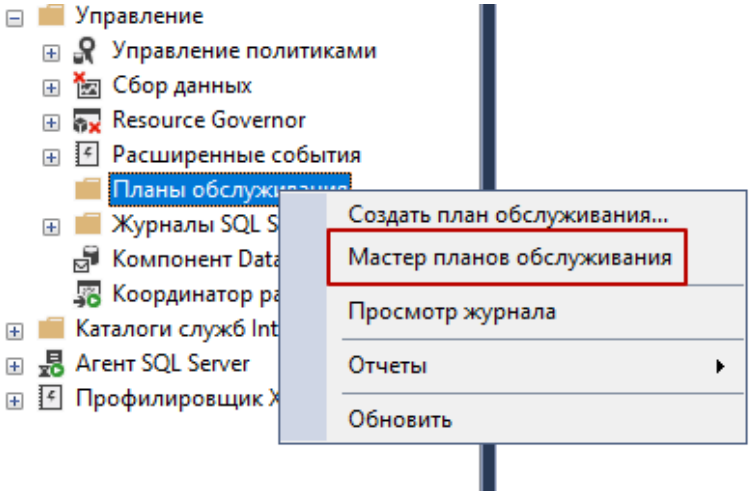

Рисунок 15.3 – Запуск мастера создания плана обслуживания

2. При запуске мастера сначала появится стартовая страница с описанием мастера (Рисунок 15.4).

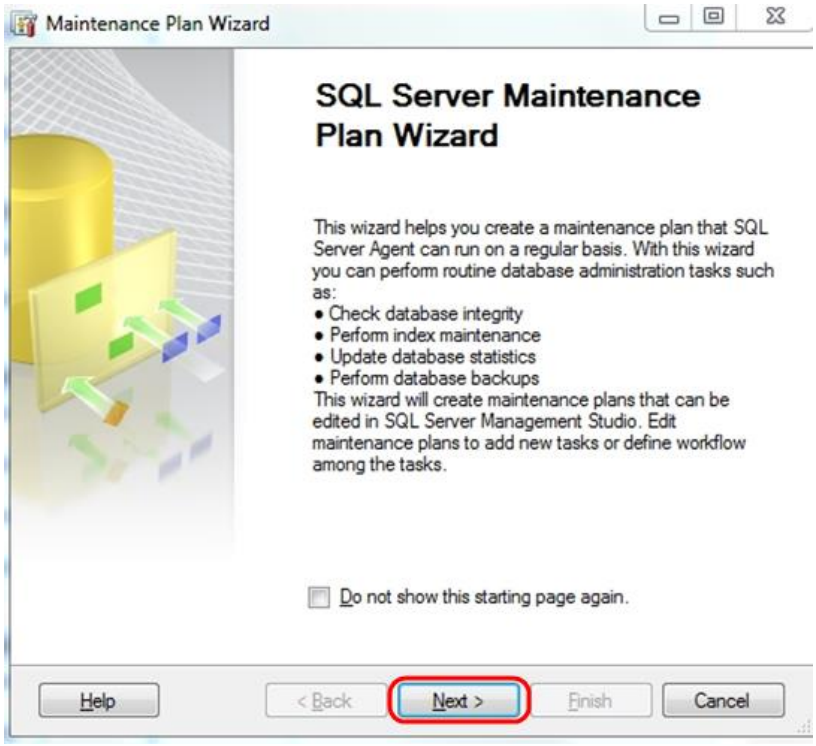

Рисунок 15.4 – Стартовая страница «Мастер планов обслуживания (Maintenance Plan Wizard)»

3. Далее необходимо задать имя и описание плана обслуживания (Рисунок 15.5).

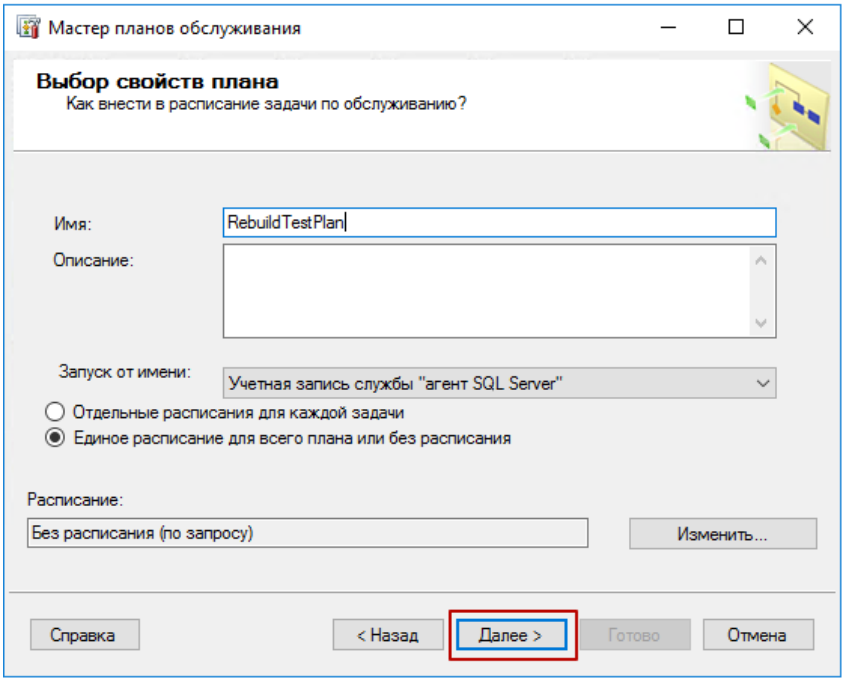

Рисунок 15.5 – Задание имени плана обслуживания

4. При выборе имени также надо выбрать расписание выполнения данного плана обслуживания. Время надо выбирать, когда нагрузка на БД минимальна. В примере это каждое воскресенье в 0:00 (Рисунок 15.6).

