

АСУРЭО

Руководство системного администратора

2026

Содержание

1	НАЗНАЧЕНИЕ РУКОВОДСТВА.....	8
2	ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ	9
3	КОМПОНЕНТЫ СИСТЕМЫ И ИХ НАЗНАЧЕНИЕ	10
4	ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ	15
4.1	Серверная часть.....	15
4.1.1	Серверная часть с абонентами	15
4.2	Клиентская часть	16
5	ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	18
5.1	Сервер приложений и баз данных.....	18
5.2	Почтовый сервер	19
5.3	Рабочие станции	19
5.4	Настройки браузера Яндекс и политик безопасности для него.....	21
5.4.1	Запросы на отправку	21
5.4.2	Настройка размера шрифта в браузере.....	21
5.4.3	Настройка браузера для печати	22
5.4.4	Настройка работы через прокси-сервер	23
5.4.5	Настройка доверенных сайтов	24
5.4.6	Установка расширения для браузера «Помощник ЗРП.Net».....	25
5.4.7	Особенности отображения уведомлений в ОС Linux.....	29
6	КОМПЛЕКТ ПОСТАВКИ НА ОС СЕМЕЙСТВА LINUX.....	31
7	КОМПЛЕКТ ПОСТАВКИ НА ОС MS WINDOWS	32
8	ПОСЛЕДОВАТЕЛЬНОСТЬ УСТАНОВКИ СИСТЕМЫ НА ОС СЕМЕЙСТВА LINUX.....	33
9	ПОСЛЕДОВАТЕЛЬНОСТЬ УСТАНОВКИ НА ОС MS WINDOWS	35
10	УСТАНОВКА И НАСТРОЙКА СИСТЕМНОГО ПО НА ОС MS WINDOWS.....	36
10.1	Установка и настройка веб-сервера IIS	36
10.1.1	Установка веб-сервера IIS	36
10.1.2	Дополнительные настройки web-сервера IIS.....	37
10.1.3	Рекомендации	38
10.2	Настройка отображения шрифтов	39
10.3	Установка и настройка СУБД на ОС MS Windows	41
10.3.1	Установка СУБД MS SQL на ОС MS Windows	41
10.3.2	Настройка СУБД MS SQL на ОС MS Windows	42
10.3.3	Установка СУБД PostgreSQL на ОС MS Windows	48
10.4	Настройка HTTPS в IIS.....	53
10.4.1	Общая информация	53
10.4.2	Установка и настройка сертификата для IIS 10.x	53
10.4.3	Настройка сайта на веб-сервере IIS для работы с SSL.....	54

10.5	Настройка basic-авторизации для комплекса на ОС MS Windows	56
10.5.1	Общие сведения.....	56
10.5.2	Настройка web-сервера IIS на Windows Server.....	57
10.5.3	Настройка ПК в части basic-авторизации.....	60
10.6	Установка и настройка etcd на ОС MS Windows	60
11	УСТАНОВКА И НАСТРОЙКА СИСТЕМНОГО ПО НА ОС LINUX.....	62
11.1	Установка ОС Astra Linux	62
11.2	Обновление ОС Astra Linux	67
11.3	Установка docker и docker-compose	68
11.4	Настройка прав и доступов для управления СП и docker	68
11.5	Настройка сети docker	69
11.6	Подготовка веб-сервера nginx и настройка конфигурационного файла default.conf.....	71
11.7	Настройка HTTPS для веб-сервера nginx	83
11.8	Настройка basic-авторизации для комплекса на ОС Linux	84
11.8.1	Общие сведения.....	84
11.8.2	Настройка web-сервера nginx на ОС Linux	84
11.8.3	Настройка ПК в части basic-авторизации.....	85
11.9	Настройка basic authentication для защиты SOAP-сервисов в nginx.....	86
11.10	Настройка Kerberos авторизации для Системы.....	88
11.10.1	Общие сведения.....	88
11.10.2	Ввод в домен	88
11.10.3	Настройка доменной авторизации для .Delphi.....	89
11.10.4	Настройка доменной авторизации для веб-версии Системы.....	89
11.10.5	Настройка клиентов для доменной авторизации в веб-версии Системы	90
11.11	Установка и настройка СУБД на ОС семейства Linux.....	91
11.11.1	Установка СУБД на ОС семейства Linux.....	91
11.11.2	Настройка СУБД на ОС семейства Linux.....	95
11.12	Установка etcd на ОС Linux	97
12	УСТАНОВКА И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА СИСТЕМЫ	99
12.1	Создание и настройка БД MS SQL.....	99
12.1.1	Создание базы данных	99
12.1.2	Создание учетной записи пользователя	102
12.1.3	Настройка прав учетной записи пользователя.....	103
12.2	Создание БД PostgreSQL	105
12.2.1	Создание БД с использованием «SQL Shell (psql) в MS Windows»	105
12.2.2	Создание БД с использованием «SQL Shell (psql) в Linux»	106
12.2.3	Создание БД с использованием инструментария PGAdmin	107
12.2.4	Создание учетной записи пользователя в инструментарии PGAdmin.....	108
12.2.5	Настройка прав учетной записи пользователя.....	109

12.3	Установка Системы на СУБД MSSQL/PostgreSQL на ОС Windows.....	110
12.3.1	Выбор производимых действий	112
12.3.2	Выбор дополнительных компонентов	114
12.3.3	Выбор версии веб-сервера	115
12.3.4	Настройка сервера приложений	117
12.3.5	Выбор базы данных	119
12.3.6	Настройка подключения к MSSQL/PostgreSQL	119
12.3.7	Настройка параметров ключа защиты	121
12.3.8	Завершение сбора информации.....	122
12.4	Установка Системы на ОС семейства Linux.....	124
12.5	Настройка Системы с помощью конфигулятора.....	127
12.5.1	Дополнительные настройки	128
12.5.2	Настройка Сервера приложений	129
12.5.3	Настройка Сервера авторизации	135
12.5.4	Настройка Сервера Delphi приложений	138
12.6	Добавление шаблонов отчетов для ЗРП.Net.....	143
12.7	Запуск приложения Системы.....	143
12.8	Обновление на ОС семейства Linux.....	146
12.9	Последовательность действий на клиентах после обновления Системы	152
12.10	Обновление на ОС MS Windows.....	155
12.11	Интеграция с Avanpost FAM	161
12.12	Проверка работоспособности ПК после установки	162
12.13	Откат к предыдущей версии ПК	162
12.14	Удаление на ОС MS Windows.....	162
12.15	Удаление на ОС семейства Linux.....	165
13	НАСТРОЙКА КЛИЕНТСКОГО РАБОЧЕГО МЕСТА	167
13.1	Настройка ClickOnce при изменении параметров веб-сервера.....	167
13.1.1	Общие сведения.....	167
13.1.2	Пересборки ClickOnce на MS Windows.....	167
13.1.3	Пересборка ClickOnce на Linux.....	168
13.2	Настройка клиентского рабочего места и установка клиентской части Системы на MS Windows.....	169
13.2.1	Настройка браузера Internet Explorer	169
13.2.2	Запуск приложений через ClickOnce	170
13.2.3	Первый запуск ПК на рабочей станции.....	172
13.2.4	Создание ярлыка интерфейса пользователя на рабочей станции	178
13.2.5	Проверка настроек прокси-сервера перед обновлением клиентской части ПК	181
13.2.6	Обновление клиентской части ПК	182
13.2.7	Хранимые версии	183

13.3	Установка клиентской части Системы на ОС Astra Linux.....	184
13.3.1	Установка клиентской части Системы с самораспаковывающегося архива	190
13.3.2	Размещение самораспаковывающегося архива на веб-сервере IIS.....	194
13.3.3	Размещение самораспаковывающегося архива на веб-сервере nginx.....	195
13.4	Настройка использования Proxy с поддержкой сетевого протокола аутентификации Kerberos.....	196
13.5	Хранение паролей на клиенте.....	196
14	НАБОР ФАЙЛОВ УСТАНОВЛЕННОГО ЭКЗЕМПЛЯРА.....	198
14.1	Описание параметров файла web.config для IIS.....	198
14.2	Описание параметров файла zvz.ini	198
14.3	Описание параметров файла клиентского zvz.ini.....	217
14.4	Описание параметров клиентского файла ZVZUser.DAT	217
14.5	Описание параметров файла sms.ZRP.WebApi.settings.json	219
14.5.1	Настройки базы данных	219
14.5.2	Настройки логирования запросов к базе данных	220
14.5.3	Настройки для подключения	220
14.5.4	Настройка доступа к серверу приложений Delphi_.....	221
14.5.5	Настройки подключения к etcd серверу	222
14.5.6	Настройки кэширования веб-запросов	222
14.5.7	Настройки коммуникации с внешними сервисами	223
14.5.8	Настройка Cross-Origin Resource Sharing	223
14.5.9	Настройки JWT_.....	224
14.5.10	Запланированные задачи	224
14.5.11	Системные настройки	225
14.5.12	Настройки интеграции с SAP	227
14.5.13	Настройки менеджера дополнительно подключаемых функций.....	227
14.5.14	Настройки Swagger.....	228
14.5.15	Настройки лицензирования	228
14.5.16	Настройки сжатия ответов.....	229
14.5.17	Настройка префикса для маршрутизации запросов внутри одного порта	229
14.5.18	Настройка архивирования файлов логирования.....	230
14.5.19	Настройка логирования полных запросов и ответов от клиента к серверу приложений	231
14.6	Описание параметров файла authServer.settings.json сервера авторизации.....	232
14.6.1	Настройки базы данных и подключения	232
14.6.2	Настройки NT авторизации	232
14.6.3	Настройки безопасности.....	234
14.6.4	Настройки клиентов	235
14.6.5	Настройка префикса для маршрутизации запросов внутри одного порта	237
14.6.6	Настройки менеджера дополнительно подключаемых функций.....	238
14.7	Описание параметров файла config.json сервера авторизации	238

14.8	Описание параметров файла Serilogsettings.json	239
14.9	Описание параметров файла appsettings.json	244
14.10	Шифрование пароля в конфигурационных файлах для ЗРП.Net.....	247
14.11	Дополнительные настройки журналирования действий сервера приложений на MS Windows.....	248
15	РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ ПК НА СУБД MS SQL.....	250
15.1	Общие сведения	250
15.2	Создание устройства	250
15.3	Предварительные условия	251
15.4	Последовательность действий по настройке плана обслуживания БД	252
15.5	Настройки процедуры резервного копирования	271
15.6	Восстановление БД.....	271
15.7	Восстановление работы интерфейсов.....	272
16	РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ ПК НА СУБД POSTGRESQL.....	273
16.1	Создание резервной копии базы данных средствами pg_dump на MS Windows	273
16.1.1	Создание bat-файла.....	273
16.1.2	Создание задания планировщика Windows.....	275
16.2	Создание резервной копии базы данных средствами pg_dump на Linux	279
16.2.1	Создание скрипта бэкапирования	279
16.2.2	Создание задачи планировщика cron.....	280
16.3	Создание резервной копии базы данных в инструментарии PGAdmin.....	280
16.4	Восстановление БД из резервной копии средствами pg_restore.....	281
16.5	Восстановление БД из резервной копии в инструментарии PGAdmin.....	282
17	НАСТРОЙКА КАРТЫ МНОГОЭКЗЕМПЛЯРНОЙ КОНФИГУРАЦИИ	287
17.1	Использование карты.....	287
17.2	Создание карты.....	287
17.3	Настройка карты многоэкземплярной конфигурации на сервере	291
18	ЛОГИРОВАНИЕ ПК.....	295
18.1	Удаление старых логов.....	296
19	ЛОГИРОВАНИЕ ЗРП.NET.....	297
19.1	Известные ошибки ЗРП.Net.....	299
20	РЕКОМЕНДАЦИИ ДЛЯ АДМИНИСТРАТОРОВ.....	316
20.1	Рекомендации по обслуживанию сервера.....	316
20.2	Рекомендации по настройке мониторинга docker в Zabbix	316
20.3	Рекомендации по штатному останову серверов приложений.....	318
20.4	Рекомендации по настройке параметра «client_max_body_size».....	319
20.5	Рекомендации по увеличению лимитов по открытым файлам на ОС Linux.....	320
20.6	Рекомендации по работе с Dr.Web	321

20.7	Рекомендации по обновлению PostgreSQL версии 12 до 15	322
20.8	Рекомендации о периодическом ребилдинге индексов в базе ПК	322
20.8.1	Ребилдинг индексов в SQL Server	322
20.8.2	Ребилдинг индексов в PostgreSQL	331
20.9	Рекомендации об усечении лога транзакций в MS SQL Server.....	332
20.10	Рекомендации по обработке ошибок	332
20.10.1	Ошибка при установке ПК	332
20.10.2	Ошибка при обновлении ПК	333
20.10.3	Ошибка при запуске сервера приложений	333
20.10.4	Ошибка при установке соединения с сервером приложений	334
20.10.5	Ошибка при запуске приложения	334
20.10.6	Ошибка при удалении HTTPS	335
20.11	Рекомендации по ограничению объема занимаемой памяти	335
20.12	Рекомендации по работе Atop	336
ПРИЛОЖЕНИЕ 1. НАБОР ФАЙЛОВ УСТАНОВЛЕННОГО ЭКЗЕМПЛЯРА		337
ПРИЛОЖЕНИЕ 2. СКРИПТ ДЛЯ ПЛАНОВОГО ОСТАНОВА СЕРВЕРОВ ПРИЛОЖЕНИЙ СИСТЕМЫ		360
ПРИЛОЖЕНИЕ 3. СКРИПТ ДЛЯ МОНИТОРИНГА РАЗМЕРА КАТАЛОГА DOCKER.....		365

1 Назначение руководства

Данное руководство предназначено для администраторов АСУРЭО (далее – Система).

2 Основные понятия, определения и сокращения

Перечень сокращений и их определений представлен в таблице 1.

Таблица 1 – Основные сокращения и определения

Понятие/ сокращение	Определение
АСУРЭО	Автоматизированная система управления ремонтами энергетического оборудования
АСУРЭО.Delphi	Сервер приложений, разработанный в среде разработки Delphi для работы в ОС Windows, использующий в своей работе толстый клиент Win32-приложение
АСУРЭО.Net	Разрабатываемый новый кроссплатформенный сервер приложений, использующий тонкий web-клиент. Поставляется при наличии соответствующих лицензий
БД	База данных
ОС	Операционная система
ПК	Программный комплекс
РПОФ	Резервное помещение ограниченной функциональности
СП	Сервер приложения
СУБД	Система управления базами данных
VIP	Виртуальный IP-адрес

3 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 3.1):

- хранилище данных;
- серверы 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. В зависимости от платформы сервер приложений Системы может представлять собой службу Windows, либо же docker-контейнер для ОС семейства Linux. Доступ возможен по прямому TCP / IP соединению или через Web-сервер. В качестве хранилища данных могут использоваться СУБД Microsoft SQL Server и PostgreSQL. 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 Системе 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.

При работе с веб-версией Системы также используется клиент-серверная инфраструктура, при этом работа клиентов осуществляется через браузер по HTTPS-протоколу.

Curl — предустановленный в контейнере ztrnet пакет. Утилита командной строки предназначена для передачи данных по протоколам HTTP, HTTPS, FTP, SFTP и другим. Используется для отладки сетевых взаимодействий, проверки доступности внешних сервисов, выполнения запросов к API, загрузки файлов и автоматизации задач администрирования через сценарии оболочки.

На рисунке 3.2 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.