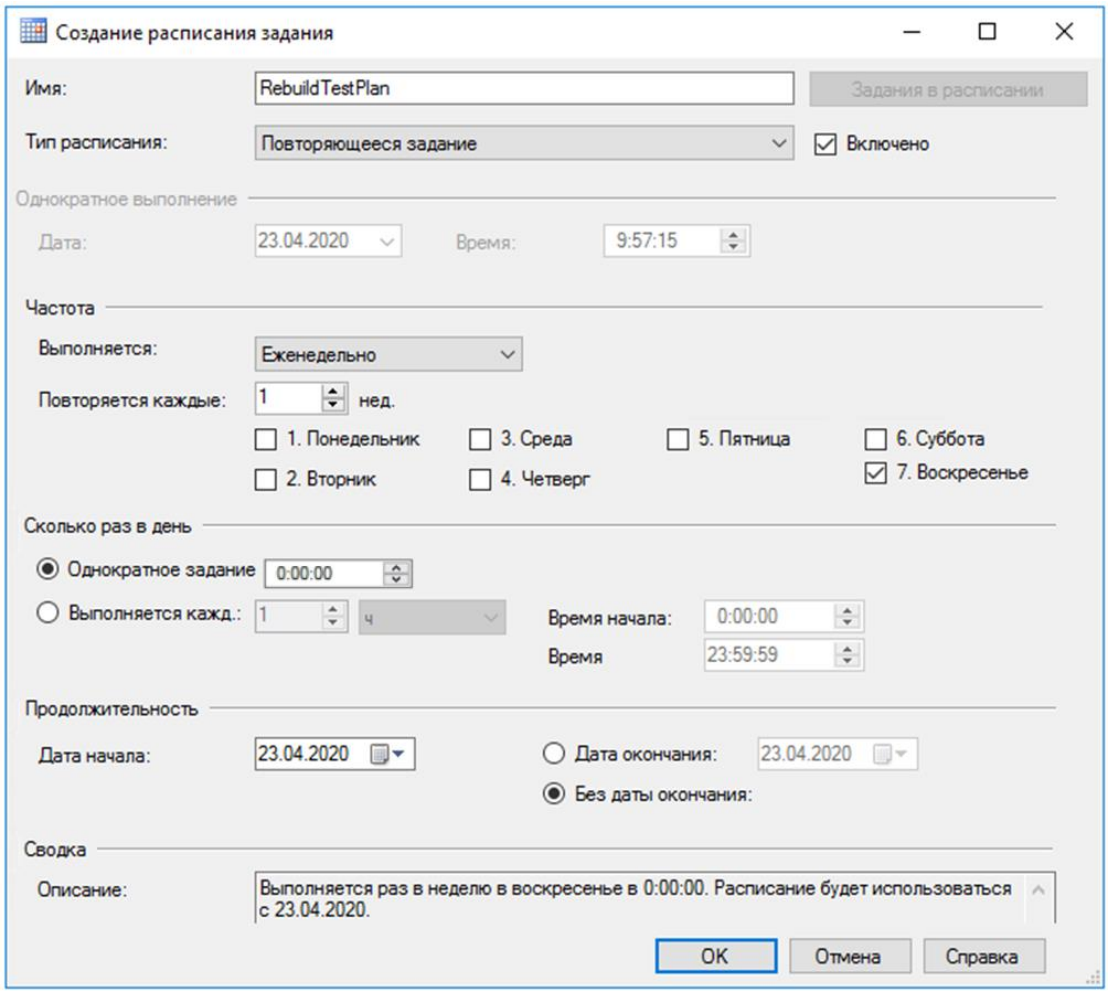

Рисунок 15.6 – Выбор расписания

5. После задания имени и времени выполнения плана обслуживания надо выбрать вид проводимых работ. В данном случае будет произведено пересоздание всех индексов (Рисунок 15.7).

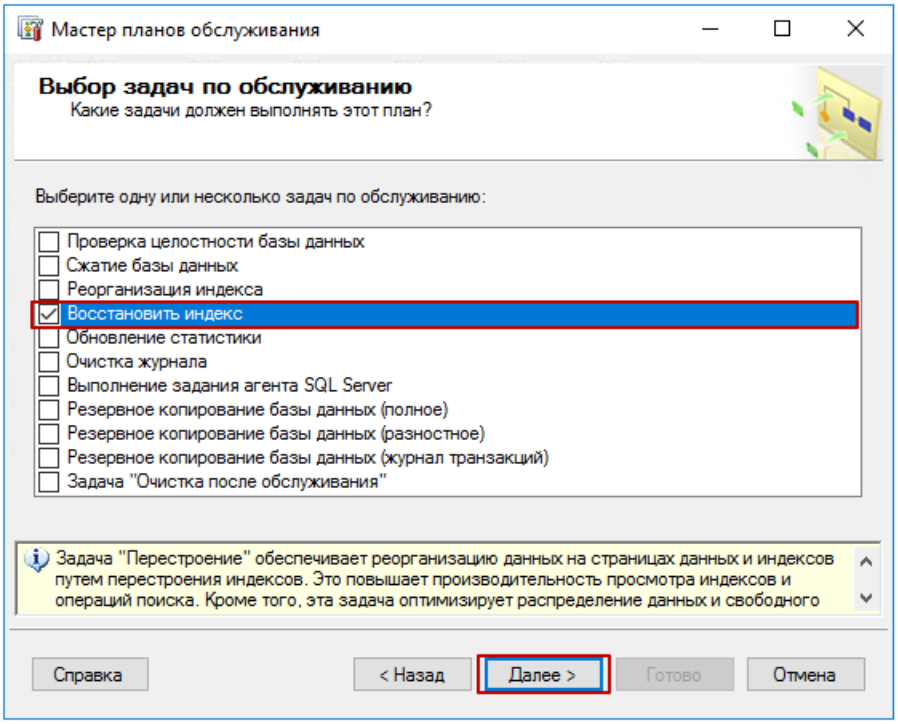

Рисунок 15.7 – Выбор опции «Восстановить индекс (Rebuild Index)»

6. Далее надо выбрать порядок выполнения задач в плане обслуживания. В один план обслуживания можно сделать несколько задач и выбрать порядок их выполнения. В представленном случае задача одна (Рисунок 15.8).

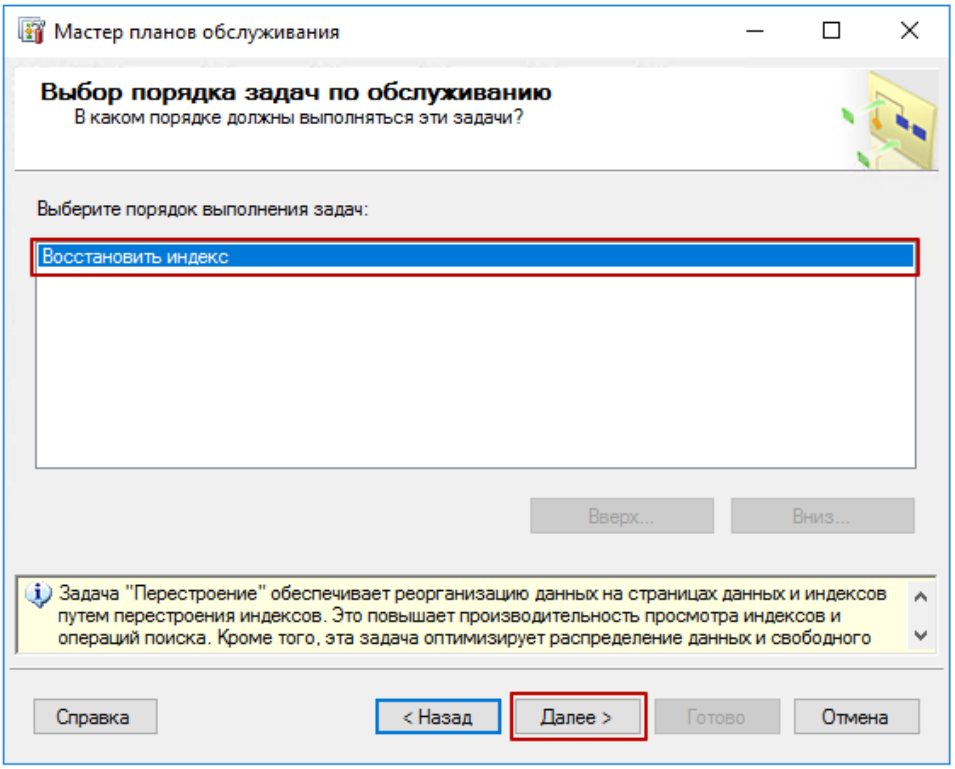

Рисунок 15.8 – Выбор порядка выполнения задач

7. После выбора порядка выполнения задач надо выбрать БД, к которым данный план обслуживания будет применяться (Рисунок 15.9).

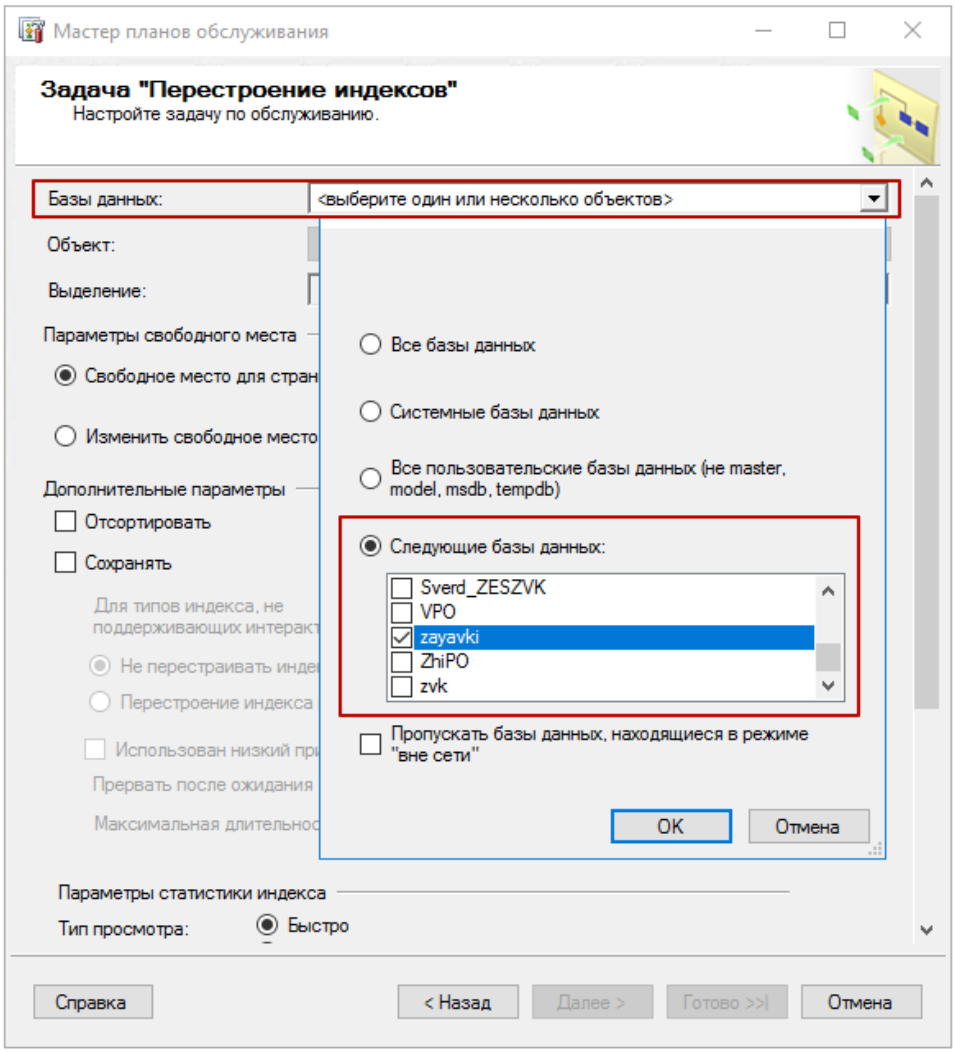

Рисунок 15.9 – Выбор БД

8. На следующем этапе надо выбрать папку, куда будет писаться лог выполнения работ (Рисунок 15.10).

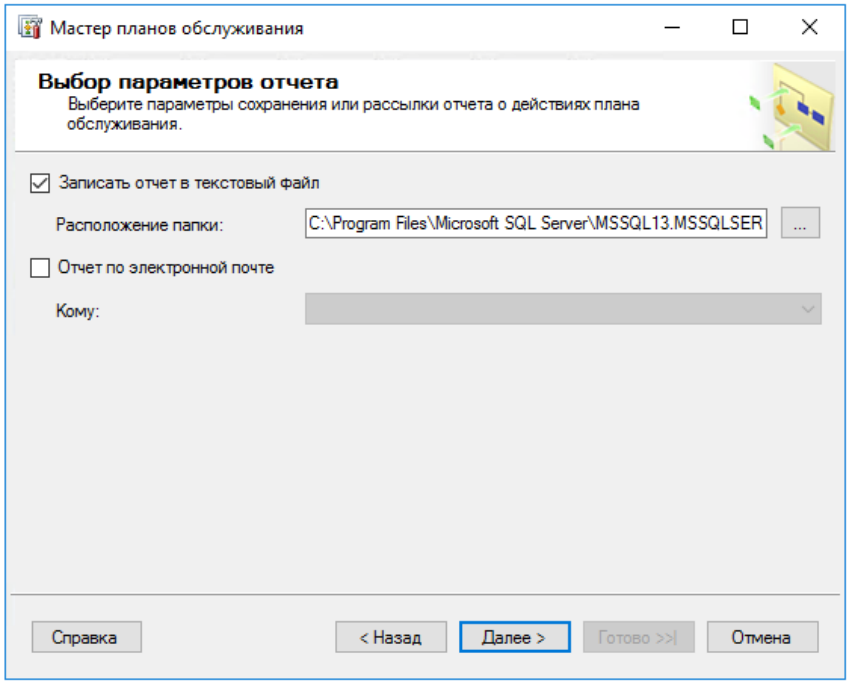

Рисунок 15.10 – Выбор папки, куда будет писаться лог выполнения работ

9. После прохождения всех этапов мастера будет выведено резюме о созданном плане обслуживания (Рисунок 15.11).