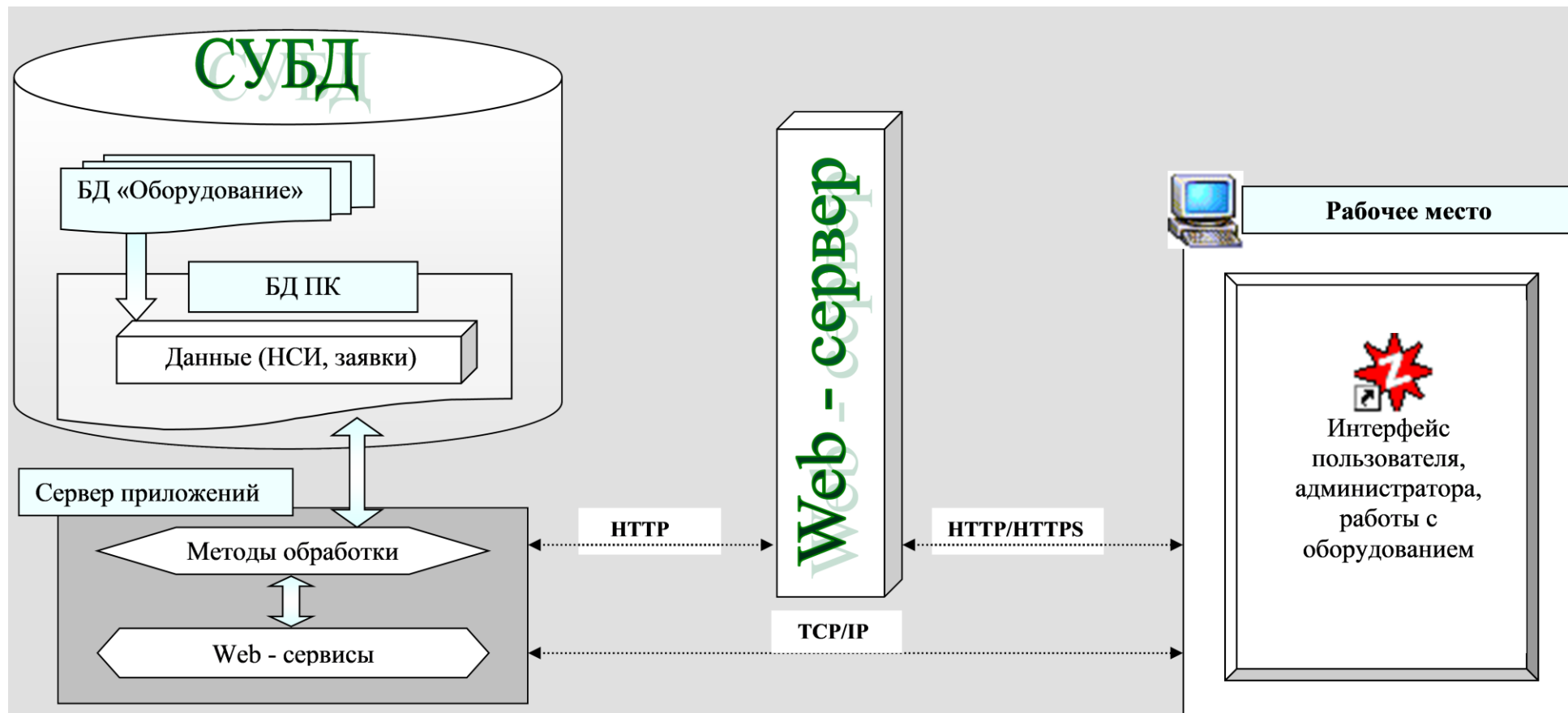


Рисунок 3.1 – Компоненты ПК

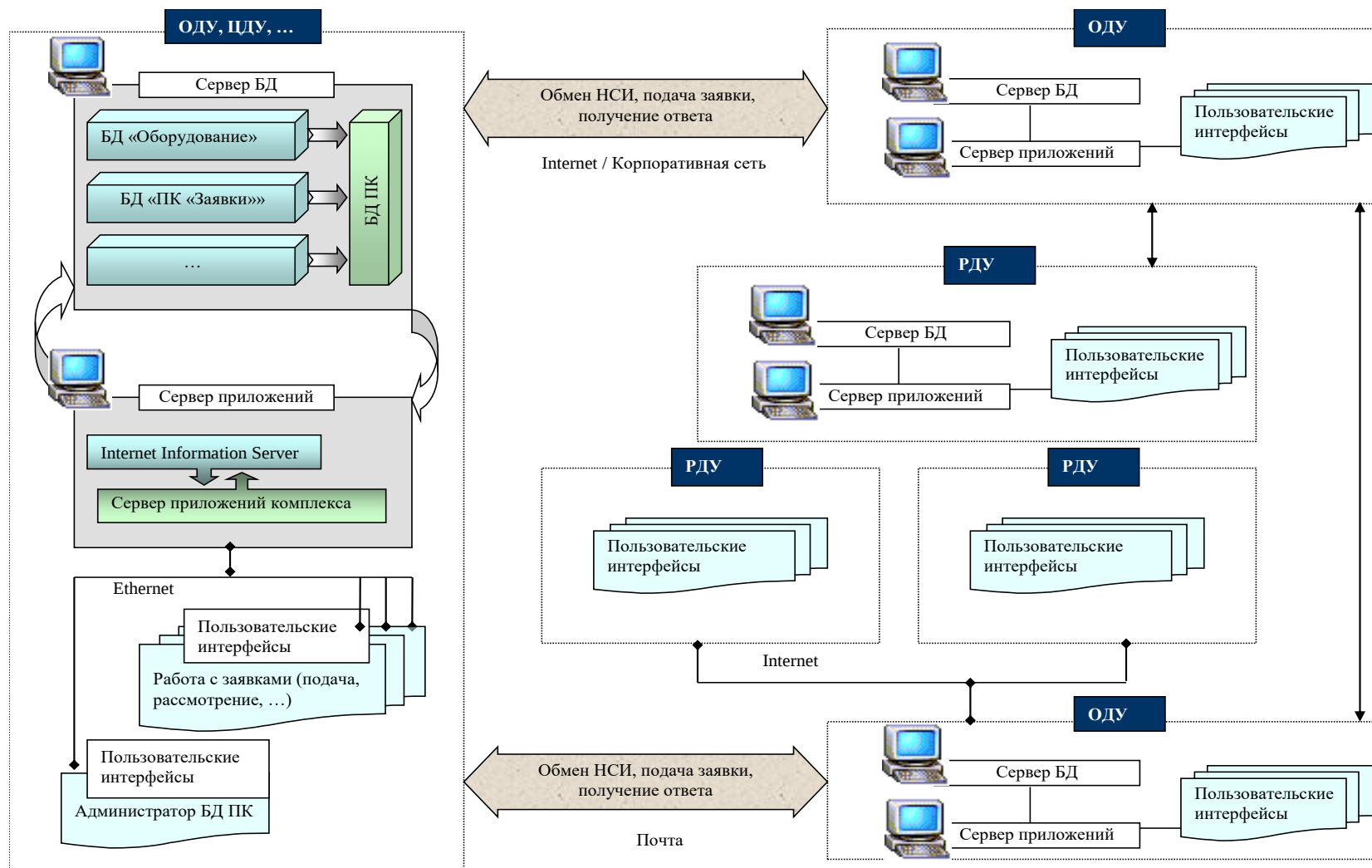


Рисунок 3.2 – Схема взаимодействия составных частей ПК

4 Требования к аппаратному обеспечению

4.1 Серверная часть

Для функционирования приложения необходимо следующее аппаратное обеспечение сервера приложений и 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);
- Дисковое пространство: не менее 200 Гб;
- Наличие USB порта;
- Наличие сетевой платы Ethernet 1 Гб/с.

- **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);
- Дисковое пространство: 500Гб;
- Наличие USB порта;
- Наличие сетевой платы Ethernet 1 Гб/с.

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

4.1.1 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);
- 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.

4.2 Клиентская часть

Для функционирования приложения необходимо следующее аппаратное обеспечение рабочей станции:

- **Минимальная конфигурация клиентского рабочего места:**

- Процессор: не ниже Intel Core i3;
- Оперативная память не ниже 4 Гб;
- Дисковое пространство: не менее 100 Гб;
- 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 i5 3,3 ГГц;
- Оперативная память не ниже 8 Гб;
- Дисковое пространство: не менее 200 Гб 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.

Для обеспечения стабильной работы Системы необходимо учитывать прямую зависимость качества канала от количества активных пользователей.

Минимальные и рекомендуемые параметры:

-
- **Минимальный порог:** 512 Кбит/с. Данное значение обеспечивает базовую работоспособность при малом количестве пользователей и низкой частоте операций.
 - **Рекомендуемое значение:** от 10 Мбит/с. Эта скорость является стандартом для комфортной работы и позволяет обрабатывать типовые запросы без задержек.

При увеличении штата сотрудников или появлении дополнительных задач (например, обмен тяжелыми файлами, видео-конференции, интеграция с другими сервисами) текущего запаса пропускной способности может не хватить. Просим учитывать, что для масштабирования Системы потребуется пропорциональное расширение канала.

5 Требования к программному обеспечению

5.1 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 8 (требуется только для установки ЗПИ.Net);
- Microsoft .Net Framework:
 - Microsoft .Net Framework версии 3.5.1 – для запуска инсталлятора;
 - Microsoft .Net Framework версии 4.5.1 – для возможности подключения дополнительных модулей;

Примечание. Начиная с версии В9, для обновления Системы 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;
- СУБД Postgres Pro 15;
- docker-compose-v2;
- веб-сервер nginx 1.21.4. Возможна установка в контейнере через образ nginx:alpine.

Внимание!

Поддержка PostgreSQL 13 завершается, и мы рекомендуем перейти на более новую версию - PostgreSQL 15. PostgreSQL 13 не поддерживается с 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 на ОС Windows 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 сервера приложений веб-версии совместно с сервером приложений Delphi.

Поставка Системы осуществляется с помощью файлов docker-образа, которые позволяют развёртывать следующее программное обеспечение:

1. Wine.
2. Сервер приложений Системы.

5.2 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 Системы необходимо установить криптографический пакет OpenSSL.

5.3 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 Системе 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 Системы гарантирована только в веб-версии. Для работы с интерфейсами администратора («Интерфейс оборудования», «Интерфейс администратора») рекомендуется использовать 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 «13.2.1 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 файл необходимо 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 файл необходимо 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. 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 файл необходимо запустить;
- если расширение не установлено, то браузер будет скачивать файл установщика каждый раз при переходе по ссылке экземпляра ПК.

5.4 Настройки браузера Яндекс и политик безопасности для него

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

5.4.1 Запросы на отправку

Для корректной работы уведомлений в Yandex.browser необходимо включить опцию «Показывать запросы на отправку» (Рисунок 5.1).

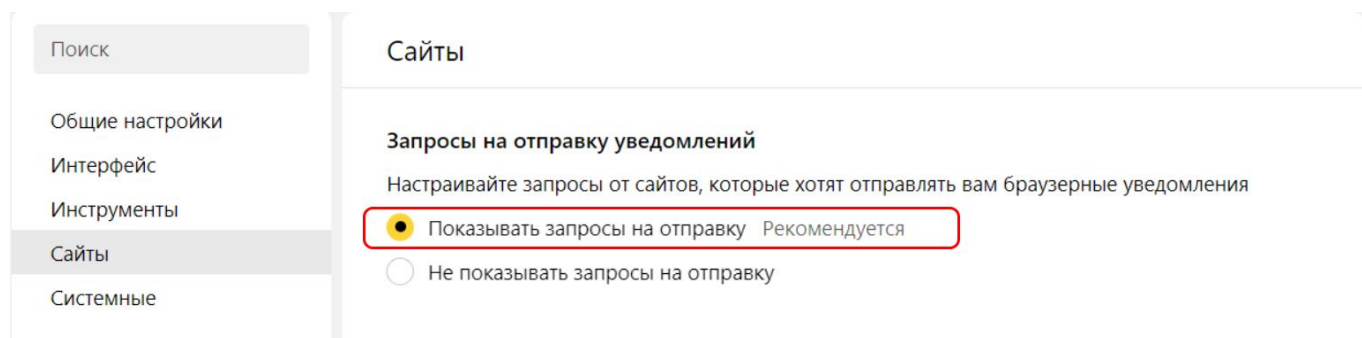


Рисунок 5.1 – Включение опции «Показывать запросы на отправку»

5.4.2 Настройка размера шрифта в браузере

В любом браузере в настройках есть возможность изменения размера шрифта в браузере (Рисунок 5.2).

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

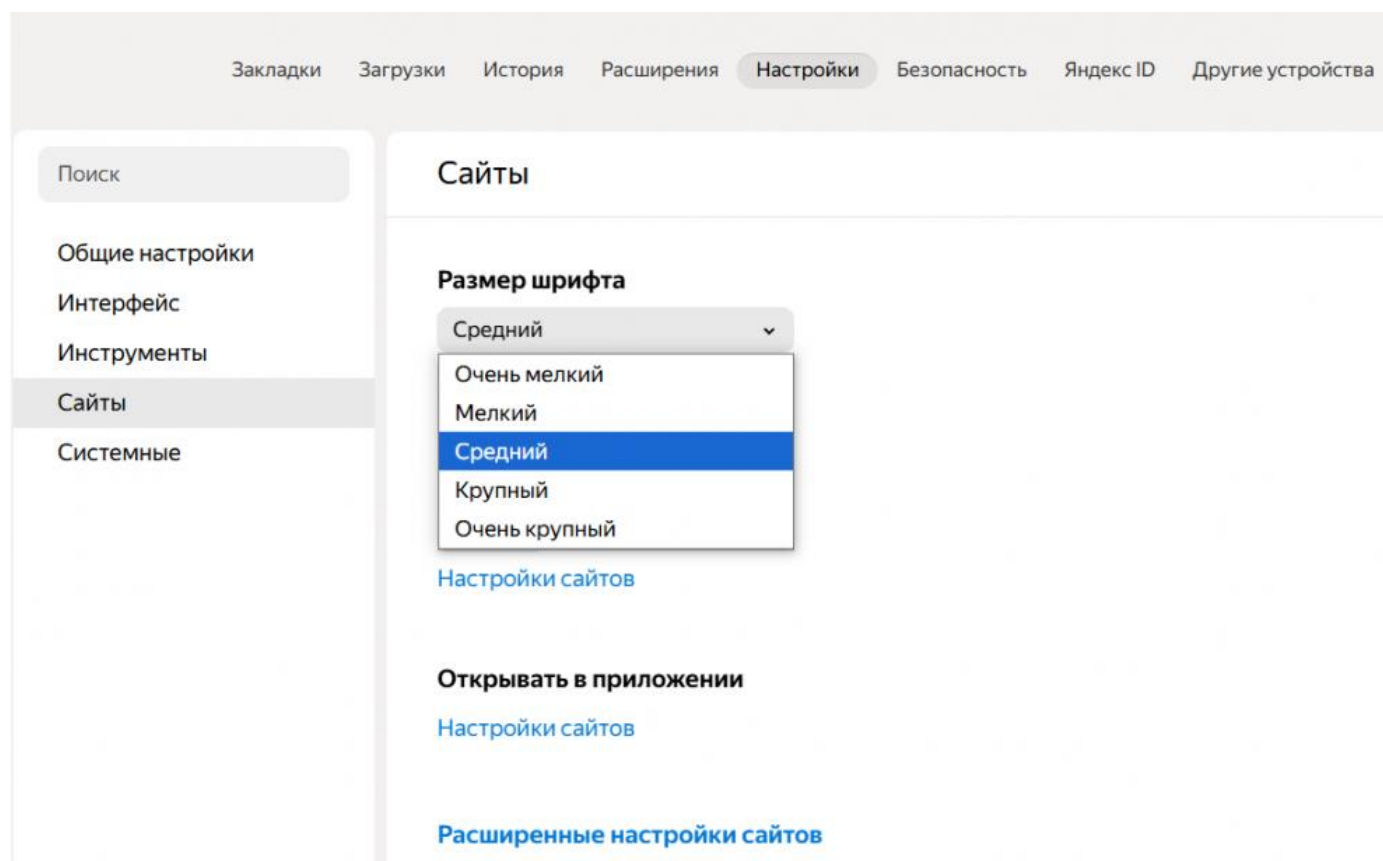


Рисунок 5.2 – Настройка размера шрифта в браузере

5.4.3 Настройка браузера для печати

Для корректной распечатки отчетов в веб-интерфейсе убедитесь, что в настройках вашего браузера включена опция «Открывать в браузере PDF-файлы» (или «Просмотр PDF в браузере») представленная на рисунке 5.3.

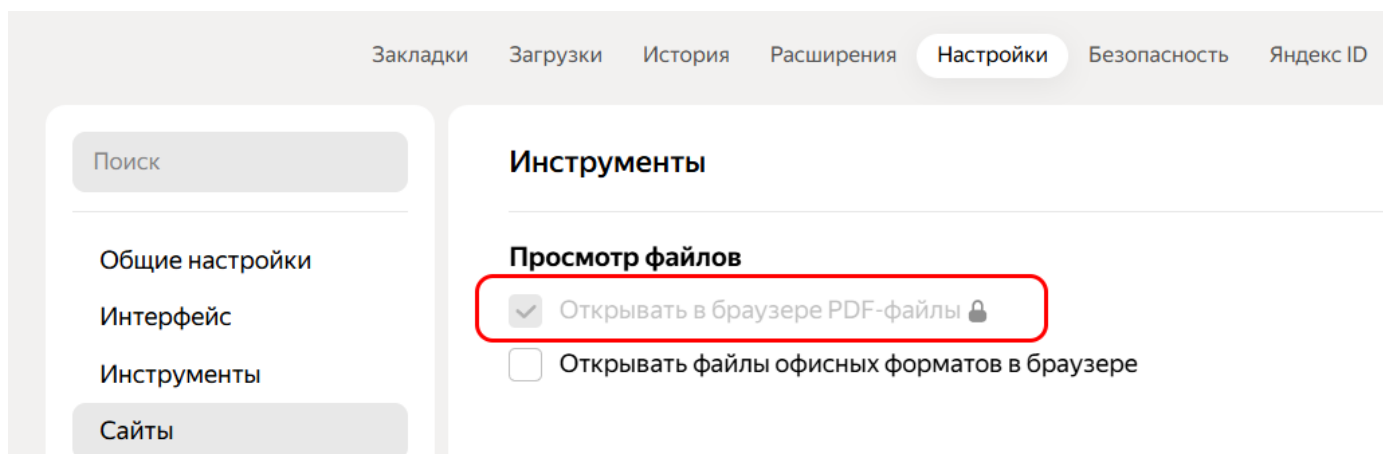


Рисунок 5.3 – Настройка браузера для печати

5.4.4 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 5.4).

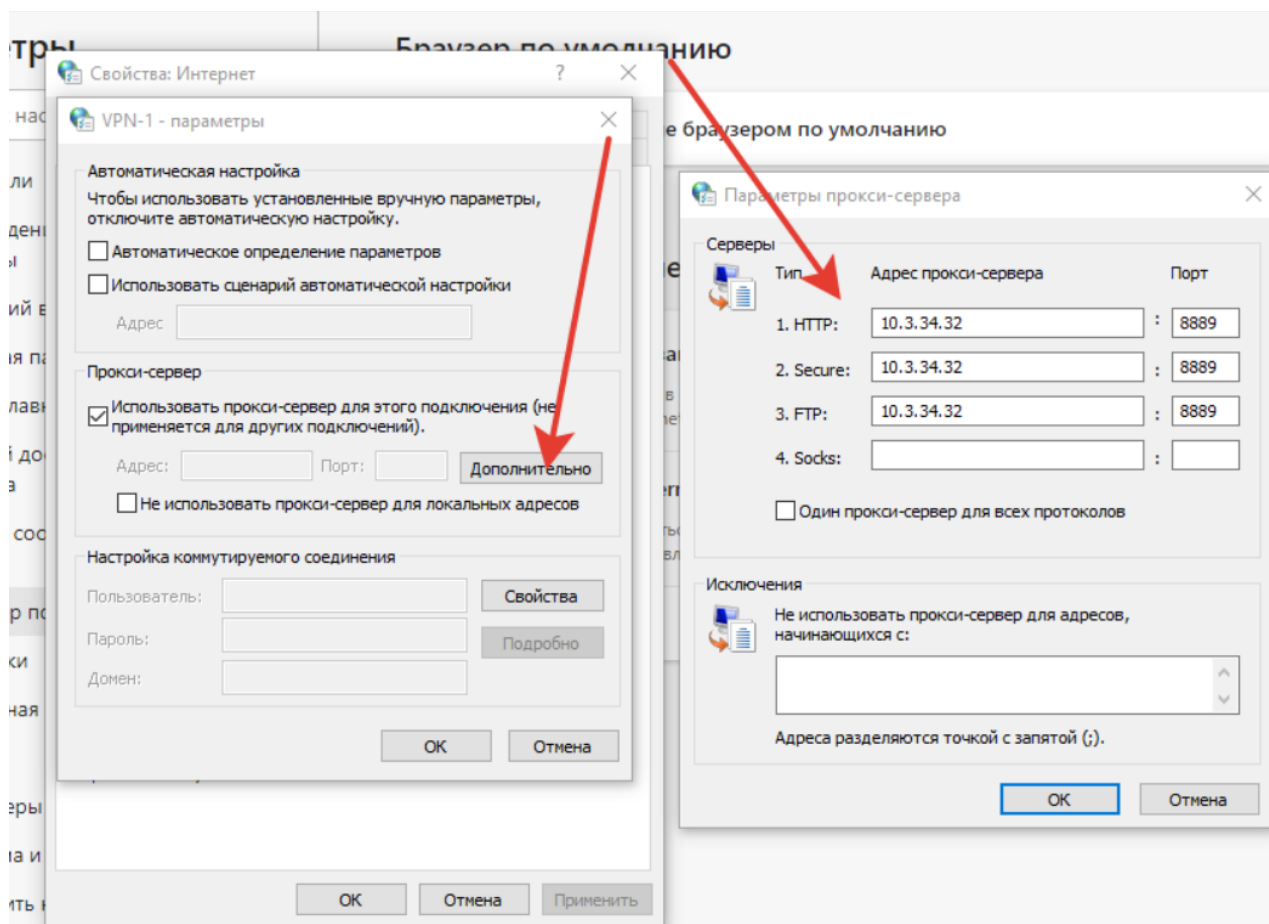


Рисунок 5.4 – Настройки подключений

При этом в системном реестре обязательно эти параметры тоже должны прописаться для каждого протокола в секции ProxyServer (Рисунок 5.5).