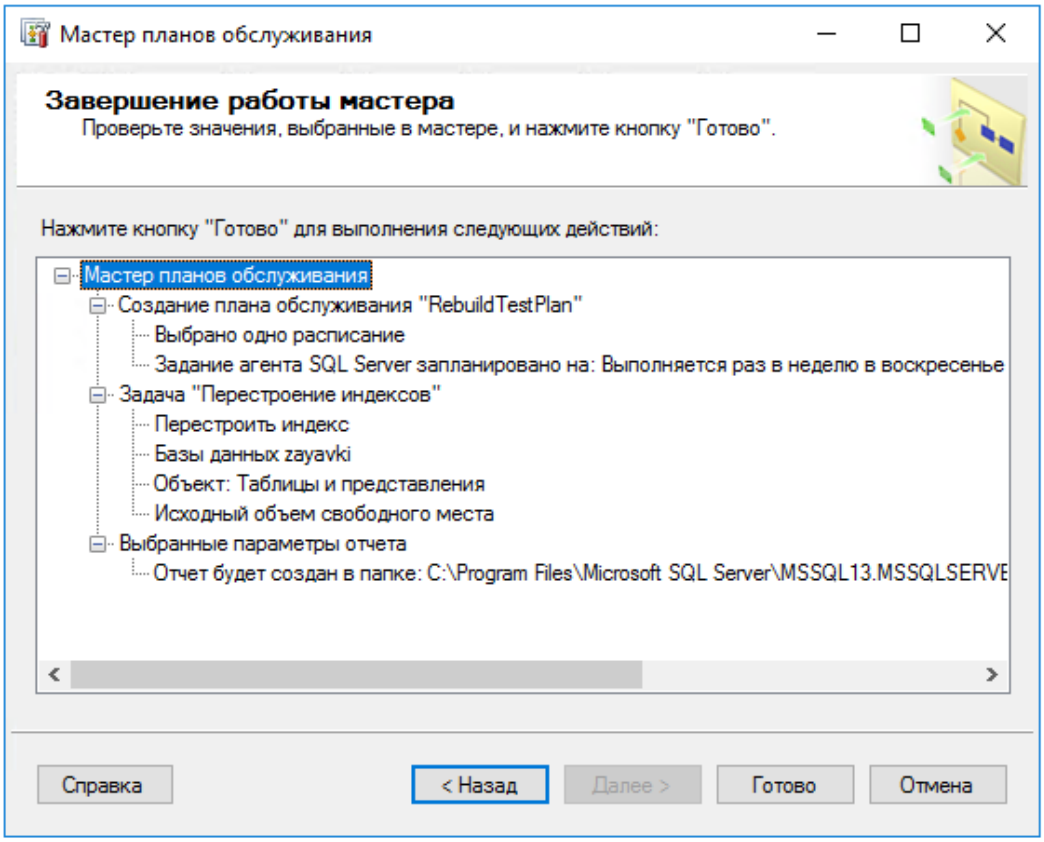

Рисунок 15.11 – Резюме о созданном плане обслуживания

10. После нажатия кнопки *«Готово» (Finish)* будет выведен отчет о создании плана обслуживания (Рисунок 15.12).

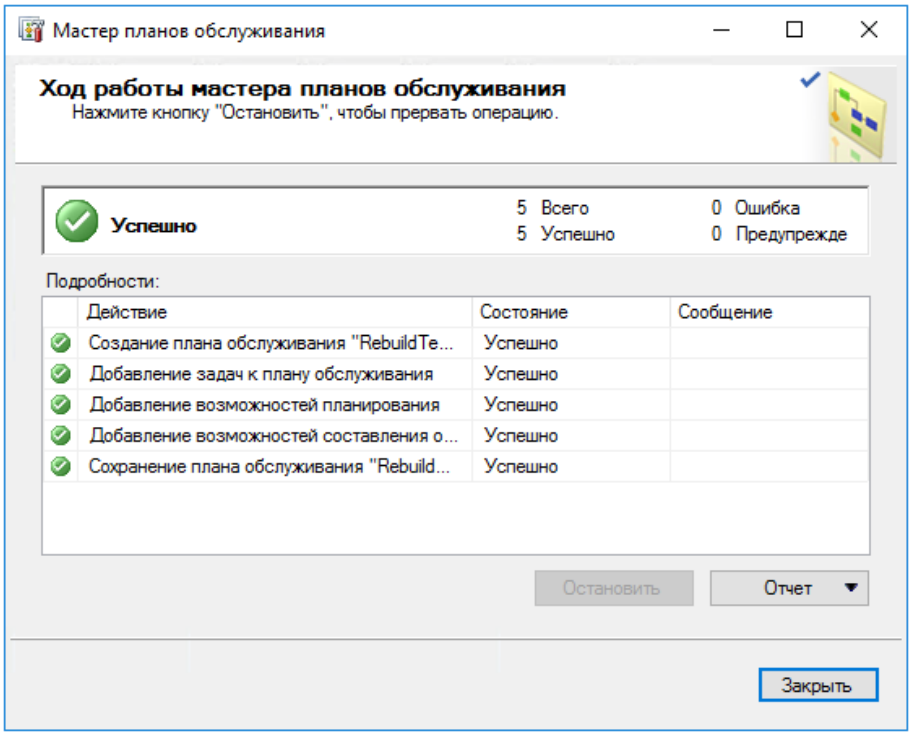

Рисунок 15.12 – Отчет о создании плана обслуживания

После создания плана обслуживания его можно вручную запустить на выполнение. По результатам будет выведено сообщение, в котором будет описан результат выполнения. На рисунке 15.13 приведен пример успешного выполнения плана обслуживания.

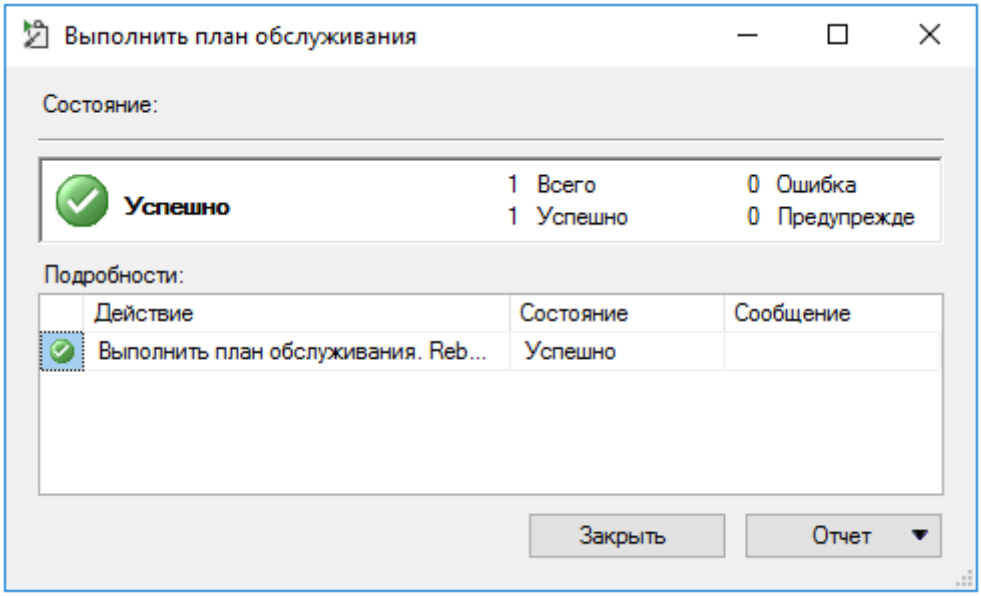

Рисунок 15.13 – Сообщение о результате выполнения плана обслуживания

Дополнительно можно вызвать отчет о выполнении плана обслуживания. Для этого необходимо нажать кнопку *«Отчет» (Report)* и выбрать *«Сохранить отчет в файл…» (Save Report to File…)* (Рисунок 15.14).

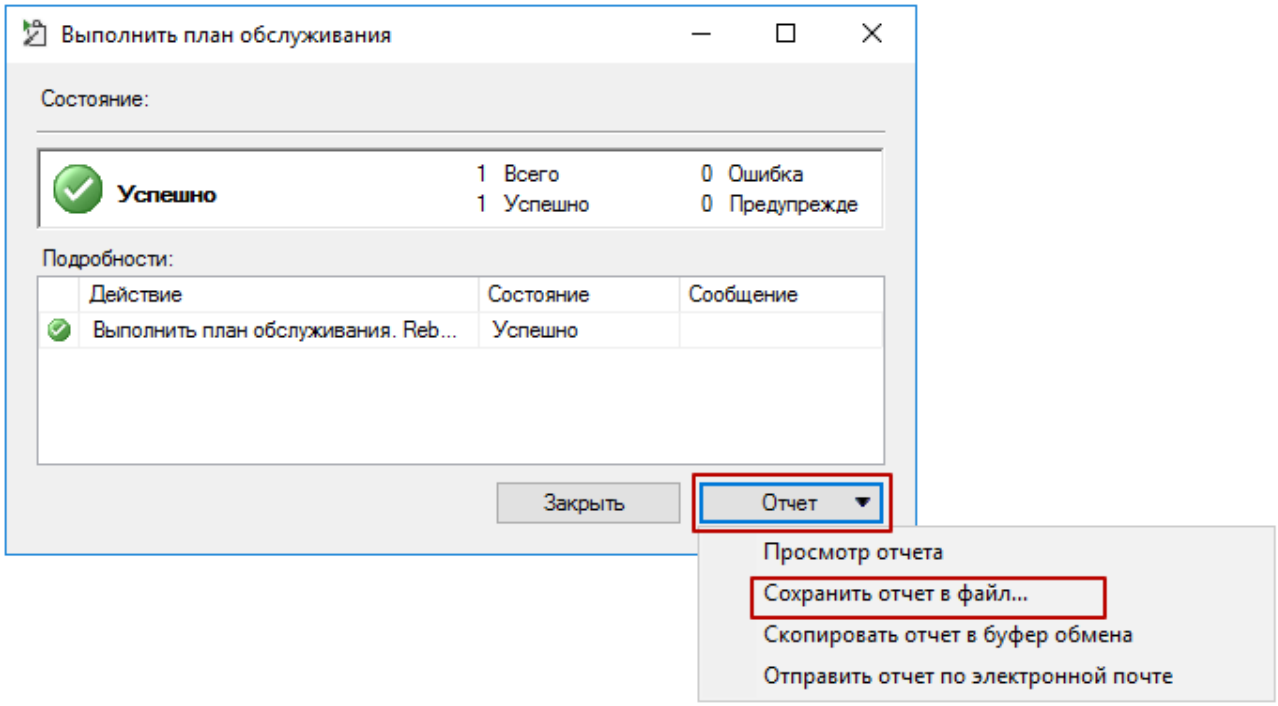

Рисунок 15.14 – Вызов отчета о выполнении плана обслуживания

На рисунке 15.15 представлен пример отчета о выполнении плана.

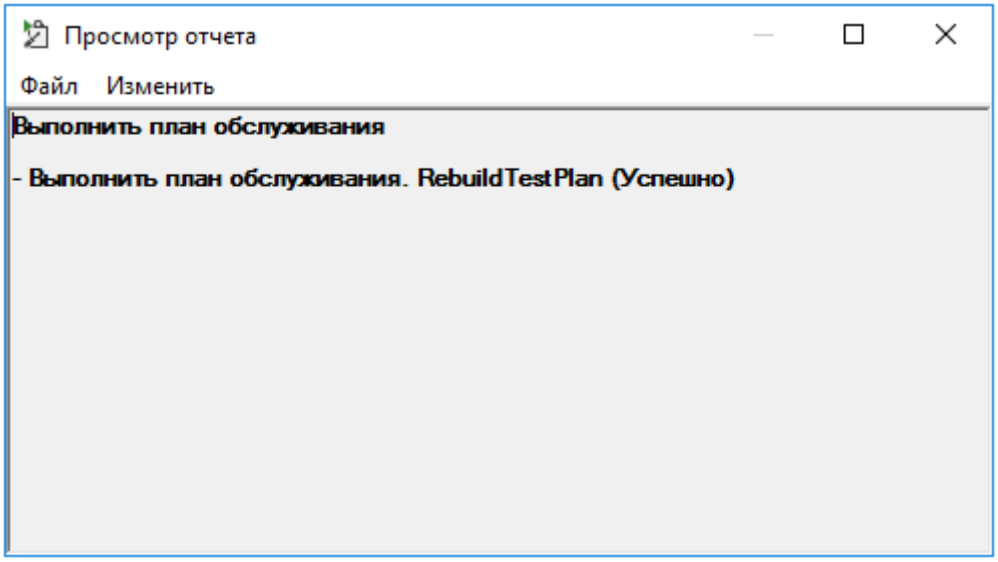

Рисунок 15.15 – Пример отчета о выполнении плана

Лог выполнения планов обслуживания хранится (если не был выбран другой путь хранения логов в п.8) в папке Log в директории куда был установлен MS SQL Server. Имя

файла, например, выглядит так – rebuild_Subplan_1_20150526152201. Где rebuild имя плана обслуживания. В файле содержится подробная информация о выполнении.

15.3 Рекомендации об усечении лога транзакций

При активном использовании АСУРЭО возможно сильное увеличение физического размера файлов БД на жестком диске. Как правило, основное увеличение приходится на лог транзакций БД. В этом случае рекомендуется периодически контролировать размер файла **.ldf** (например, файл (*kla) **.ldf** может занимать 30 Гб, а размер самой базы (*mdf) быть не более 1 Гб) и, при необходимости, делать усечение лога транзакций. Процедуру можно проводить как вручную, так и автоматически при помощи планировщика заданий MSSQL Server.

Если в логе сервера приложений появляется ошибка вида:

```
21:22:16.854 T:6068 M:134216735/422572/928528 Debug: Возбуждено исключение:
  EMSSQLNativeException:  [FireDAC][Phys][ODBC][Microsoft][SQL Server Native Client 11.0][SQL Server]The transaction log for database 'zvk_oduyu' is full due to 'LOG_BACKUP'.
```

которая говорит о том, что переполнен лог транзакций, необходимо после уменьшения лога транзакций перезапустить службу сервера приложений.

15.4 Рекомендации по обработке ошибок

15.4.1 Ошибка при установке ПК

В установщике на шаге *«Выбор веб-сайта»* в случае возникновения ошибки будет предоставлена информация об ошибке и ссылки расположения дистрибутивов (Рисунок 15.16).