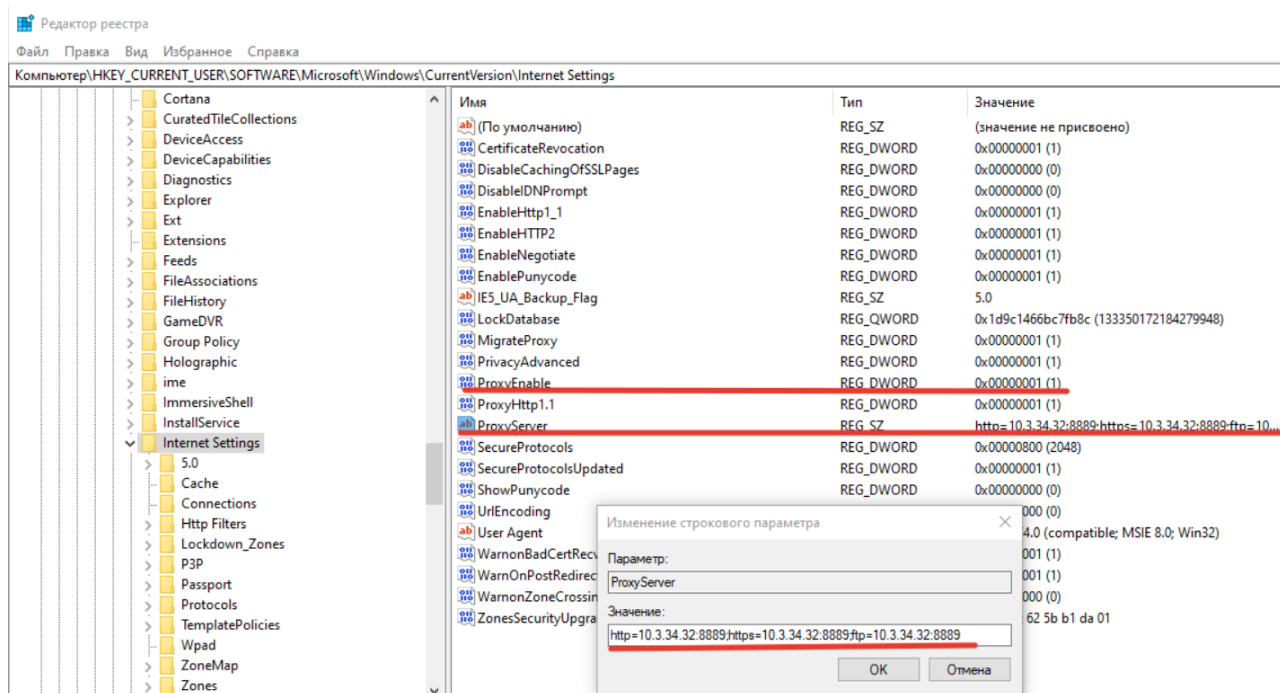


Рисунок 5.5 – Пример системного реестра

5.4.5 Настройка доверенных сайтов

Для того чтобы работала сквозная NT-аутентификация необходимо, чтобы сайты веб-версии Системы 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.

5.4.6 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 mellbkaobpfhbghncnhloeggbmkmckob.
- 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 mellbkaobpfhbghncnhloeggbmkmckob
8. В раздел «ExtensionInstallSources» внесите строковый параметр с указанием url для скачивания, по возможности <all_urls>.

Пример редактора реестра (Рисунок 5.6).

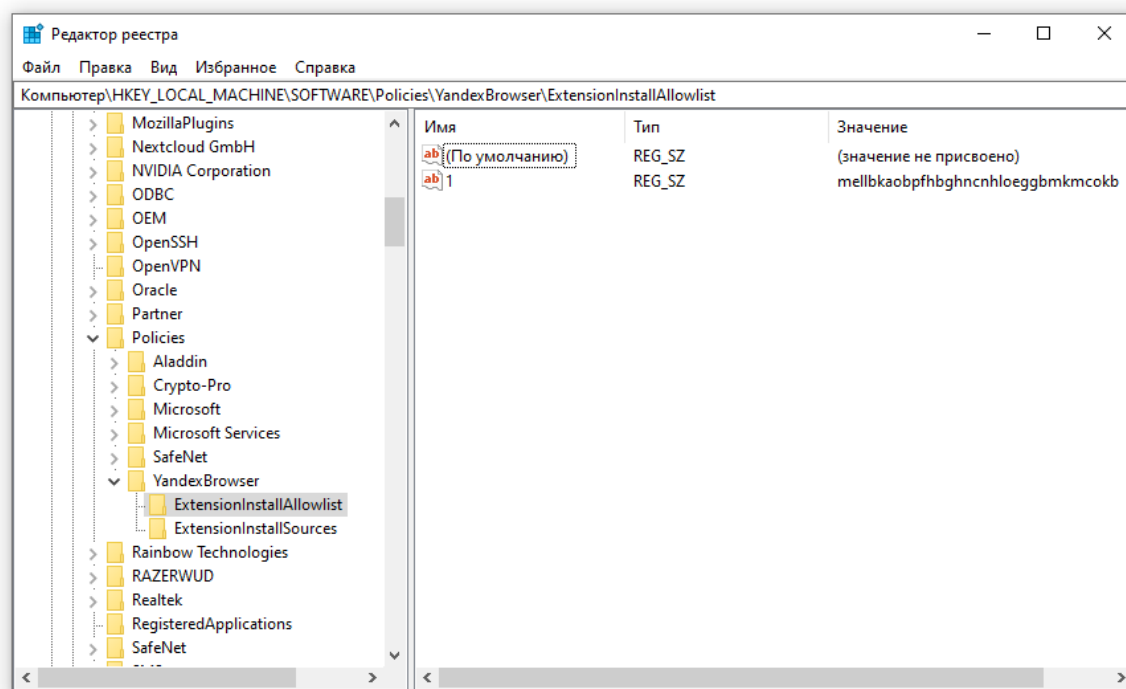


Рисунок 5.6 – Пример редактора реестра

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 5.7).

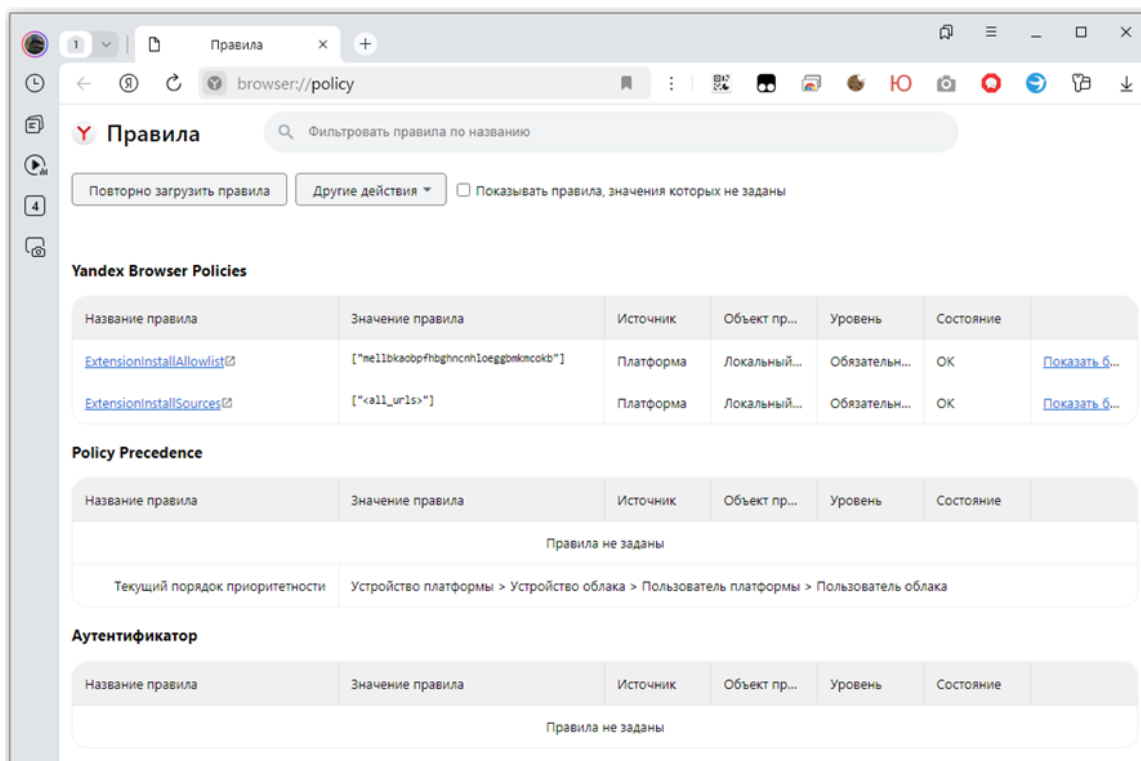


Рисунок 5.7 – Просмотр политик

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/mellbkaobpfhbgfhcnhloeggbmkmckob?hl=ru> (Рисунок 5.8).

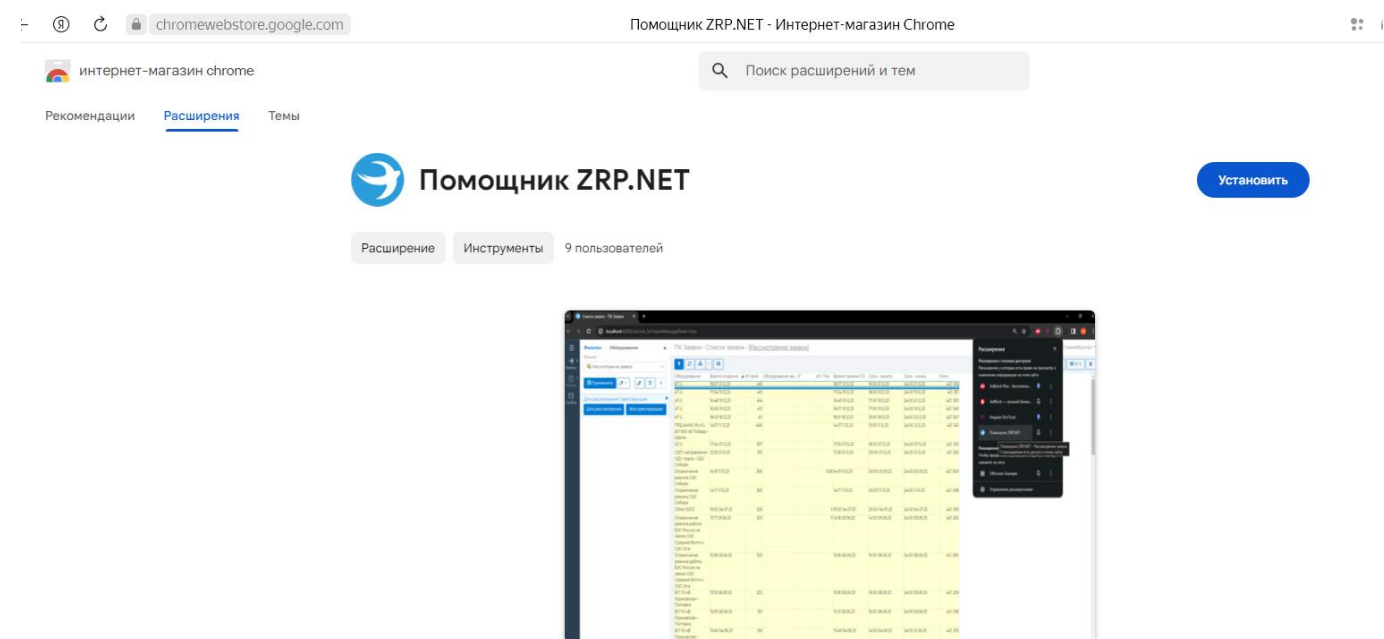


Рисунок 5.8 – Открытие ссылки

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 .сгх, как показано на рисунке 5.9.

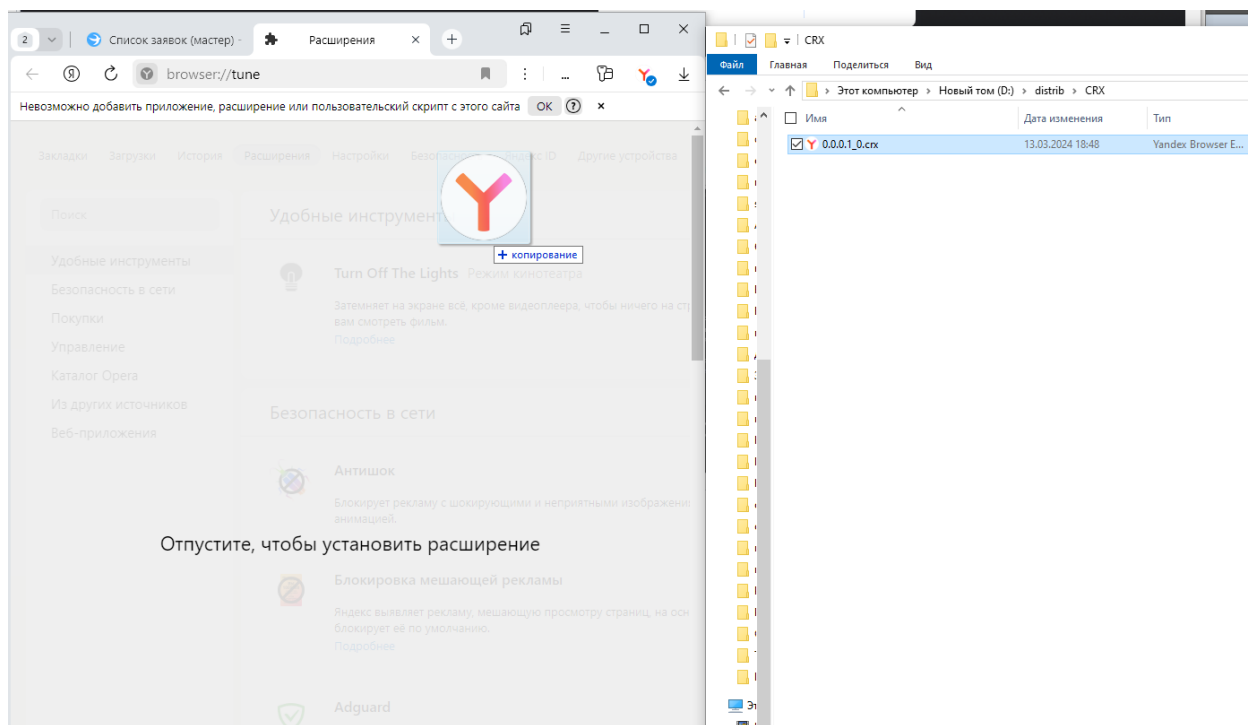


Рисунок 5.9 – Копирование файла .crx

Далее должно появиться окно с предложением установить расширение (Рисунок 5.10).

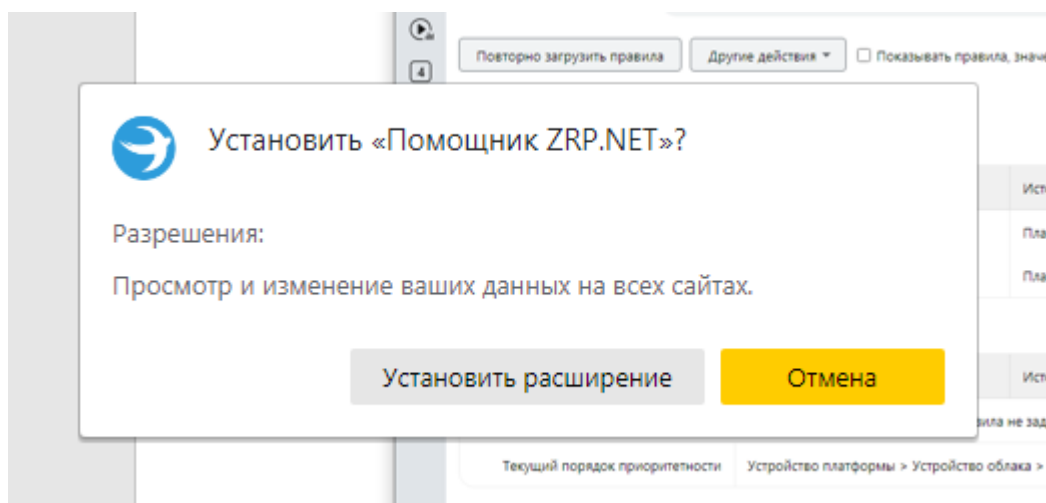


Рисунок 5.10 – Установка «Помощник ZRP.Net»

Необходимо выбрать пункт «Установить расширение». После установки расширения появится уведомление об успешности установки (Рисунок 5.11).

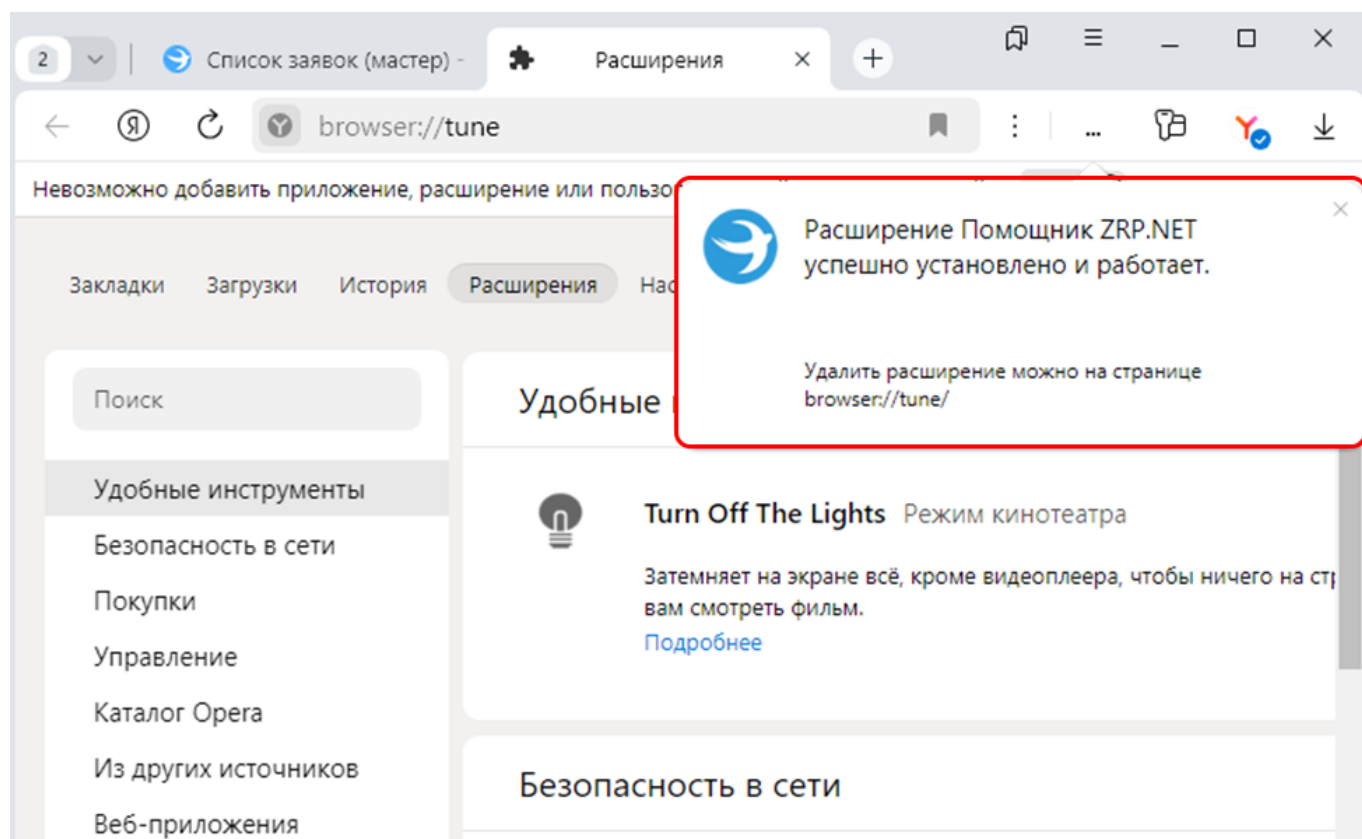


Рисунок 5.11 – Уведомление об успешности установки

Перейти в список расширений браузера по ссылке `browser://tune/` и убедиться, что расширение включено (Рисунок 5.12).

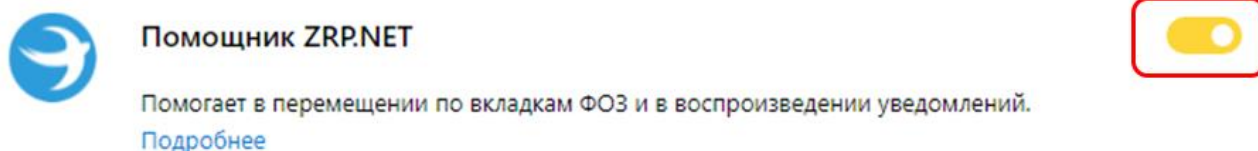


Рисунок 5.12 – Расширение включено

5.4.7 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 5.13).