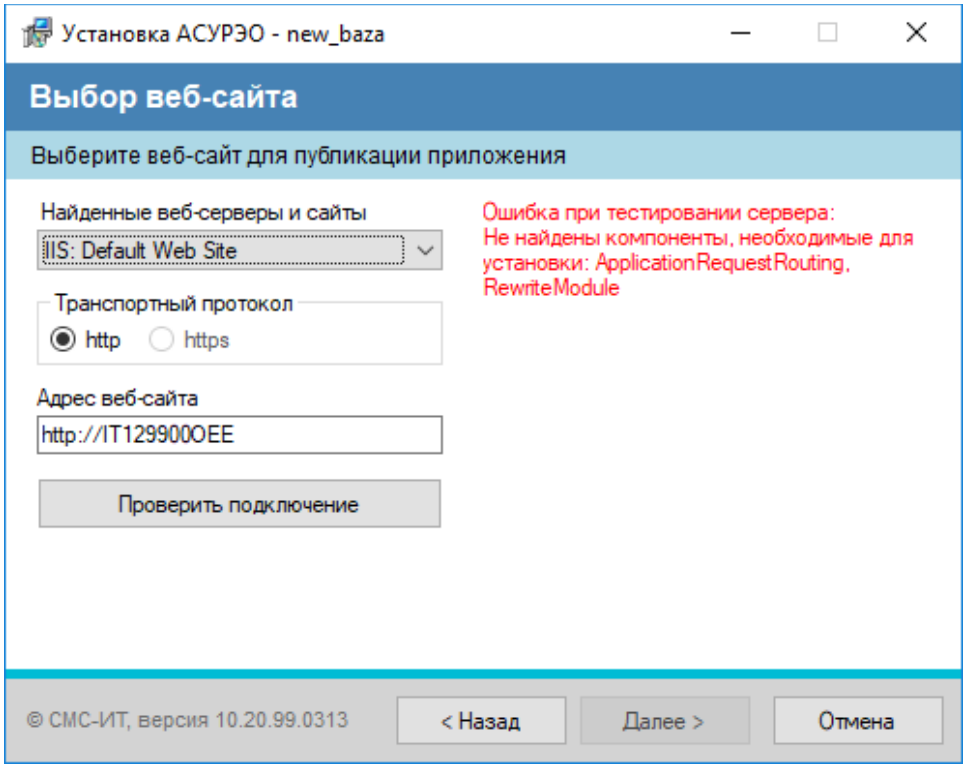

Рисунок 15.16 – Установка дополнительных компонентов IIS

Установка компонента переадресации запросов URL Rewrite 2.0 и установка компонента прокси-переадресации Application Request Routing 2.0 описана в разделе «9 Установка и настройка системного ПО».

При необходимости, нужно протестировать соединение с указанным сервером с помощью кнопки *«Проверить подключение»*.

15.4.2 Ошибка при обновлении ПК

При обновлении ПК в случае возникновения ошибки, не позволяющей произвести обновление необходимо сделать снимок экрана и обратиться в службу поддержки СМС-ИТ.

15.4.3 Ошибка при запуске сервера приложений

Если сервер приложений не стартует, то в лог добавляется информация о зацикливании оборудования: «Ошибка создания справочника оборудования: элемент Id='1111' ссылается сам на себя». Данная ошибка означает, что произошло зацикливание оборудования самого на себя.

Старт сервера приложений не возможен: необходимо обратиться в службу поддержки СМС-ИТ.

15.4.4 Ошибка при установке соединения с сервером приложений

В случае возникновения ошибки при получении информации с сервера выдается соответствующее сообщение об ошибке (Рисунок 15.17).

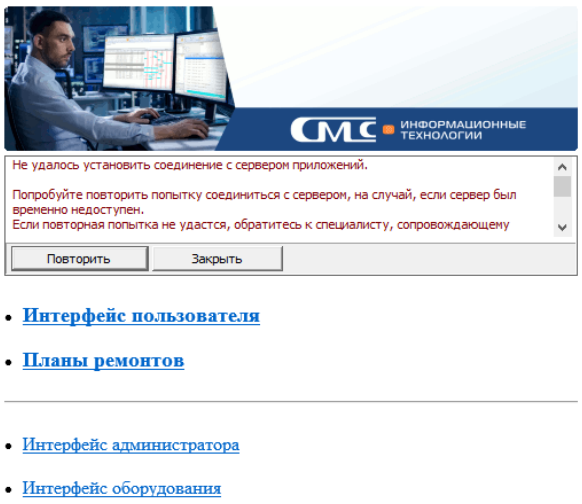

Рисунок 15.17 – Ошибка при получении пакета установки с сервера

Необходимо обратиться в службу поддержки СМС-ИТ.

После устранения причин ошибки необходимо запустить обновление версии приложения, нажав кнопку *«Повторить»*.

15.4.5 Ошибка при запуске приложения

В случае возникновения ошибки при запуске приложения (Рисунок 15.18) необходимо завершить все приложения, использующие Wine, например, Интерфейс пользователя или Интерфейс администратора и выполнить команду *wineserver -k*.

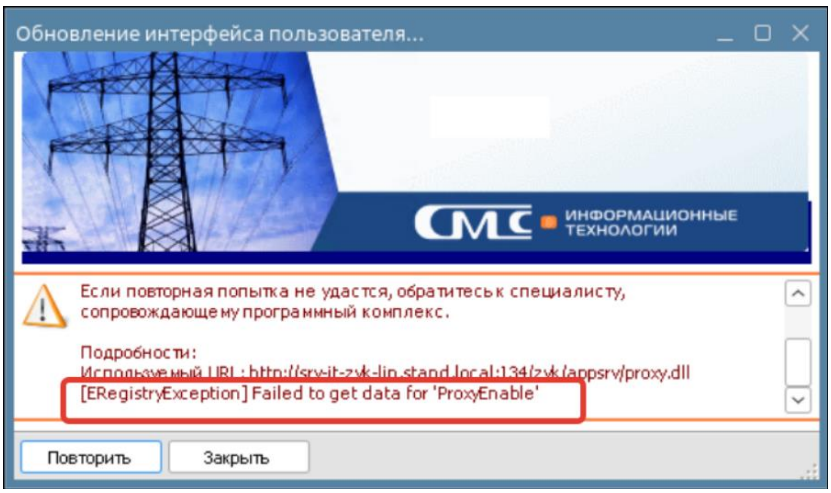

Рисунок 15.18 – Ошибка при запуске приложения

В редакторе реестра Wine в разделе:

«Компьютер\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings» создать DWORD параметр ProxyEnable со значением «0» (Рисунок 15.19).

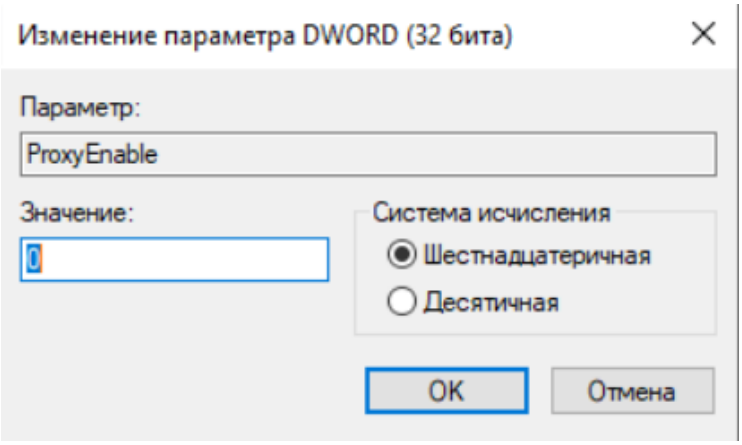

Рисунок 15.19 – Изменение параметра DWORD (32 бита)

15.4.6 Ошибка при удалении HTTPS

После удаления экземпляра ПК, работающего через https, возможна ситуация, при которой старт веб-сервера IIS может не осуществиться. Это может быть связано с тем, что другие приложения используют 443 порт. Для исправления этой ошибки необходимо выполнить следующие действия:

1. Запустить командную строку – на клавиатуре нажать клавиши «Win+R», в открывшемся окне «Выполнить» ввести команду «cmd» и нажать кнопку [OK].
2. В командной строке ввести и выполнить команду: ***netstat -aonnetstat –aon***
3. В полученной статистике найти приложения, которые используют 443 порт.
4. Остановить программы, которые используют 443 порт.

15.5 Рекомендации по ограничению объема занимаемой памяти

При достижении сервером приложений zvkservice.exe допустимого объема памяти ≈ 12 ГБ рекомендуется перезапустить сервер приложений.

Информация о превышении допустимого объема память фиксируется в логах системы и диспетчере задач.

Пример отображения информации в логе для контроля объема допустимой памяти:

00:00:45.798 T:4696 M:3192/657184/903448, где:

- 00:00:45.798 – время;
- T:4696 – ID нити процесса;
- M:3192 – объем оставшейся памяти (Мб);
- 657184 – объем занимаемой память (Кб);
- 903448 – пик максимальной памяти за текущий сеанс (Кб).

15.6 Рекомендации по штатному останову серверов приложений

При выполнении регламентных работ по перезапуску серверов, а также при выполнении обновлений АСУРЭО для штатной остановки АСУРЭО.Delphi и АСУРЭО.Net рекомендуем применять скрипт serverstop.sh (см. Приложение 2. Скрипт для штатного останова серверов приложений АСУРЭО).

Для штатной остановки серверов приложений необходимо выполнить следующие действия:

- Скопировать скрипт serverstop.sh на сервер.
- Командой *sudo chmod +x serverstop.sh* сделать скрипт исполняемым.
- Выполнить *./serverstop.sh* из терминала из директории, где лежит скрипт serverstop.sh.

15.7 Рекомендации по настройке параметра «client_max_body_size»

В случае, если в результате отправки графика ремонтов в Журнале сообщений подсистемы «Ремонты» отображается ошибка: «модуль SOAP. Ошибка Send: HTTP/1.1.413 Request Entity Too Large», то на предприятие-приемнике и предприятие-инициатора необходимо для веб-сервера nginx увеличить параметр «client_max_body_size» (Рисунок 15.20).

Для этого необходимо:

1. Открыть конфигурационный файл nginx: sudo nano /etc/nginx/nginx.conf
2. Добавить строку: client_max_body_size 50M;
3. Перезапустить nginx: *sudo systemctl restart nginx*.

```
*nginx.conf
1  user  www-data;
2  worker_processes  auto;
3
4  error_log  /var/log/nginx/error.log notice;
5  pid        /var/run/nginx.pid;
6
7  load_module /etc/nginx/modules-enabled/ngx_http_auth_spnego_module.so; # Настройки для spnego
8
9
10 events {
11     worker_connections  1024;
12 }
13
14
15 http {
16   map $http_upgrade $connection_upgrade {
17     default upgrade;
18     '' close;
19   }
20
21     include       /etc/nginx/mime.types;
22     default_type  application/octet-stream;
23
24     log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
25                       '$status $body_bytes_sent "$http_referer" '
26                       '"$http_user_agent" "$http_x_forwarded_for"';
27
28     access_log  /var/log/nginx/access.log  main;
29
30     sendfile        on;
31
32     client_max_body_size 50M;
33
34     keepalive_timeout  65;
35
36     include /etc/nginx/sites-enabled/default.conf;
37 }
38
```

Рисунок 15.20 – Увеличение параметра «client_max_body_size»

15.8 Рекомендации по увеличению лимитов по открытым файлам на ОС Linux

В связи с утечками дескрипторов в ОС Linux при использовании Wine, необходимо увеличить лимиты по открытым файла, чтобы не возникало проблем в работе АСУРЭО из-за нехватки лимитов по умолчанию. При использовании кластера выполнить на обоих серверах.

Для этого необходимо выполнить следующие действия:

1. Увеличить ограничение на открытие файлов, выполнив команду:

   sudo nano /etc/security/limits.conf

   Добавить:

   - soft nofile 1048576
   - hard nofile 10485760

2. Выполнить команду: *sudo nano /etc/sysctl.conf*

   Добавить:

   - fs.file-max = 15728640
   - fs.nr_open = 20971520

3. Далее необходимо выполнить команду: *sudo sysctl –p*
4. Перезапустить сервер для вступления лимитов в силу.
5. В docker-compose.yml для контейнера сервера приложений на одном уровне с блоком image добавить блок вида:

   ulimits:

   nofile:

   soft: 1048576

   hard: 10485760

6. После чего перезапустить экземпляр с помощью команды *docker-compose down -v && docker-compose up -d*, предварительно перейдя в папку с docker-compose.yml.

ВАЖНО. Правки в docker-compose.yml вносить только после внесения изменений в системные файлы и перезагрузки сервера. Лимиты контейнера не могут быть больше лимитов системы, соответственно указываем либо равные системным лимитам, либо меньше.

Приложение 1. Набор файлов установленного экземпляра

После успешного завершения процесса установки ПК в папке «C:\Program Files (x86)\ZVK» будет создана папка с именем экземпляра, указанного при установке.

Папка экземпляра содержит набор файлов (Таблица 1), необходимых для корректной работы комплекса (путь указан относительно пути «C:\Program Files (x86)\ZVK\<название экземпляра>\»).

Таблица 1 – Набор файлов установленного экземпляра

Название файла (папки) и путь	Описание
..\help\	Набор файлов контекстно-зависимой справки
..\Logs\	Набор файлов лога, каждый из которых относится к соответствующей дате
..\server\	Набор файлов, организующих работу сервера приложений
..\server\iconv.dll	Системная библиотека
..\server\zvk.ini	Файл инициализации программного комплекса
..\server\ZVKService.exe	Служба, реализующая функции сервера приложений
..\server\Server110.bpl	Библиотека, реализующая логику работы ПК
..\server\ZVK.sms	Библиотека, реализующая логику работы ПК
..\server\zvkcomm110.bpl	Библиотека, реализующая логику работы ПК
..\server\ZvkDevStat.sms	Библиотека, реализующая логику работы ПК
..\server\Client	Набор файлов интерфейсов ПК
..\server\Client\DeviceDescr.exe	Интерфейс оборудования
..\server\Client\ZVKAdmin.exe	Интерфейс администратора
..\server\Client\ZVKUser.exe	Интерфейс пользователя
..\server\Client\Zvk.exe	Интерфейс стартовой страницы выбора интерфейсов
..\server\Client\alert.wav	Звуковой файл с оповещением о приходе сообщений
..\server\events\	Набор библиотек, осуществляющих связь программного комплекса с внешними системами через обработчиков событий
..\server\format\	Набор библиотек, реализующих обмен сообщениями определенного формата
..\server\format\maket\maket_mod.dll	Библиотека поддержки обмена сообщениями в формате макетов ЦДУ
..\server\format\xml\xml_mod.dll	Библиотека поддержки обмена сообщениями в формате XML
..\server\transport\	Набор библиотек, реализующих обмен сообщениями посредством определенного транспорта
..\server\transport\email\email.dll	Библиотека, реализующая обмен сообщениями по e-mail
..\server\transport\soap\soap.dll	Библиотека, реализующая обмен сообщениями по прямому соединению (soap)