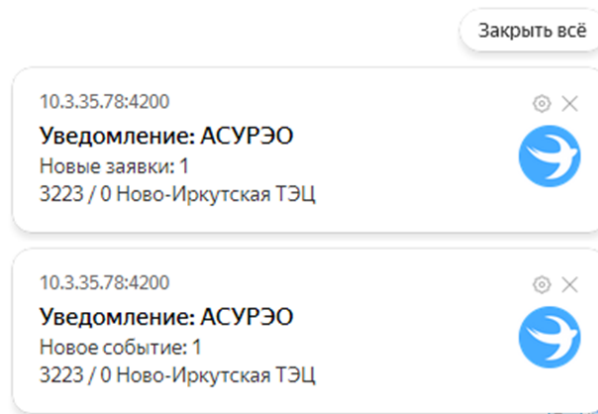


Рисунок 5.13 – Отображение уведомлений в Firefox

- В Chrome и Яндекс сначала отображаются уведомления как на рисунке 5.14, но в какой-то момент начинают отображаться уведомления как на рисунке 5.13.

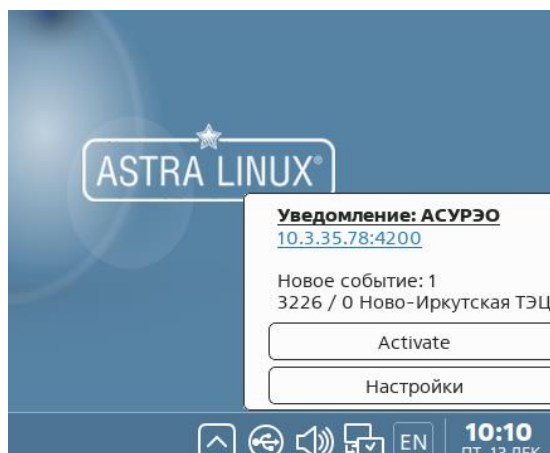


Рисунок 5.14 – Отображение уведомлений в Chrome и Яндекс

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.

6 Комплект поставки на ОС семейства Linux

В комплект поставки программного комплекса на ОС семейства Linux входят:

- файлы docker-образа для создания контейнеров Системы (.Dephi, .Net), включая мигратор базы данных – средство для обновления базы данных Системы, часть инсталлятора Системы, 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
- файл программного ключа zvkkey.lic

7 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.

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).

8 Последовательность установки Системы на ОС семейства Linux

Установку Системы 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.
1. Установка ОС Linux.
 2. Установка docker.
 3. Установка docker-compose.
 4. Создание группы в ОС Linux для управления СП и docker.
 5. Установка web-сервера nginx и настройка конфигурационного файла.
 6. Установка и настройка СУБД Postgres Pro.
 7. Восстановление из дампа БД Системы, создание пользователя, осуществляющего доступ к БД.
 8. Загрузка docker образы Системы.
 9. Настройка конфигурационного файла zvk.ini.
 10. Загрузка docker контейнера web-сервера nginx и настройка конфигурационного файла.
 11. Настройка конфигурационного файла docker-compose.yml.
 12. Запуск контейнеров Системы и web-сервера nginx.

После установки Системы необходимо запустить браузер и перейти на главную страницу.

Для авторизации необходимо использовать имя и пароль настроенной учётной записи в Системе.

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 Последовательность установки на ОС MS Windows

Установку Системы 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 Систему.
4. Проверить работоспособность установленного ПО.

10 Установка и настройка системного ПО на ОС MS Windows

10.1 Установка и настройка веб-сервера IIS

10.1.1 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 с IIS необходимо выполнить следующие действия:

1. Включить роль IIS (Рисунок 10.1).

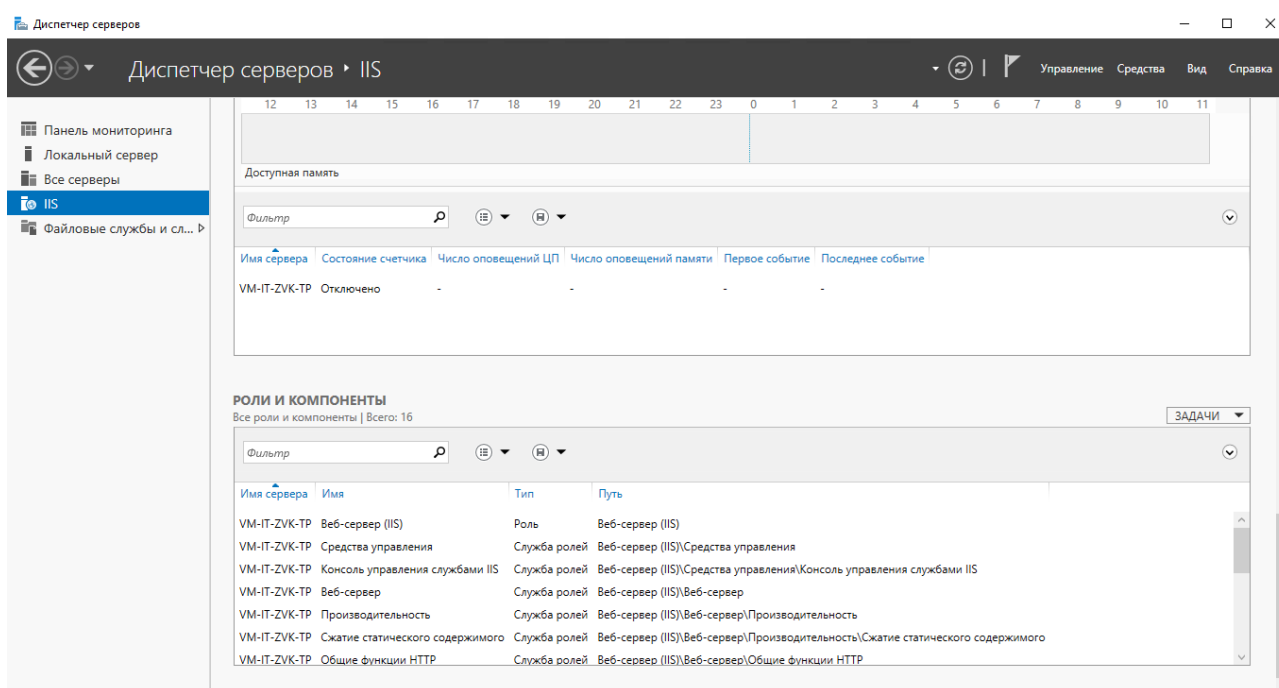


Рисунок 10.1 – Роль Веб-сервер (IIS)

2. Установить службы ролей совместимости с IIS 6 (Рисунок 10.2).

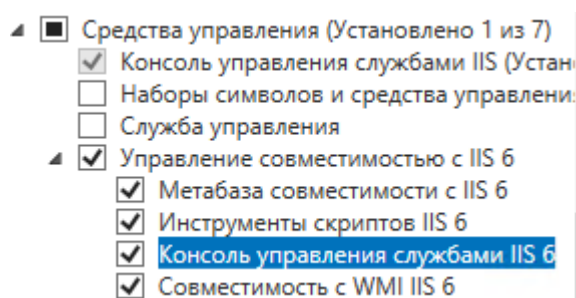


Рисунок 10.2 – Службы ролей совместимости с IIS 6

3. Также установить основные службы ролей (Рисунок 10.3).

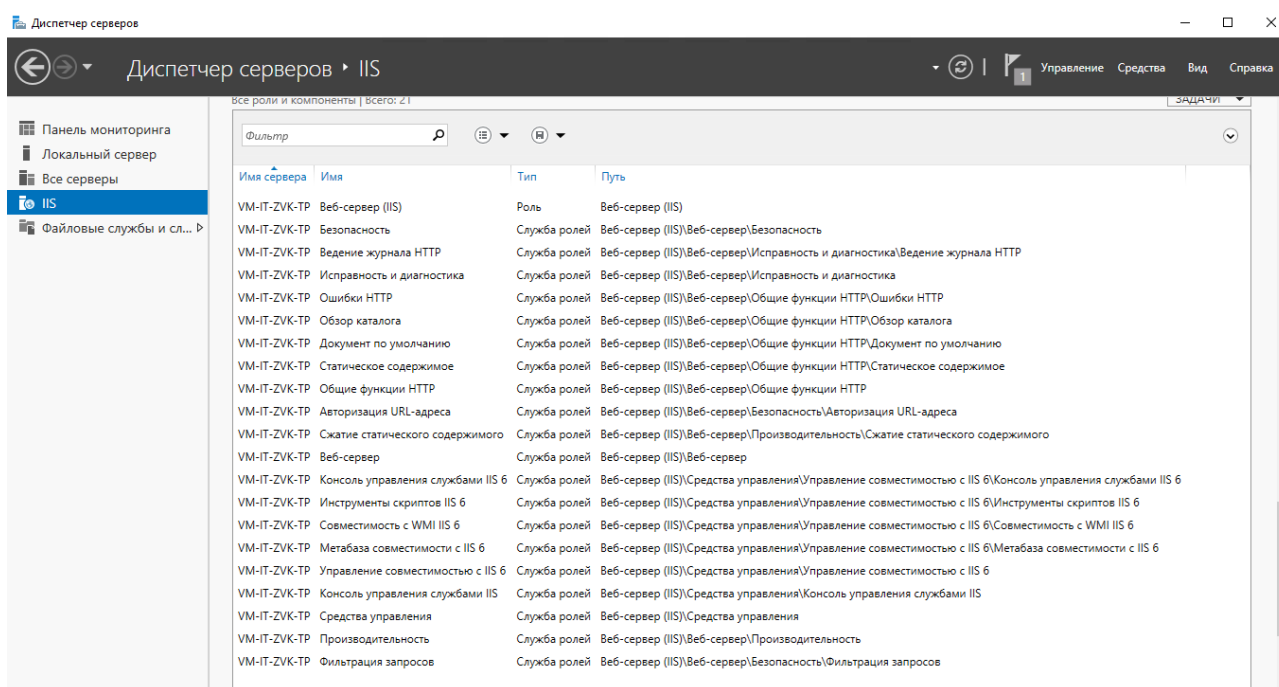


Рисунок 10.3 – Основные службы ролей

10.1.2 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 компонента 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 дополнительного компонента Application Request Routing требуется вручную включить Proxy в Application Request Routing Cache -> Server Proxy Settings -> Enable Proxy (Рисунок 10.4).

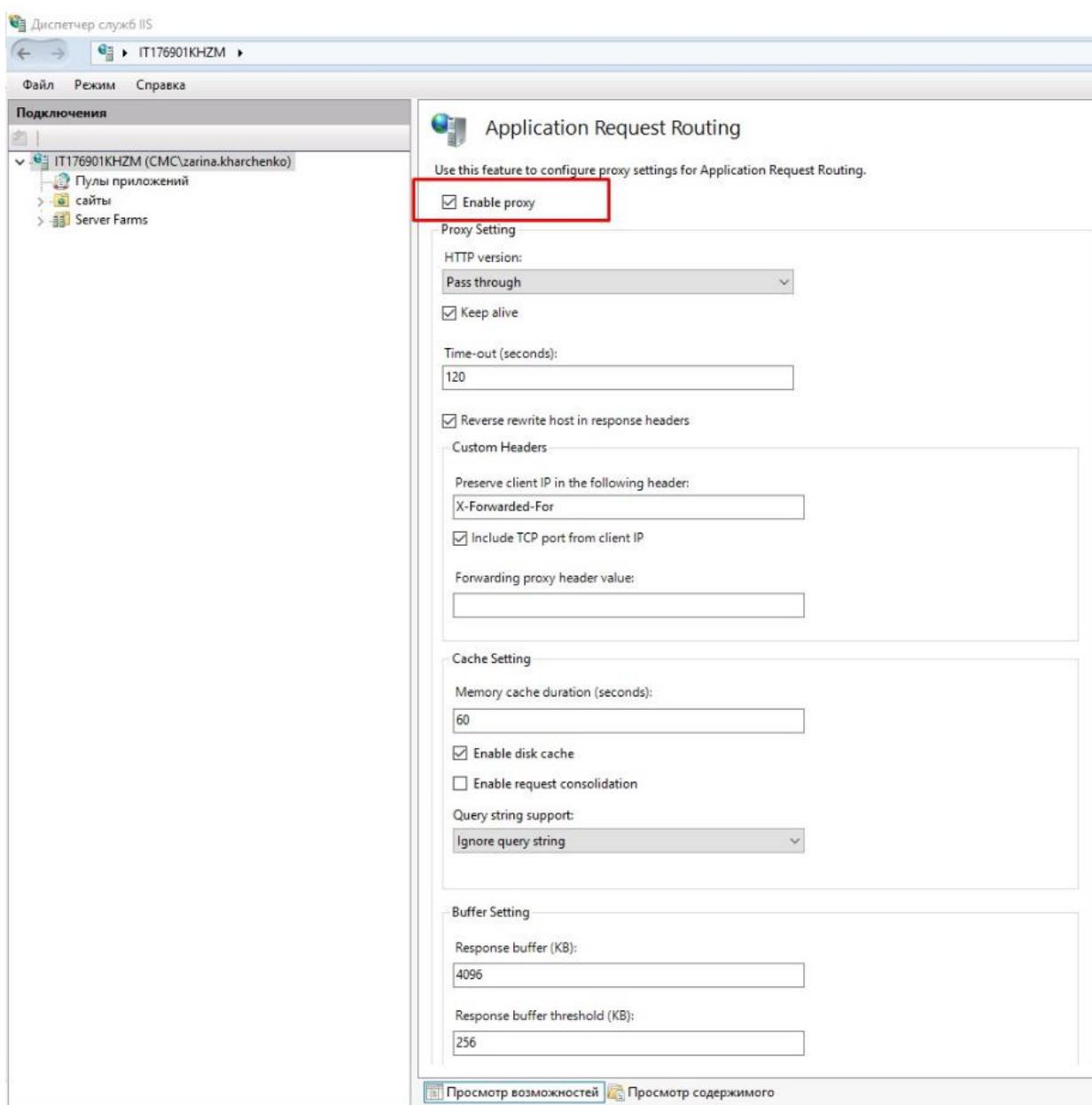


Рисунок 10.4 – Включение дополнительного компонента «Enable Proxy»

10.1.3 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».

10.2 Настройка отображения шрифтов

Для корректного отображения шрифтов в установщике и в клиенте Системы необходимо установить следующие настройки. На панели управления Control Panel необходимо выбрать «Региональные стандарты» (*Regional and Language Options*) (Рисунок 10.5).

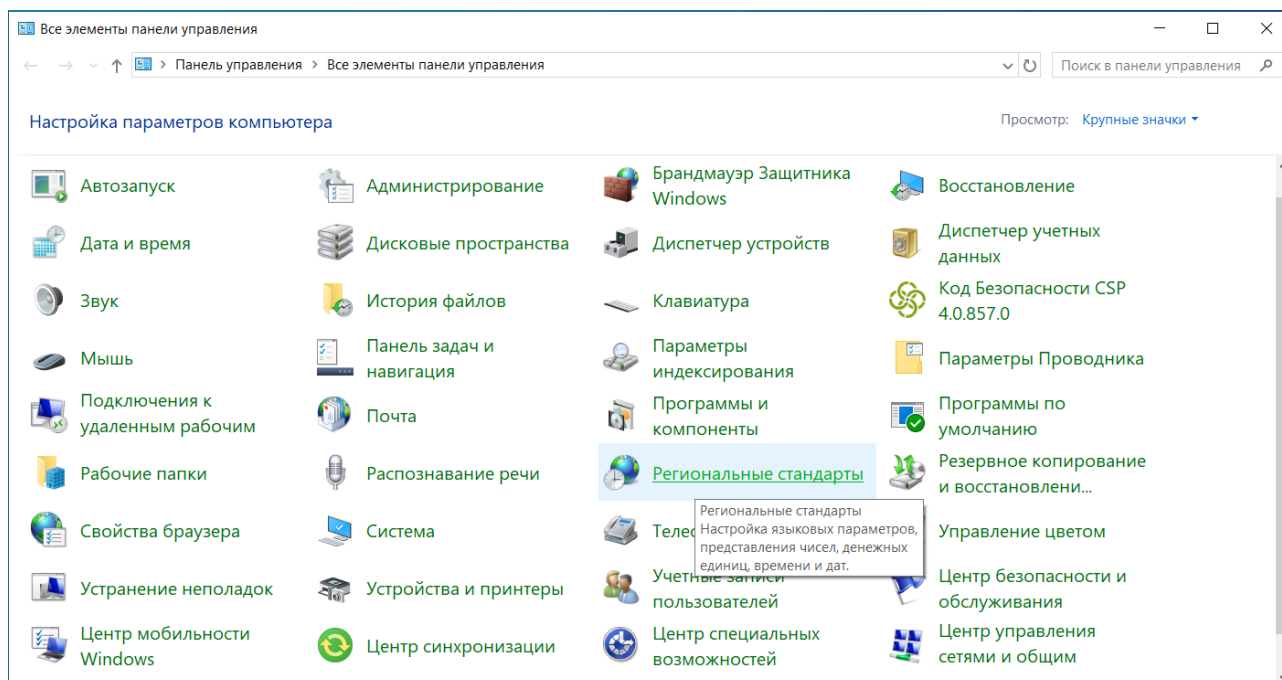


Рисунок 10.5 – Панель управления Control Panel

В окне «Регион» на вкладке «Дополнительно» (Advanced) для настройки «Язык программ, не поддерживающих Юникод» (Language for non-unicode programs) необходимо изменить язык системы на Русский (Russian) (Рисунок 10.6).

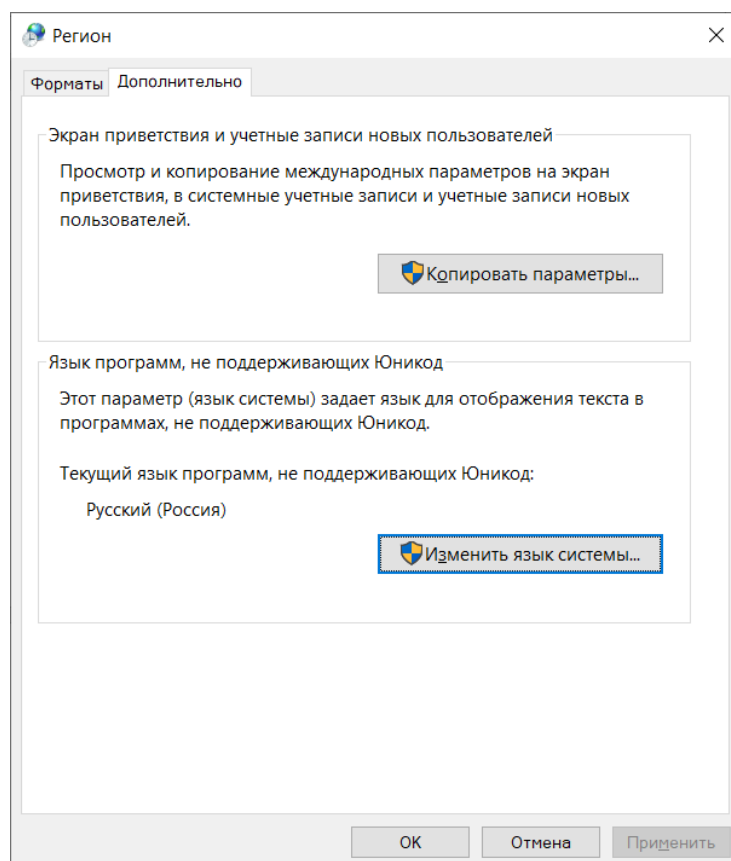


Рисунок 10.6 – Настройка региональных стандартов

Для применения настроек необходимо перезагрузить систему. Для этого в диалоговом окне необходимо нажать на кнопку «Yes» (Рисунок 10.7).

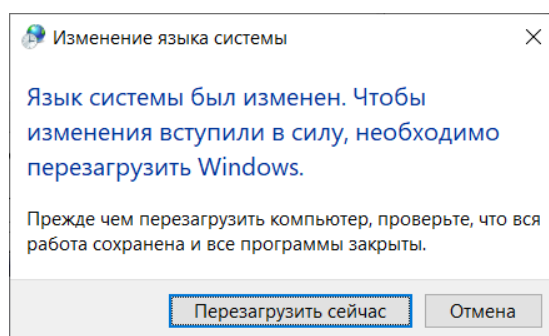


Рисунок 10.7 – Диалоговое окно «Изменение языка системы»

Необходимо в настройке Windows «Регион и язык» в окне «Регион» на вкладке «Форматы» установить значения (Рисунок 10.8):

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

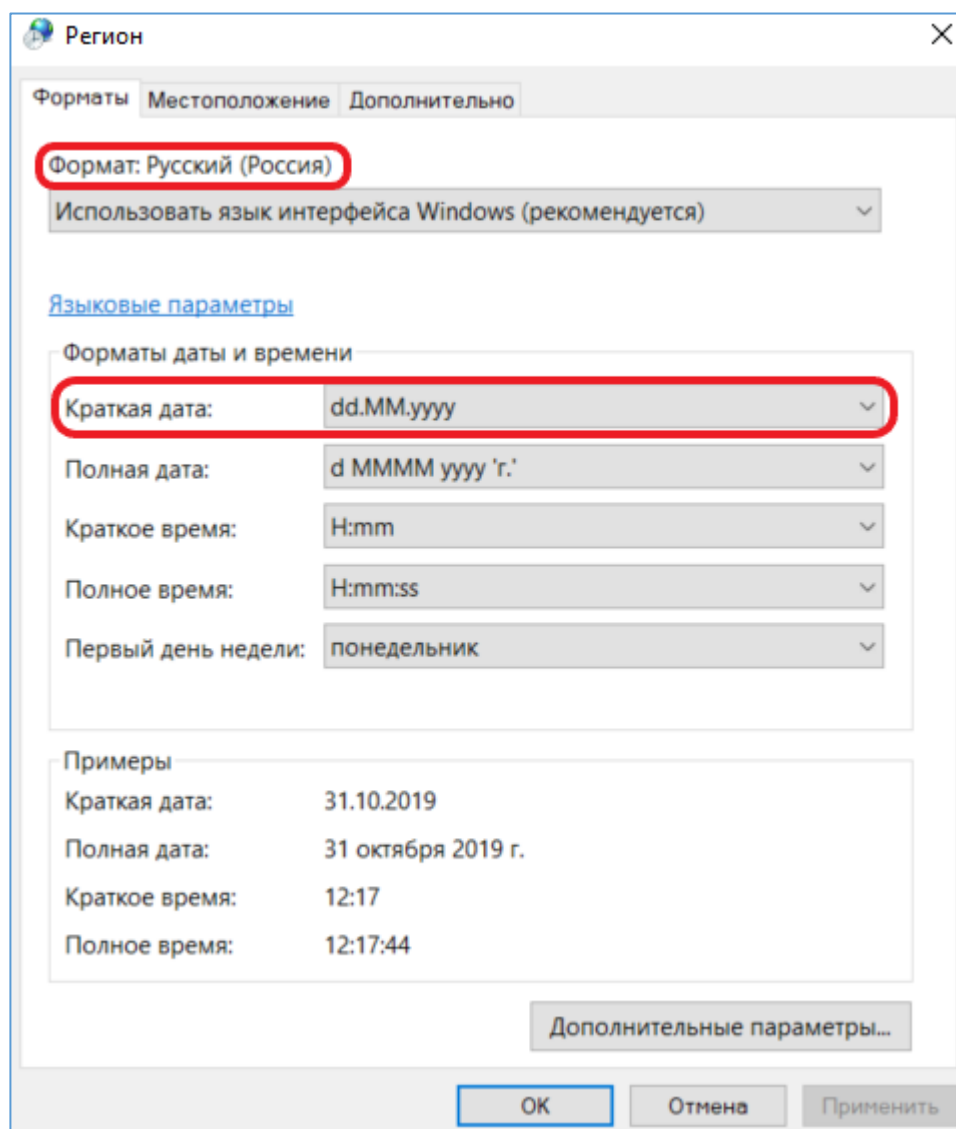


Рисунок 10.8 – Настройка языка и краткой даты

10.3 Установка и настройка СУБД на ОС MS Windows

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

10.3.1 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 10.9);

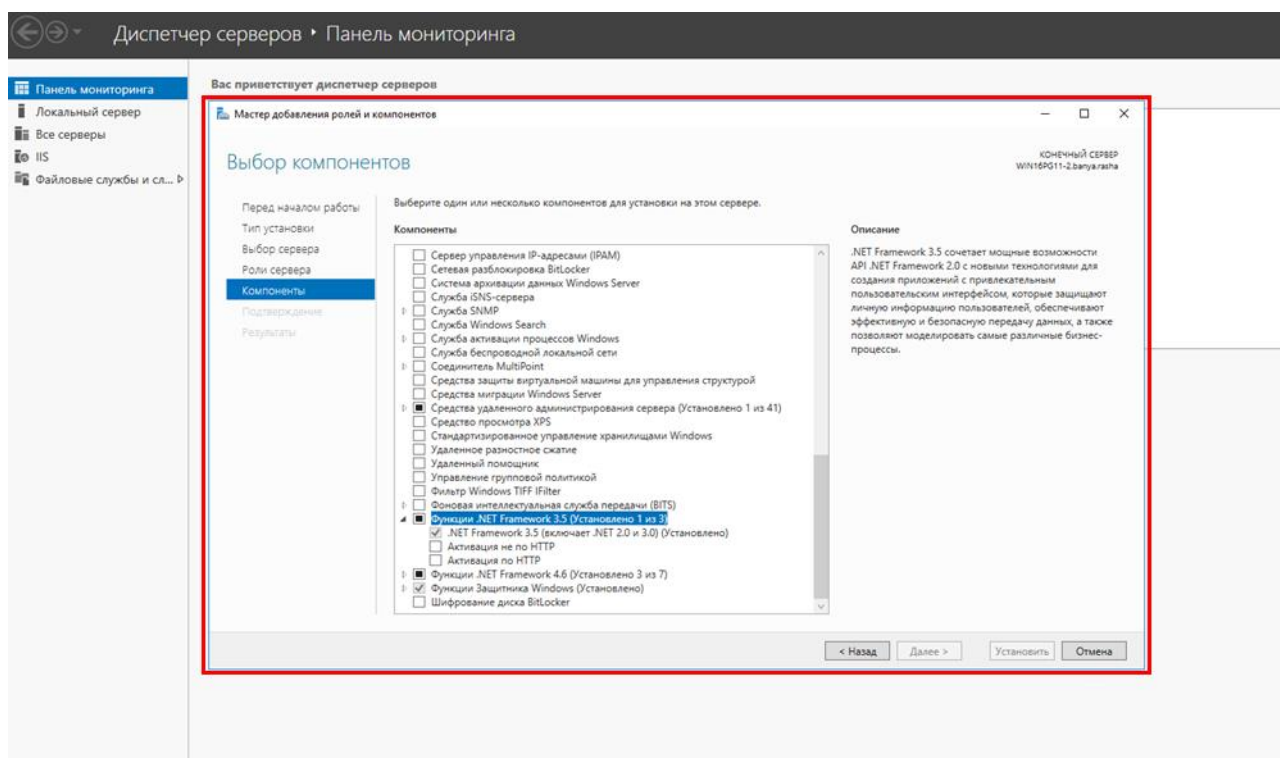


Рисунок 10.9 – Добавление компонента «Функции . Net Framework 3.5»

- 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».

10.3.2 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 10.10).

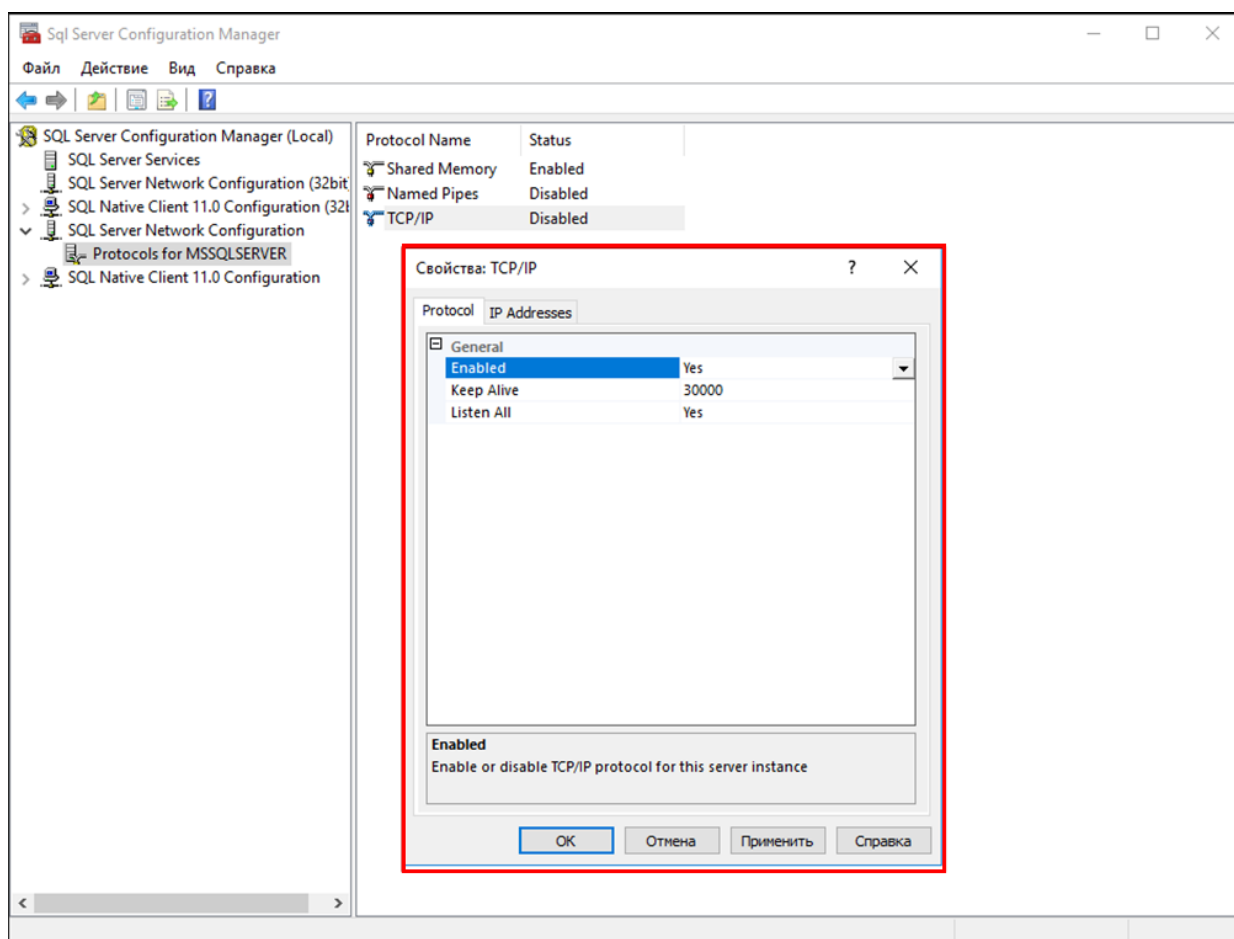


Рисунок 10.10 – Разрешение использования протокола TCP/IP

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 10.11). Если сервер приложений и СУБД MS SQL Server установлены на одном физическом (виртуальном) сервере, то п.3 пропускается.

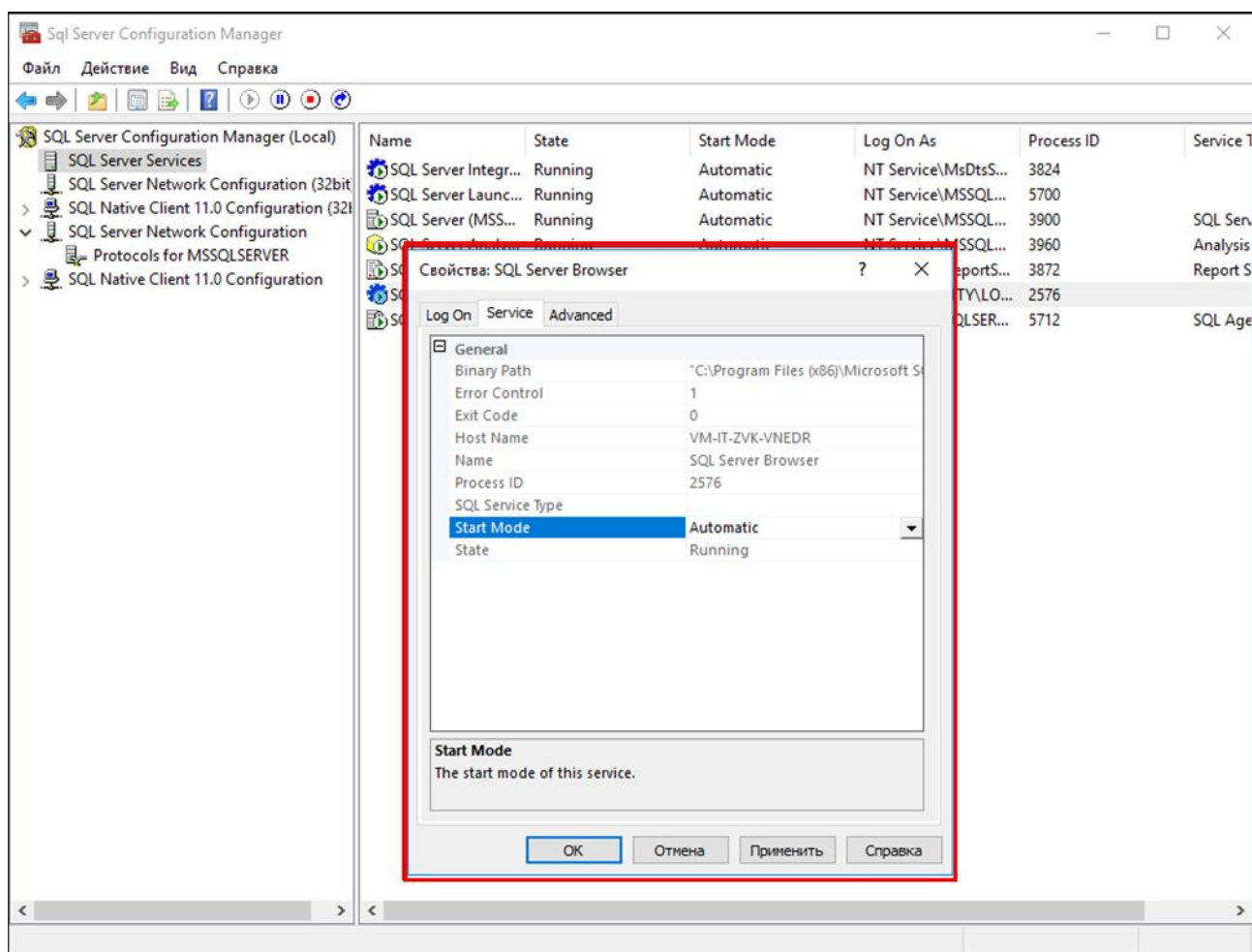


Рисунок 10.11 – Подключение службы «SQL Server Browser»

4. Для запуска службы «SQL Server Browser» перейти на вкладку «Вход» (*Log On*) и нажать на кнопку «Пуск» (*Start*), затем кнопку «OK» (Рисунок 10.12).

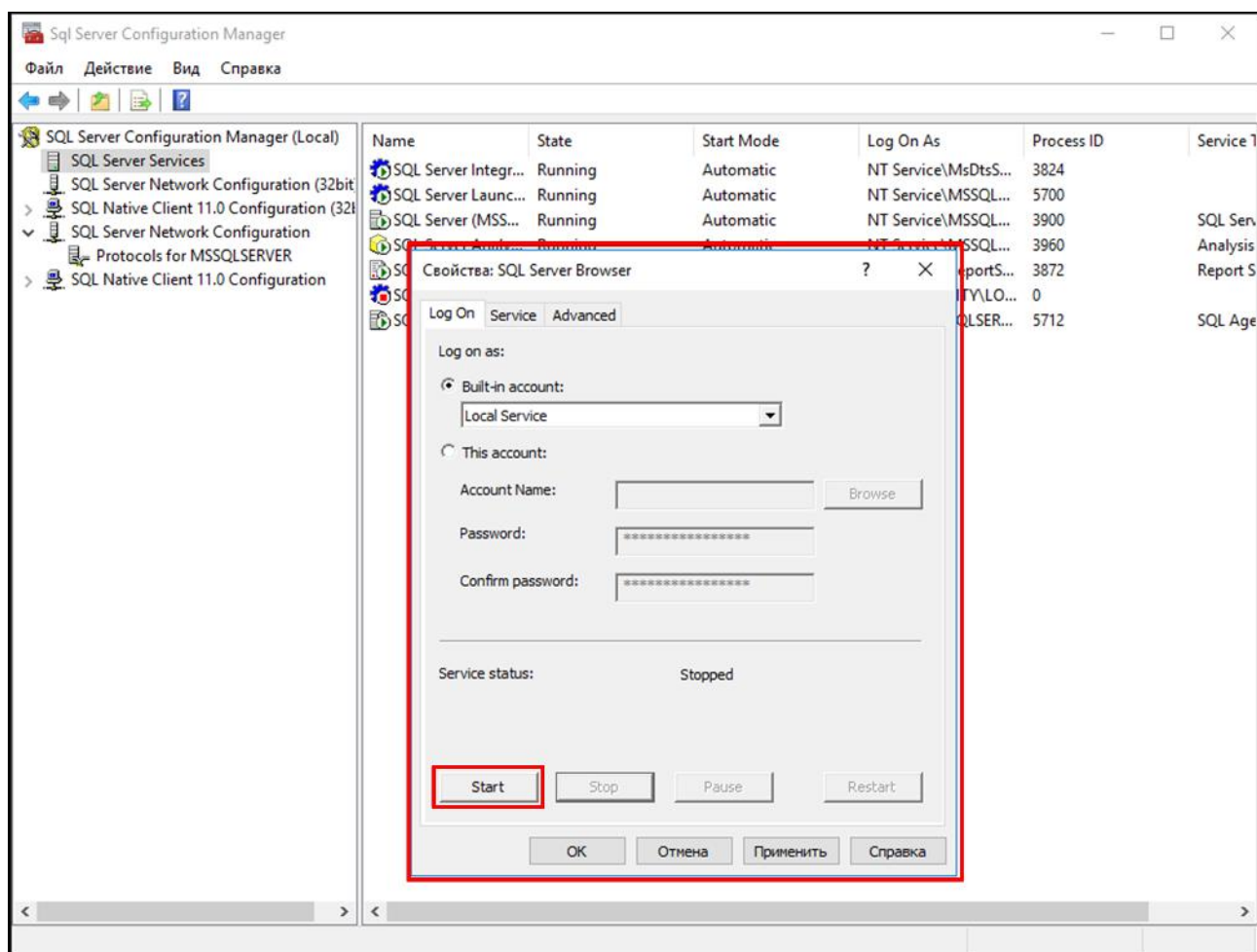


Рисунок 10.12 – Запуск службы «SQL Server Browser»

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 10.13).