..\index.html	Файл приглашения к работе с программным комплексом
..\DeviceDescr.htm	Файл приглашения к работе с интерфейсом оборудования
..\ZVKAdmin.htm	Файл приглашения к работе с интерфейсом администратора
..\ZVKUser.htm	Файл приглашения к работе с интерфейсом пользователя.
..\RPUser.htm	Файл приглашения к работе с интерфейсом пользователя.
..\DevDescr.htm	Файл приглашения к работе с интерфейсом пользователя.
..\web.config	Файл конфигурации веб-сервера IIS (требуется только для IIS 7 и выше)
..\logo.gif	Файл приглашения к работе с программным комплексом (изображение)
..\readme.txt	Файл информации о ПК
..\SMSITLoader.cab	Файлы загрузки стартовой страницы выбора интерфейсов
..\Setup [дата] [время].log	Файл протокола, создаваемый при установке экземпляра комплекса.
..\Update [дата] [время].log	Файл протокола, создаваемый при обновлении экземпляра комплекса
tools.dll	Библиотека, используемая при деинсталляции экземпляра комплекса
unins000.dat	Перечень файлов, созданных при установке или обновлении экземпляра (учитывается при деинсталляции экземпляра)
unins000.exe	Деинсталлятор экземпляра комплекса
..\server\client\ClientIntegration.dll	Библиотека клиентской интеграции со смежными системами.
..\server\client\dbalert.wav	Файл звуковых оповещений
..\server\client\majoralert.wav	Файл звуковых оповещений
..\server\client\month_enrg.wav	Файл звуковых оповещений
..\server\client\month_lep_elt.wav	Файл звуковых оповещений
..\server\client\month_rza.wav	Файл звуковых оповещений
..\server\client\month_sdtu.wav	Файл звуковых оповещений
..\server\client\RPUser.exe	Файл звуковых оповещений
..\server\client\year_enrg.wav	Файл звуковых оповещений
..\server\client\year_lep_elt.wav	Файл звуковых оповещений
..\server\client\year_rza.wav	Файл звуковых оповещений
..\server\client\year_sdtu.wav	Файл звуковых оповещений
..\server\Format\RPXML\rp_xml_mod.dll	Библиотека, используемая для формирования сообщений ПК «Планы ремонтов»
..\server\AnyDacMsSql.sms	Библиотека, реализующая взаимодействие сервера приложений с MS SQL
..\server\CharsetRecoder.sms	Библиотека, реализующая логику работы ПК
..\server\CheckSettings.sms	Библиотека, реализующая логику работы ПК
..\server\ClientUpdater.sms	Библиотека, реализующая логику работы ПК
..\server\DbErrorLocalizeSupport.sms	Библиотека, реализующая логику работы ПК
..\server\DbProvider.sms	Библиотека, реализующая логику работы ПК
..\server\DBSessionManager.sms	Библиотека, реализующая логику работы ПК

..\server\DocLockManager.sms	Библиотека, реализующая логику работы ПК
..\server\EnumService.sms	Библиотека, реализующая логику работы ПК
..\server\EventAggregator.sms	Библиотека, реализующая логику работы ПК
..\server\EventHandler.sms	Библиотека, реализующая логику работы ПК
..\server\HistoryLogger.sms	Библиотека, реализующая логику работы ПК
..\server\Integration.sms	Библиотека, реализующая логику работы ПК
..\server\kernel.sms	Библиотека, реализующая логику работы ПК
..\server\libeay32.dll	Библиотека, реализующая работу с SSL
..\server\Listener.sms	Библиотека, реализующая логику работы ПК
..\server\MessageDispatcher.sms	Библиотека, реализующая логику работы ПК
..\server\MsSqlSupport.sms	Библиотека, реализующая логику работы ПК
..\server\PermanentStorage.sms	Библиотека, реализующая логику работы ПК
..\server\Permissions.sms	Библиотека, реализующая логику работы ПК
..\server\ReadinessHelper.ini	Конфигурационный файл библиотеки интеграции с ПАК Готовность (наличие необязательно).
..\server\ReadinessRpHelper.sms	Библиотека, реализующая интеграцию с ПАК Готовность (наличие необязательно).
..\server\ReadinessZvkHelper.sms	Библиотека, реализующая интеграцию с ПАК Готовность (наличие необязательно).
..\server\ReservedModulesLoader.sms	Библиотека, реализующая логику работы ПК
..\server\Roles.sms	Библиотека, реализующая логику работы ПК
..\server\RP.sms	Библиотека, реализующая логику работы ПК Планы ремонтов
..\server\Rp2Ias.sms	Библиотека, реализующая интеграцию с АС ОБМ (наличие необязательно).
..\server\RPIntegration.sms	Библиотека, реализующая логику работы ПК
..\server\Scheduler.sms	Библиотека, реализующая логику работы ПК
..\server\SessionContext.sms	Библиотека, реализующая логику работы ПК
..\server\SettingsStorage.sms	Библиотека, реализующая логику работы ПК
..\server\ssleay32.dll	Библиотека, реализующая работу с SSL
..\server\StandbyStub.sms	Библиотека, реализующая логику работы ПК
..\server\TaskManager.sms	Библиотека, реализующая логику работы ПК
..\server\TimeService.sms	Библиотека, реализующая логику работы ПК
..\server\Users.sms	Библиотека, реализующая логику работы ПК
..\server\WorkTime.sms	Библиотека, реализующая логику работы ПК
..\server\ZVKLogic.sms	Библиотека, реализующая логику работы ПК
..\auth\web.config	Файл конфигурации веб-сервера IIS (требуется только для IIS 7 и выше)

Приложение 2. Скрипт для штатного останова серверов приложений АСУРЭО

Ниже приведён скрипт для остановки сервера приложений АСУРЭО, а также сервера приложений веб-версии АСУРЭО. В тексте скрипта необходимо заменить переменные, помеченные зелёным, на собственные значения.

server_directory – расположение серверной директории АСУРЭО. По умолчанию /opt/asureo

ASUREO_name – наименование контейнера сервера приложений АСУРЭО. По умолчанию ASUREO.

```
#!/bin/bash
server_directory='/opt/asureo/'
ASUREO_name='ASUREO'
kill -9 $(ps aux | grep 'ZRP.Configurator.Web.dll' | grep -v 'grep' | awk '{print $2}');
kill -9 $(ps aux | grep 'Sms.ZRP.WebApi.dll' | grep -v 'grep' | awk '{print $2}');
kill -9 $(ps aux | grep 'AuthServer.dll' | grep -v 'grep' | awk '{print $2}');
docker exec $ASUREO_name wine cmd /k net stop ZVK_asu;
sleep 10;
docker-compose -f "$server_directory"docker-compose.yml down;
exit;
```