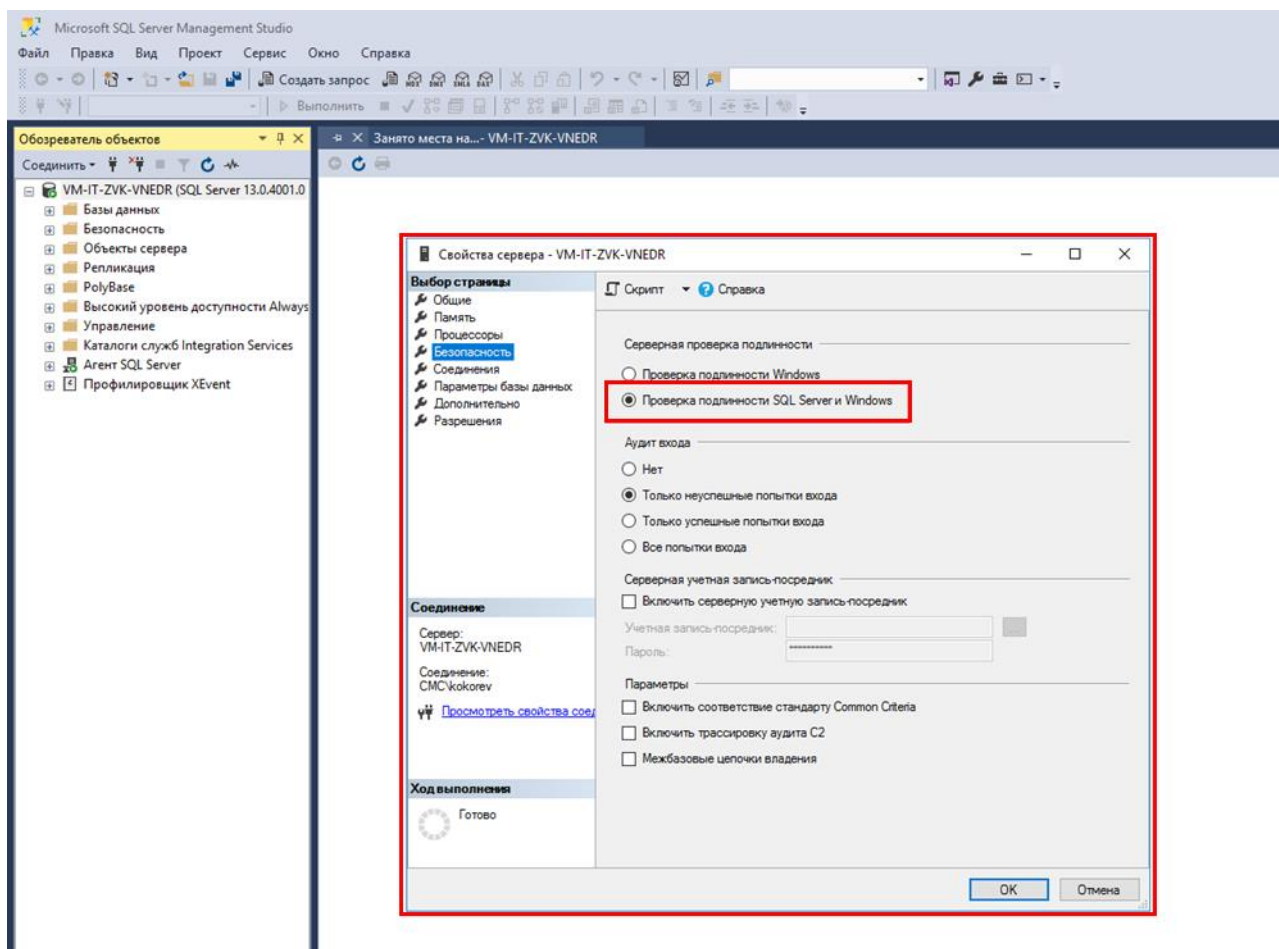


Рисунок 10.13 – Установка разрешения использования проверки подлинности SQL

6. Нажать на кнопку «OK» 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 10.14).

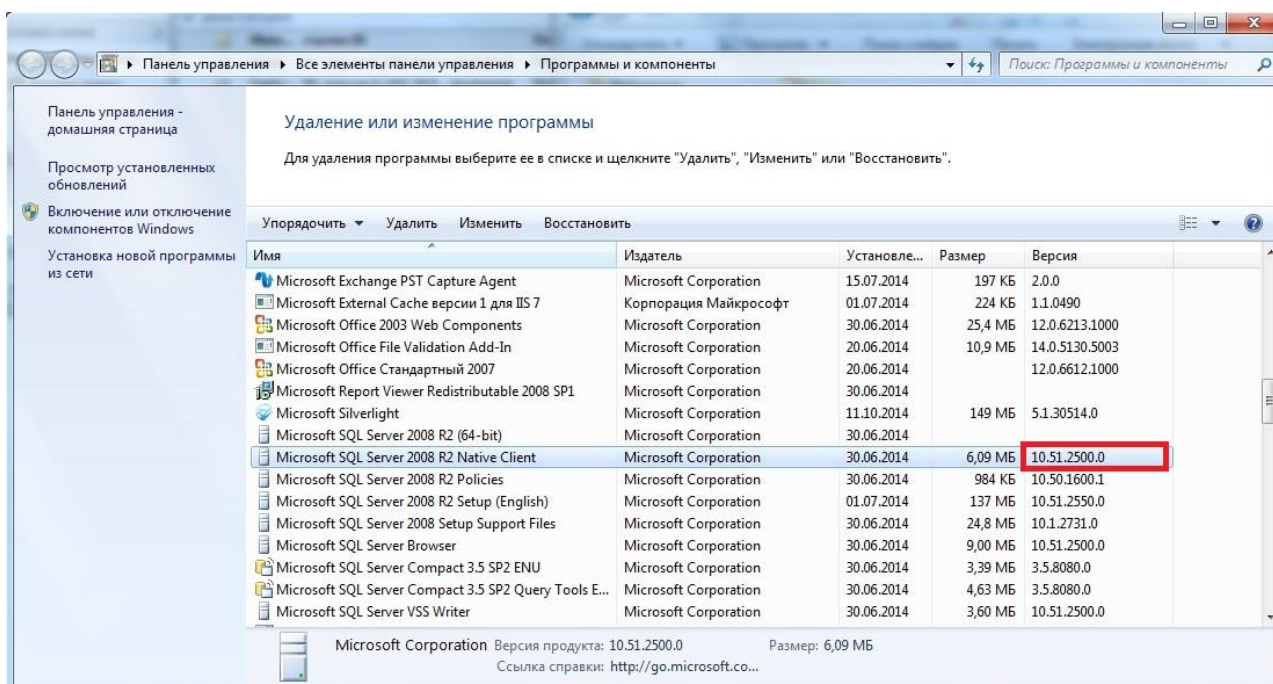


Рисунок 10.14 – Проверка наличия и версионности Native Client

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 10.15).

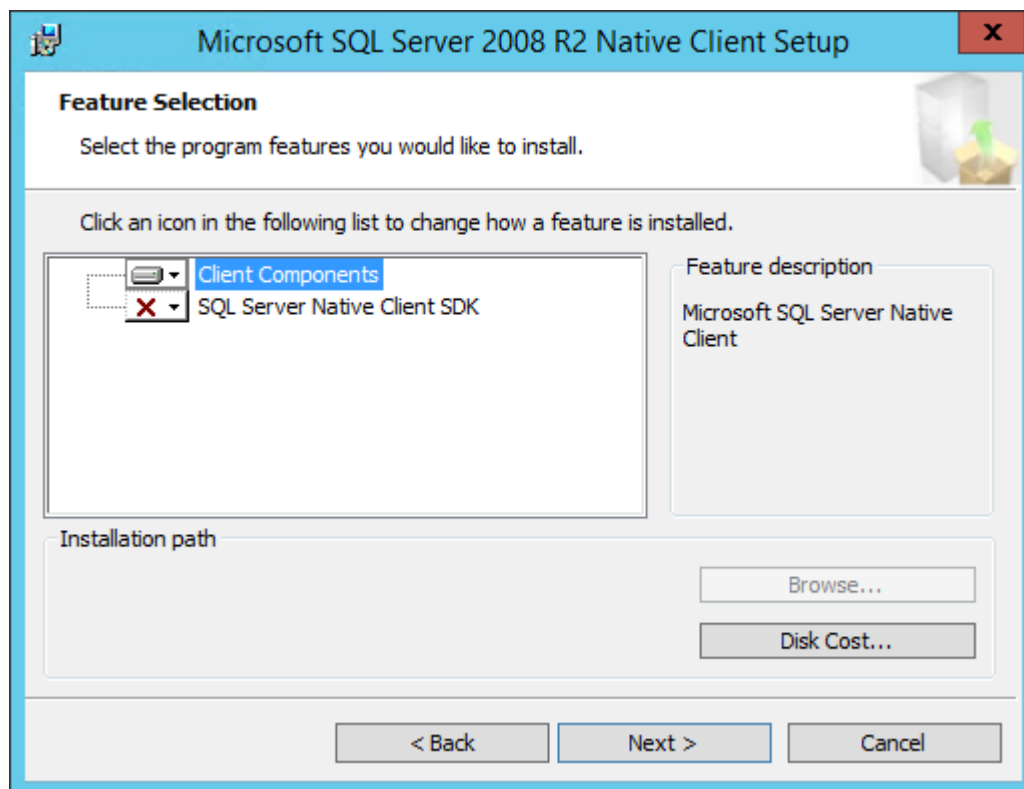


Рисунок 10.15 – Окно выбора устанавливаемых функций Native Client

10.3.3 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 10.16).

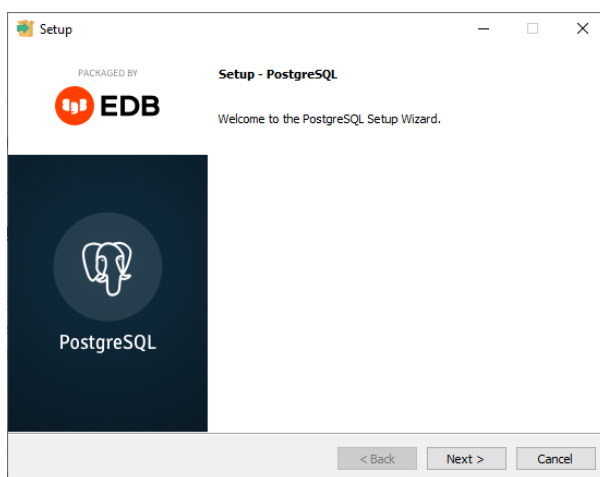


Рисунок 10.16 – Мастер установки

3. При установке PostgreSQL предоставляется возможность выбора директории установки (по умолчанию предлагается директория «*C:\Program File\PostgreSQL\15*») (Рисунок 10.17).

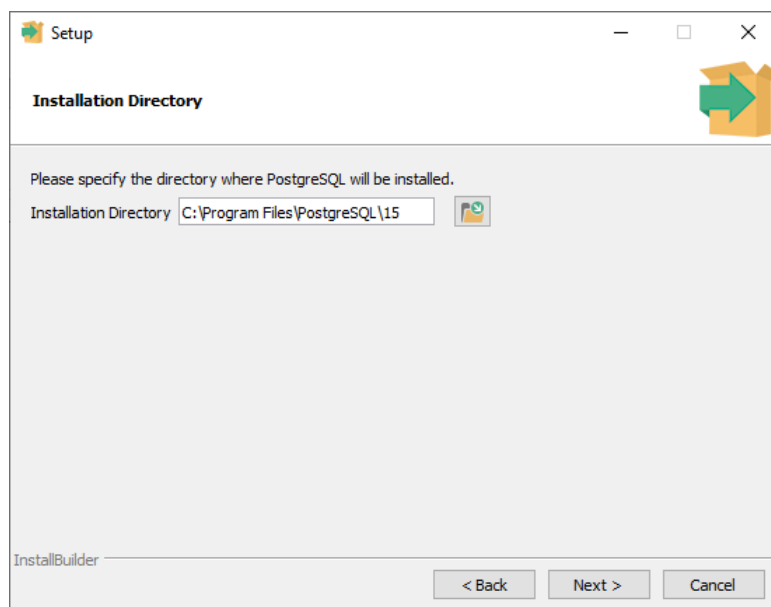


Рисунок 10.17 – Выбор папки установки

4. В окне «*Select Components*» выбрать необходимые компоненты для установки (Рисунок 10.18).

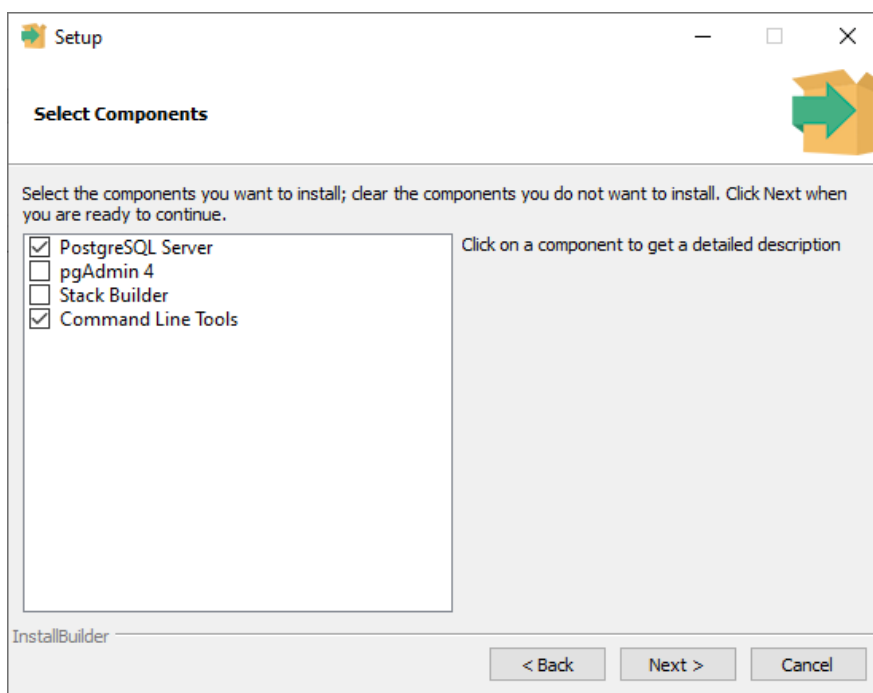


Рисунок 10.18 – Компоненты устанавливаемой программы

5. Выбор каталога данных (Рисунок 10.19).

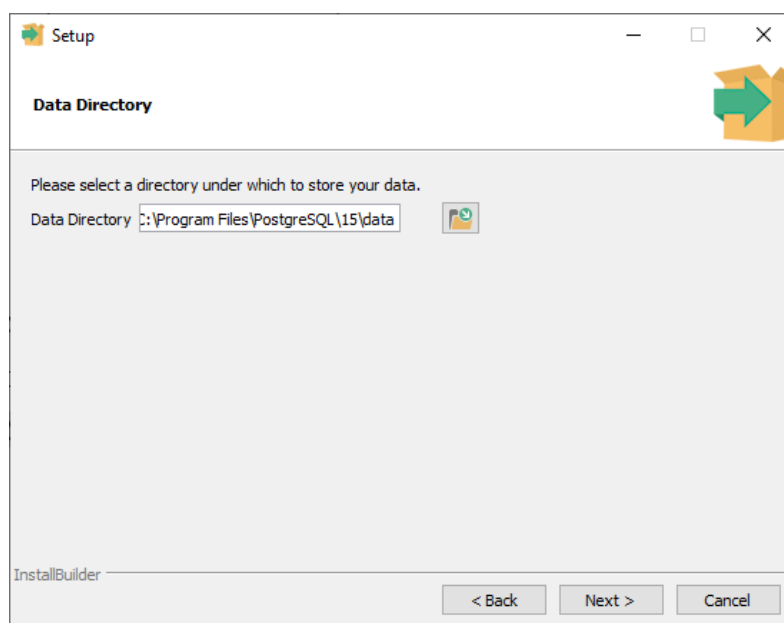


Рисунок 10.19 – Выбор каталога данных

6. На следующих шагах задаются параметры сервера (Рисунок 10.20, Рисунок 10.21, Рисунок 10.22).

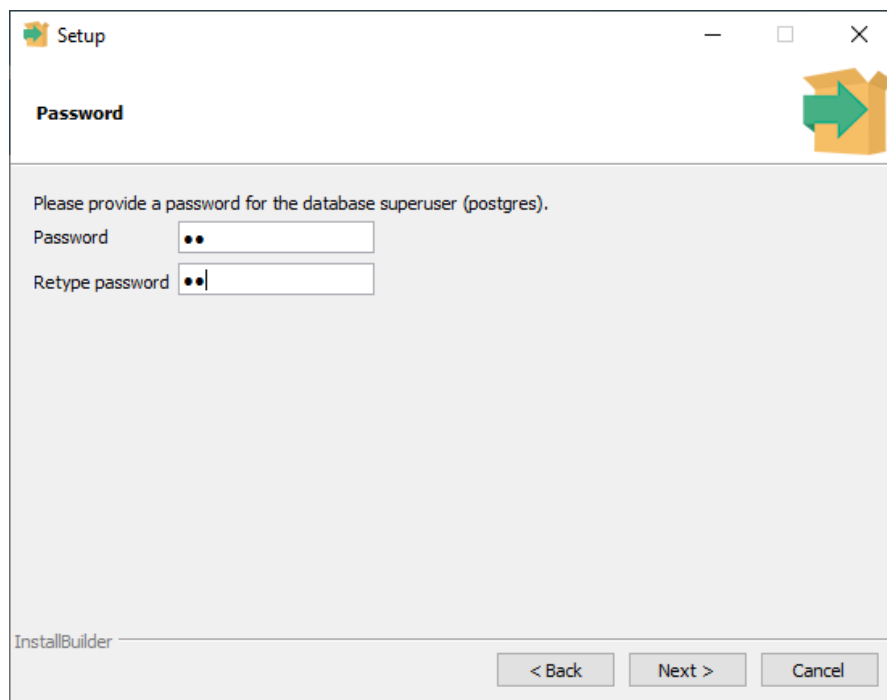


Рисунок 10.20 – Пароль суперпользователя базы данных

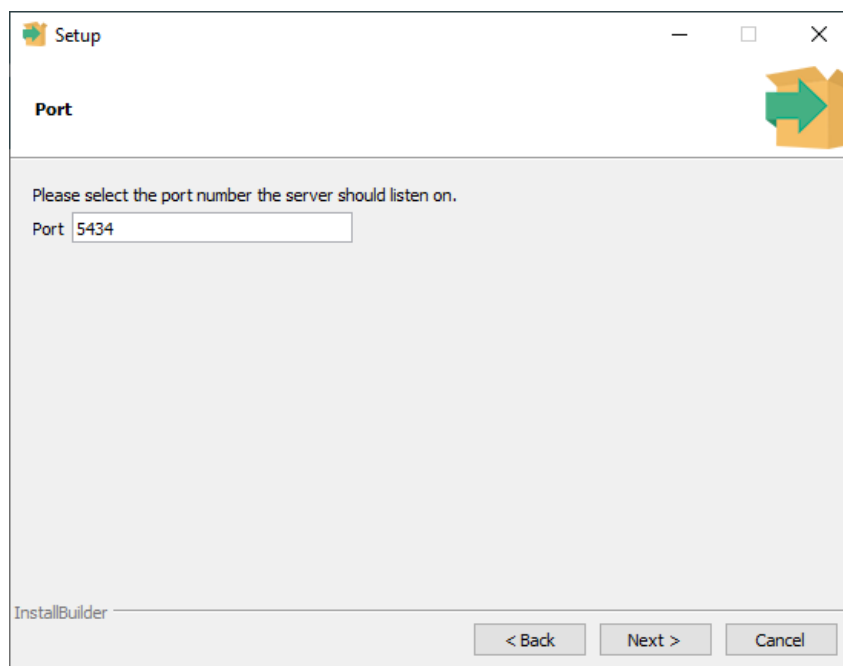


Рисунок 10.21 – Номер порта

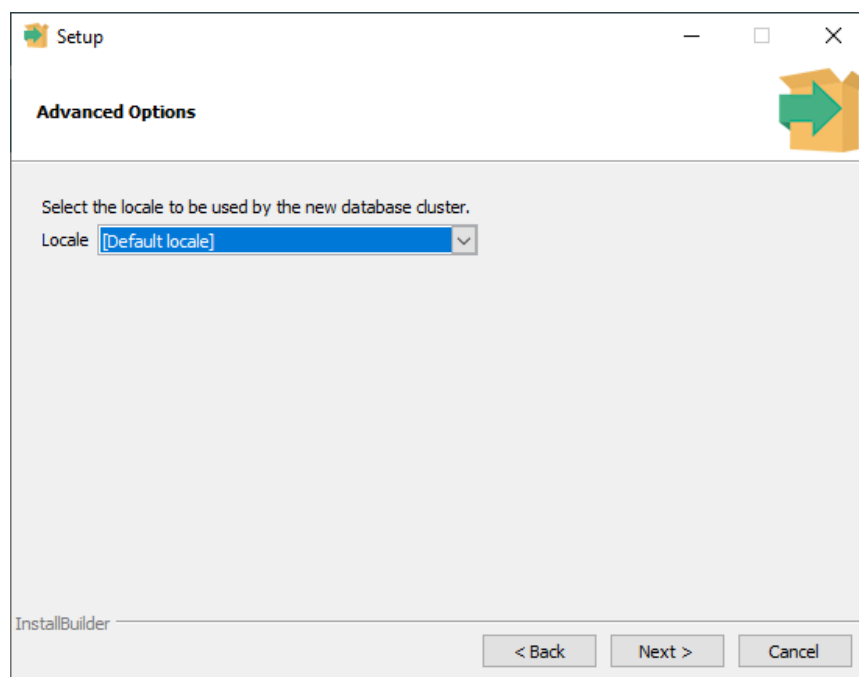


Рисунок 10.22 – Locale

7. На следующем шаге в окне мастера отображается вся информация, полученная программой установки (Рисунок 10.23).

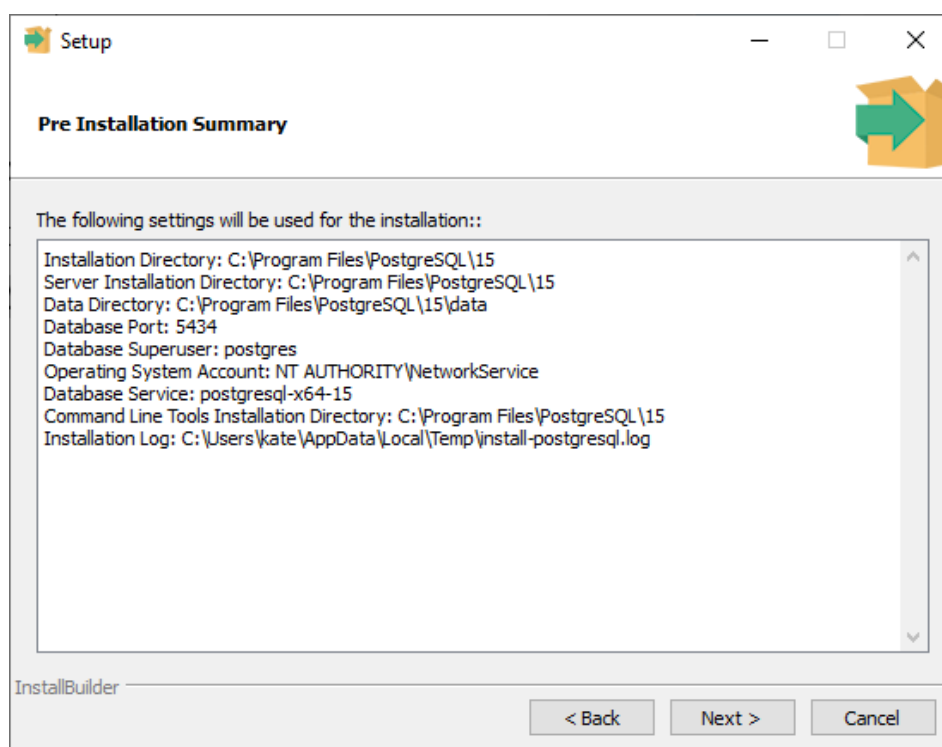


Рисунок 10.23 – Завершений сбора информации

8. На следующем шаге в окне мастера отображается информация о готовности к установке PostgreSQL (Рисунок 10.24).

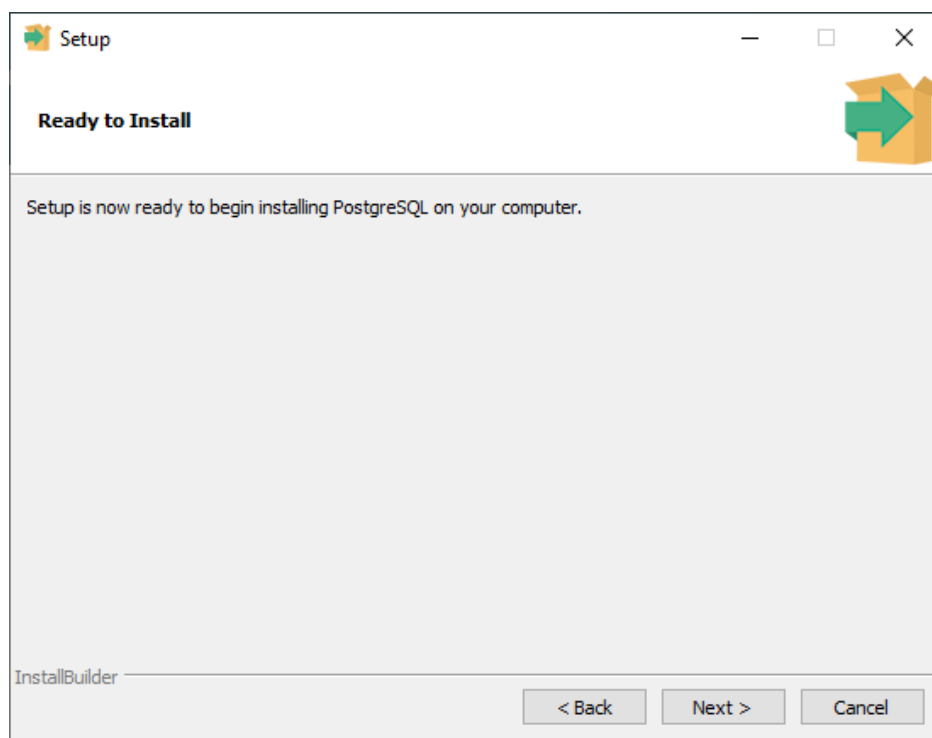


Рисунок 10.24 – Готовность к установке PostgreSQL

9. Последним этапом является процесс копирования файлов (Рисунок 10.25).

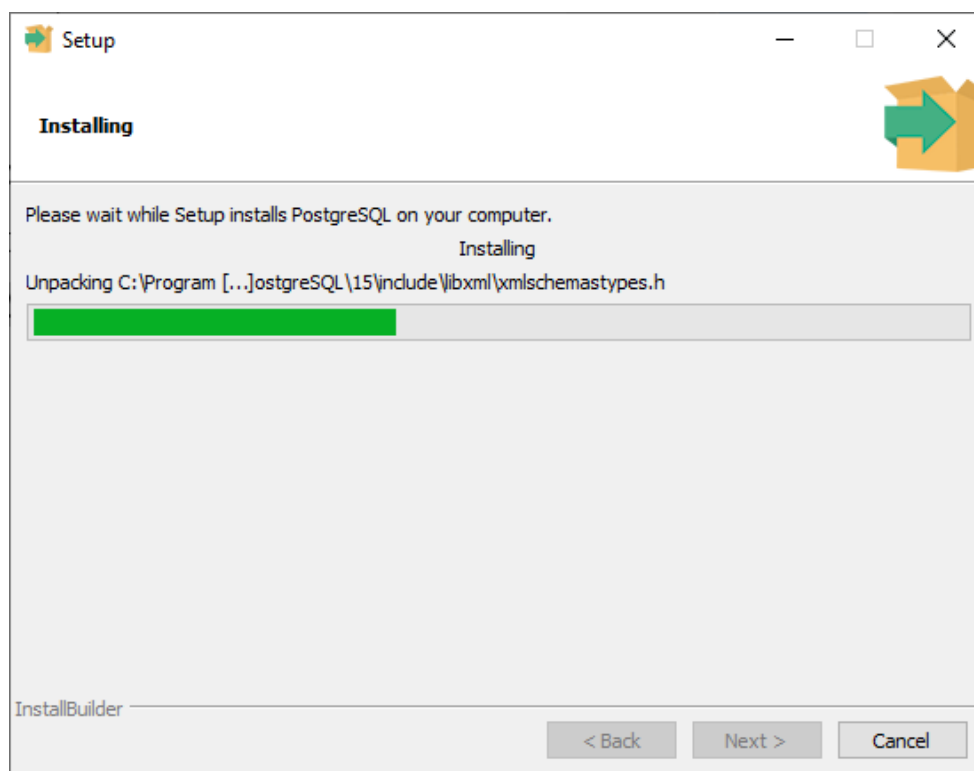


Рисунок 10.25 – Процесс копирования файлов

10. По окончании процесса установки появляется окно завершения установки (Рисунок 10.26).

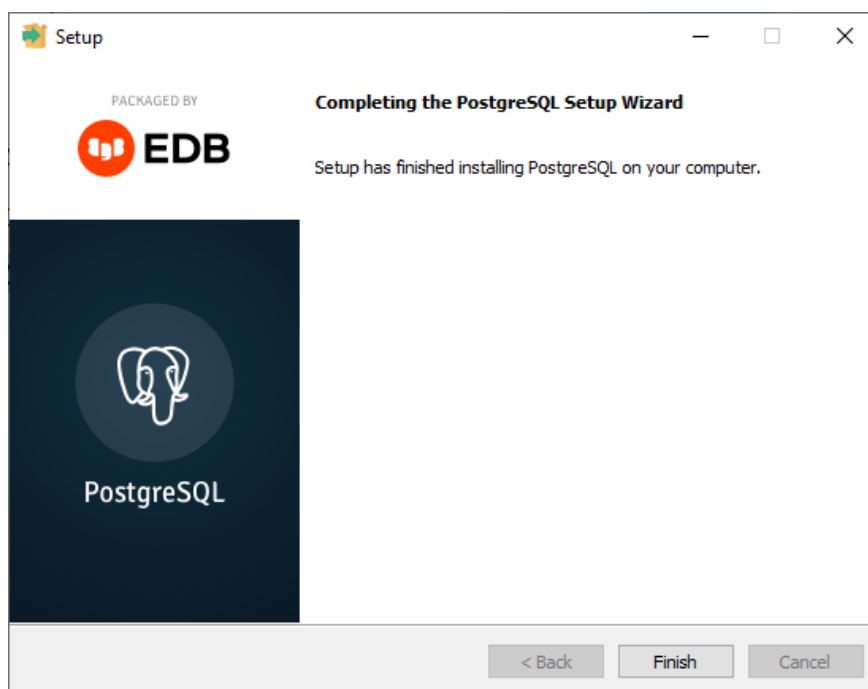


Рисунок 10.26 – Окно завершения установки

10.4 Настройка HTTPS в IIS

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 10.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.
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 10.27).

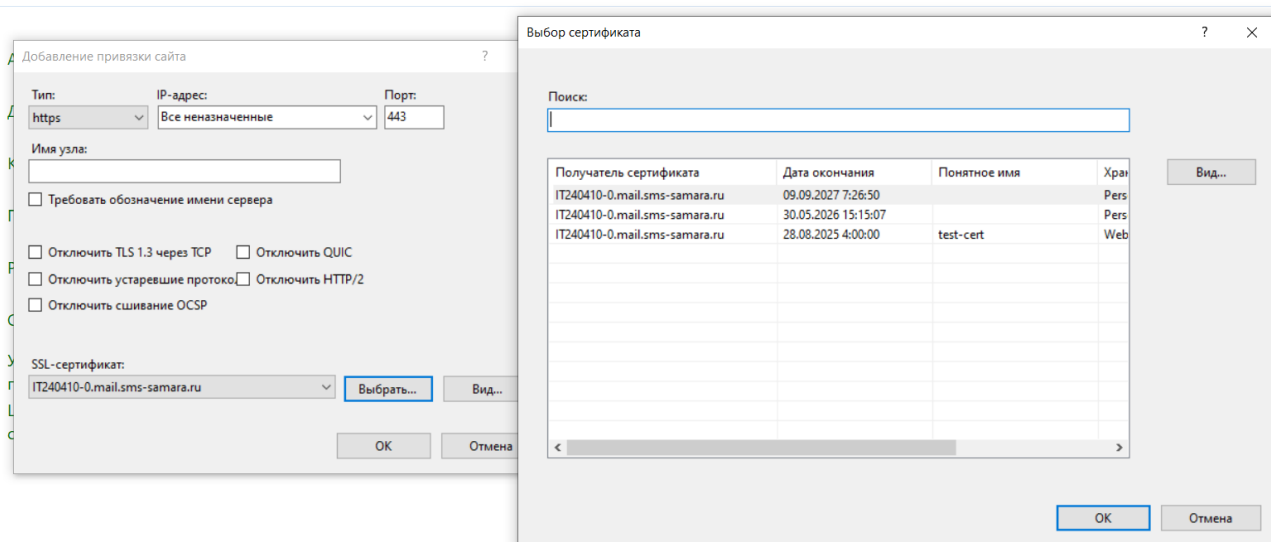


Рисунок 10.27 – Окно «Добавление привязки узла»

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 комплекс.

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 10.28).

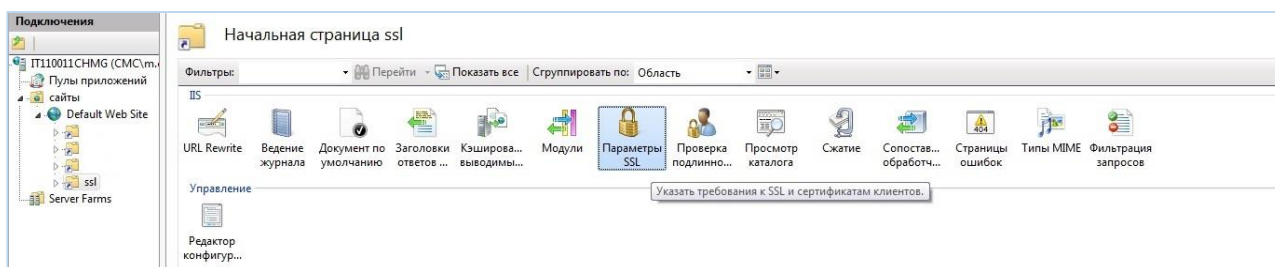


Рисунок 10.28 – Начальная страница SSL

В параметрах SSL в «Сертификатах клиента» выбрать «Игнорировать» и далее в действиях выбрать «Применить». После этого необходимо перезагрузить сайт, на котором проводилась настройка (Рисунок 10.29). 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.

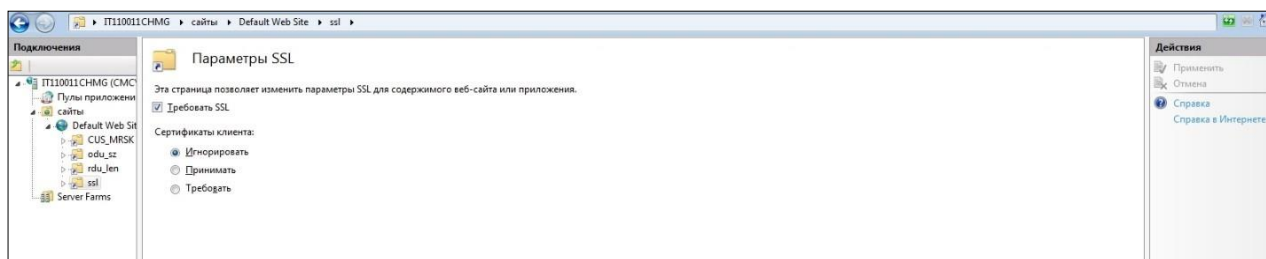


Рисунок 10.29 – Параметры SSL

В результате сайт будет работать через защищенное соединение (Рисунок 10.30).

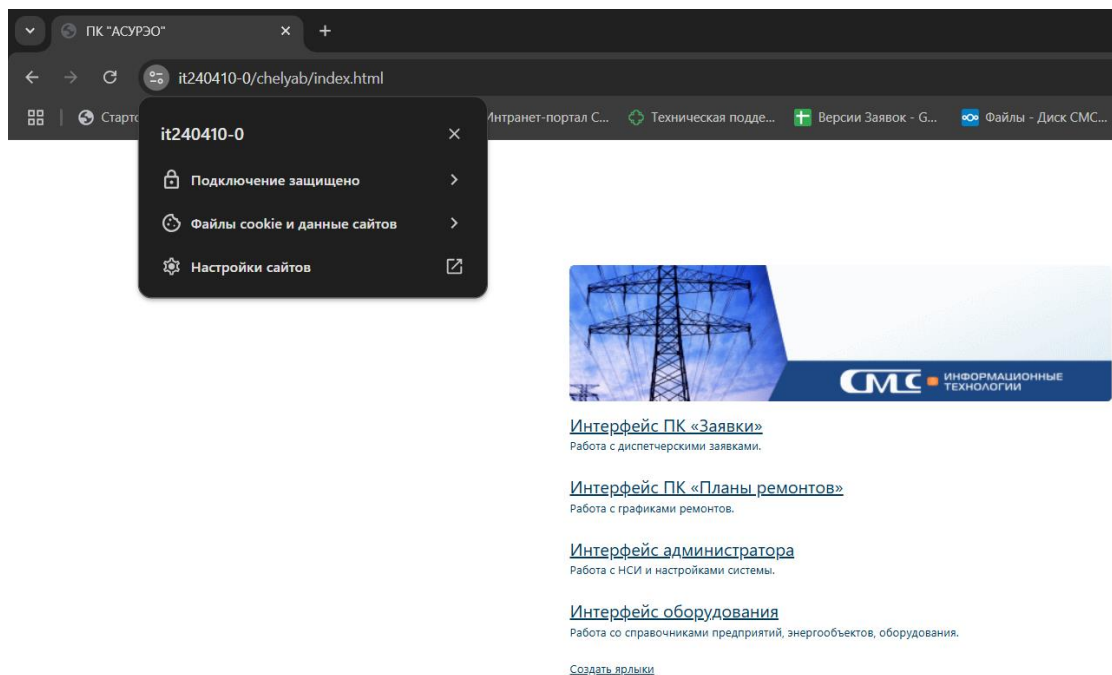


Рисунок 10.30 – Работа сайта через защищенное соединение

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 zvsk.ini.

10.5 Настройка basic-авторизации для комплекса на ОС MS Windows

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 одной 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 защищённости 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 10.31).

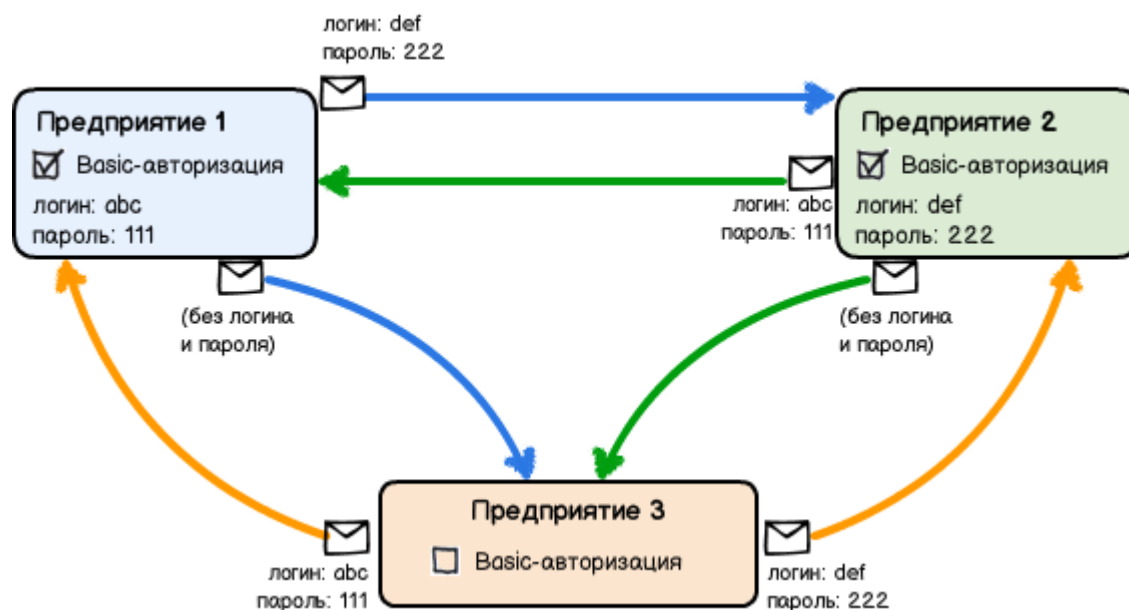


Рисунок 10.31 – Схема отправки сообщений по протоколу SOAP

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

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 10.32).

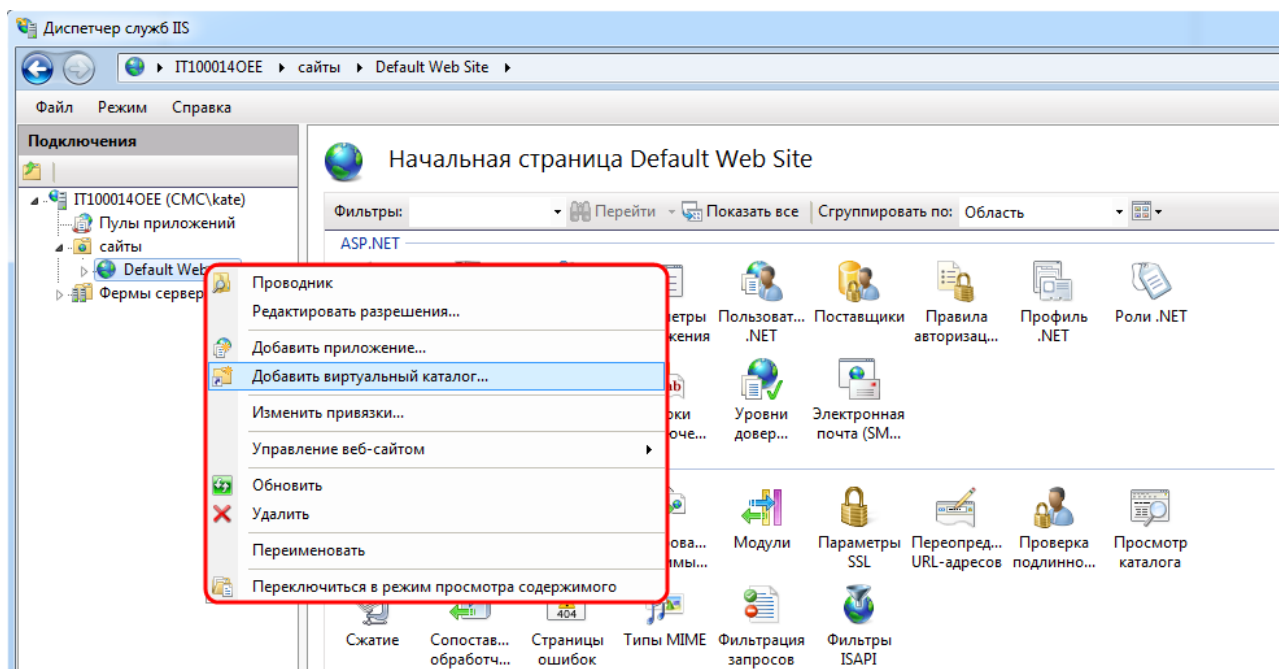


Рисунок 10.32 – Сайт на который установлен ПК

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 10.33).

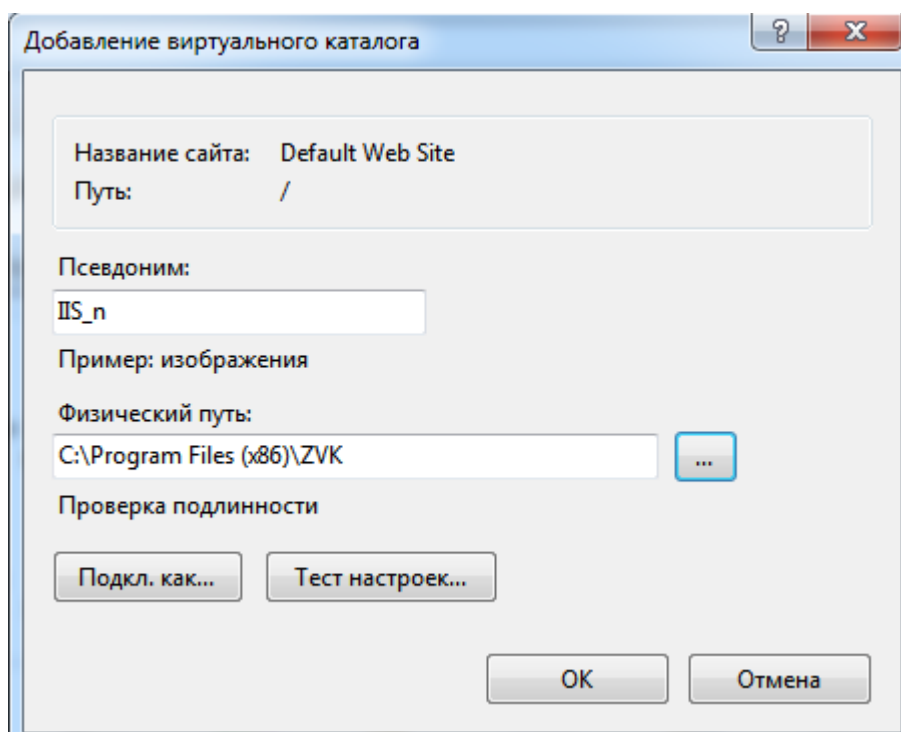
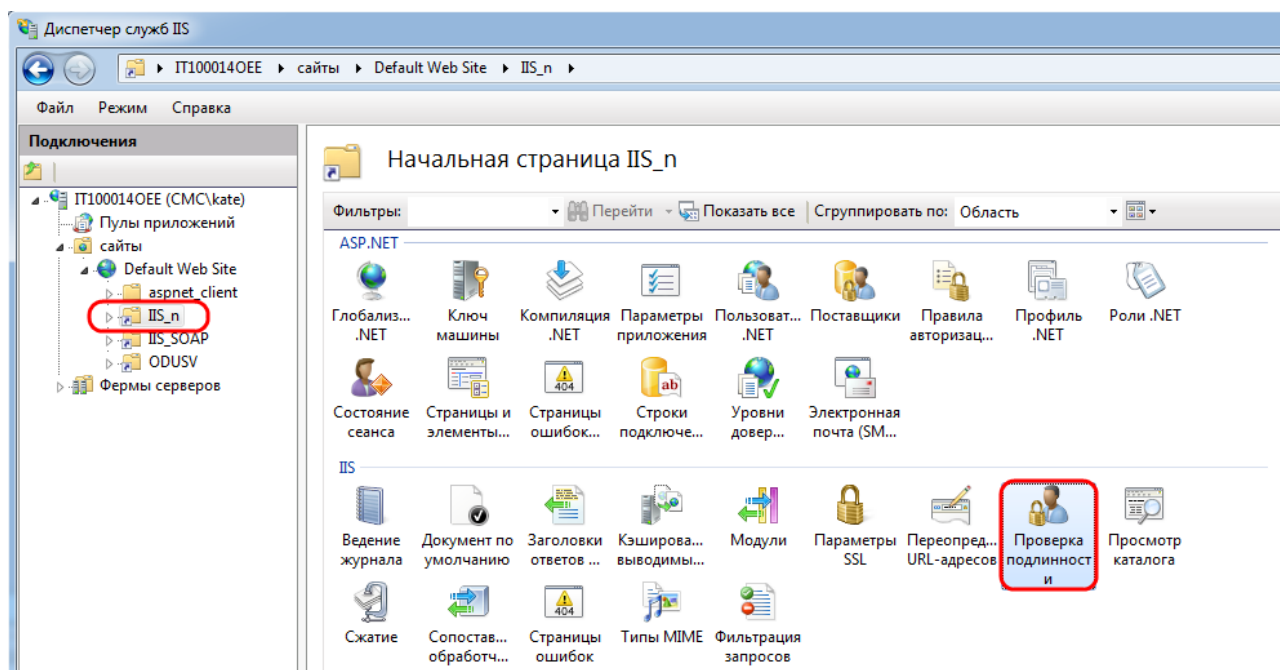


Рисунок 10.33 – Добавление виртуального каталога

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).

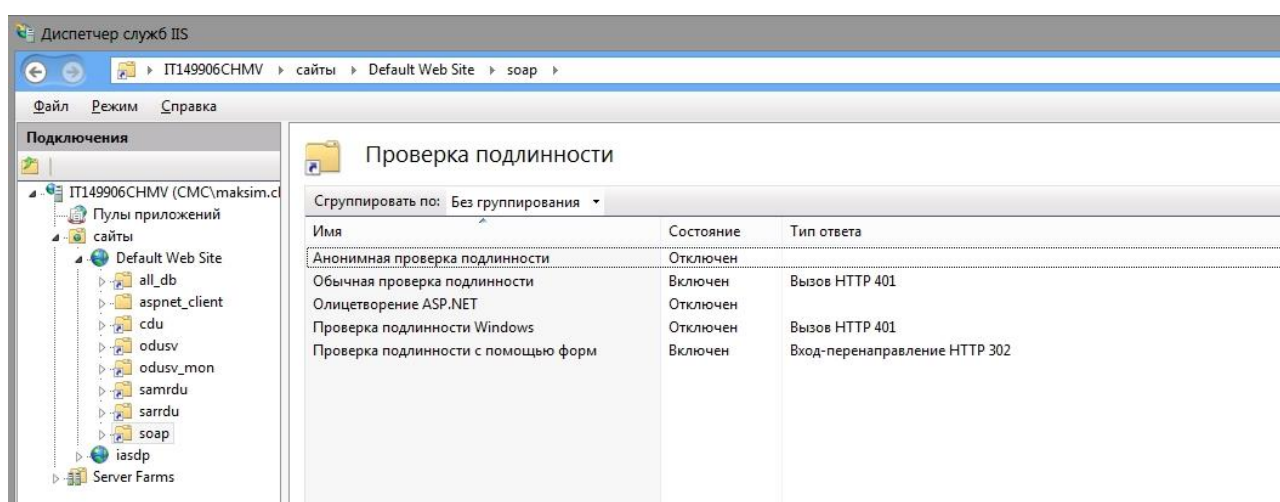
2) Перейти в Диспетчер Служб IIS и найти сайт, на котором установлен ПК. Перейти к виртуальному каталогу, созданному ранее (Рисунок 10.34).



3) Перейти на вкладку «Проверка подлинности» (Рисунок 10.35).

4) Отключить «Анонимную проверку подлинности» (Рисунок 10.35).

5) Включить «Обычная проверка подлинности» (Рисунок 10.35).



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 10.36). Пароль учетной записи транспортных настроек не должен содержать символ «№».

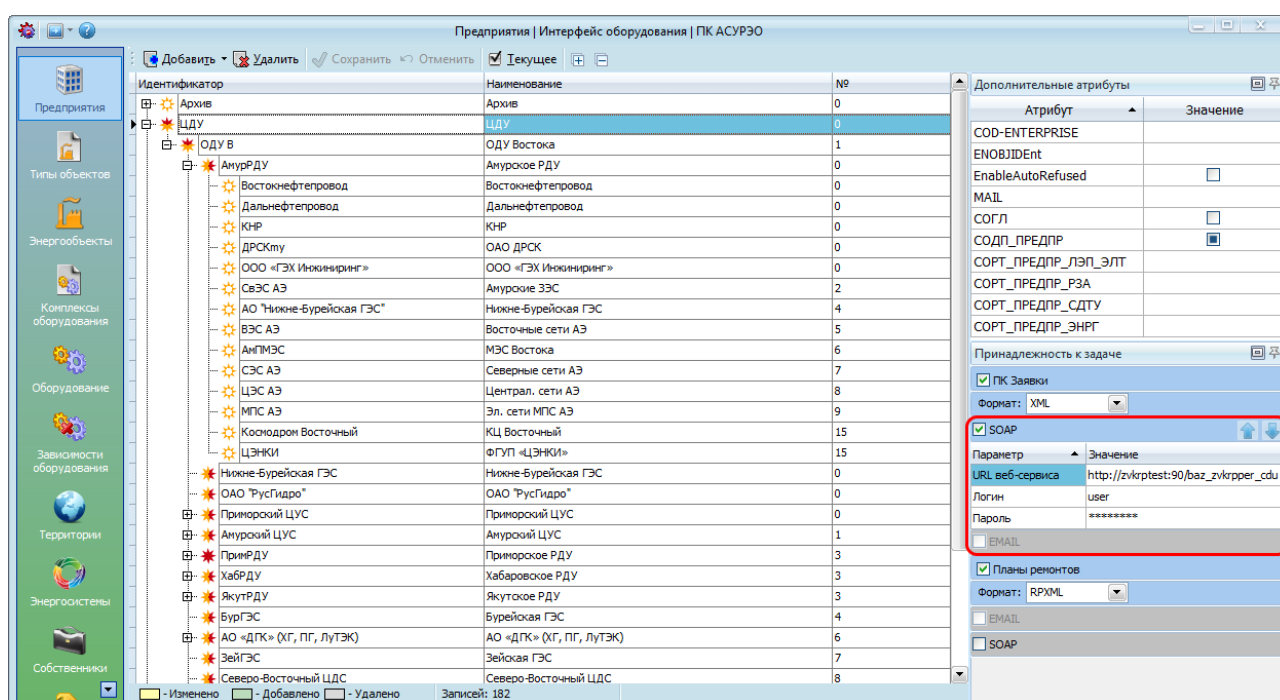


Рисунок 10.36 – Настройка транспорта SOAP

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 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 исполняемому файлу, в текущем примере «c:\etcd\etcd.exe». Остальные параметры оставить без изменений.
- Запустить службу, убедиться в её работоспособности.

11 Установка и настройка системного ПО на ОС Linux

11.1 Установка ОС Astra 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 11.1 – Рисунок 11.5).

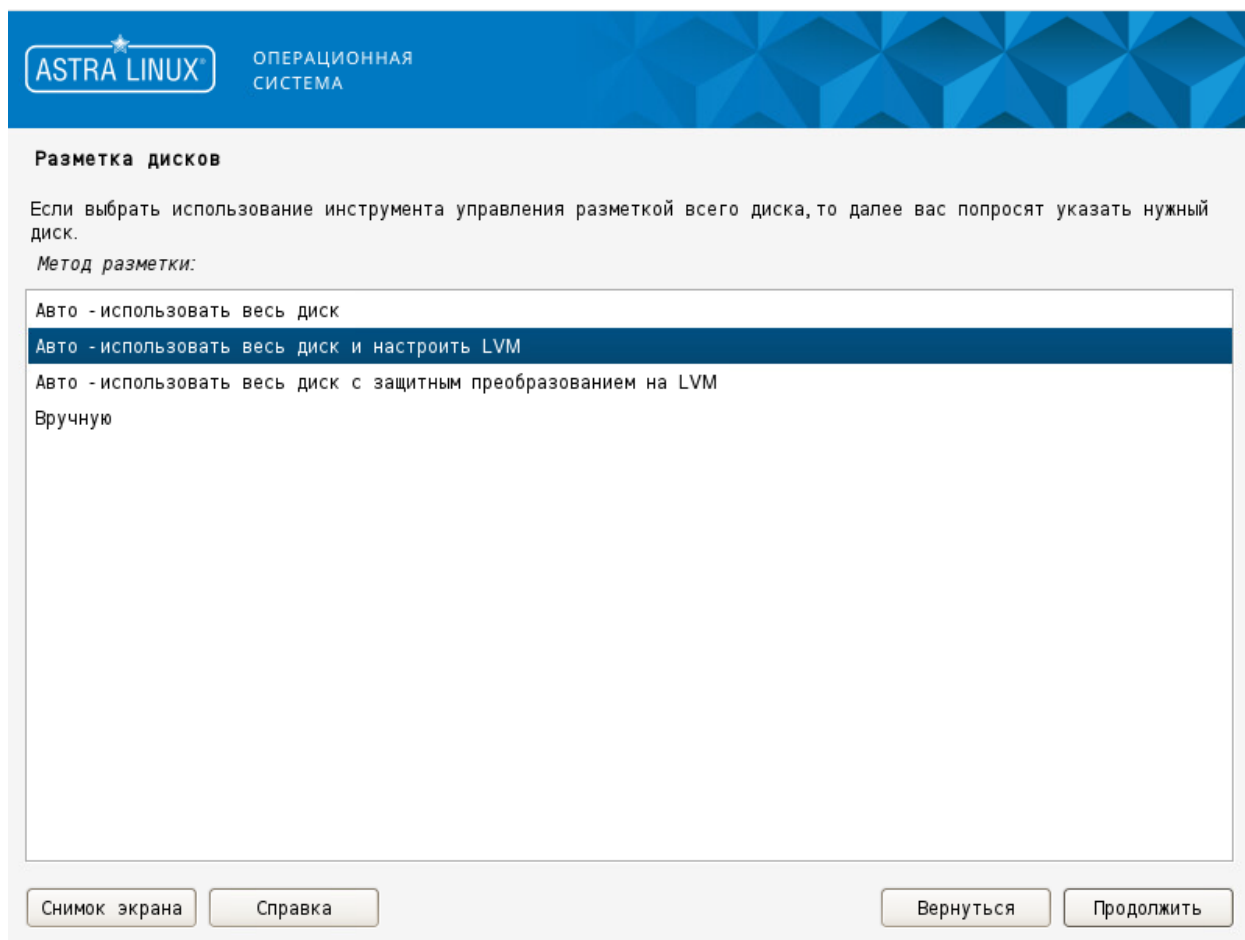


Рисунок 11.1 – Метод разметки дисков

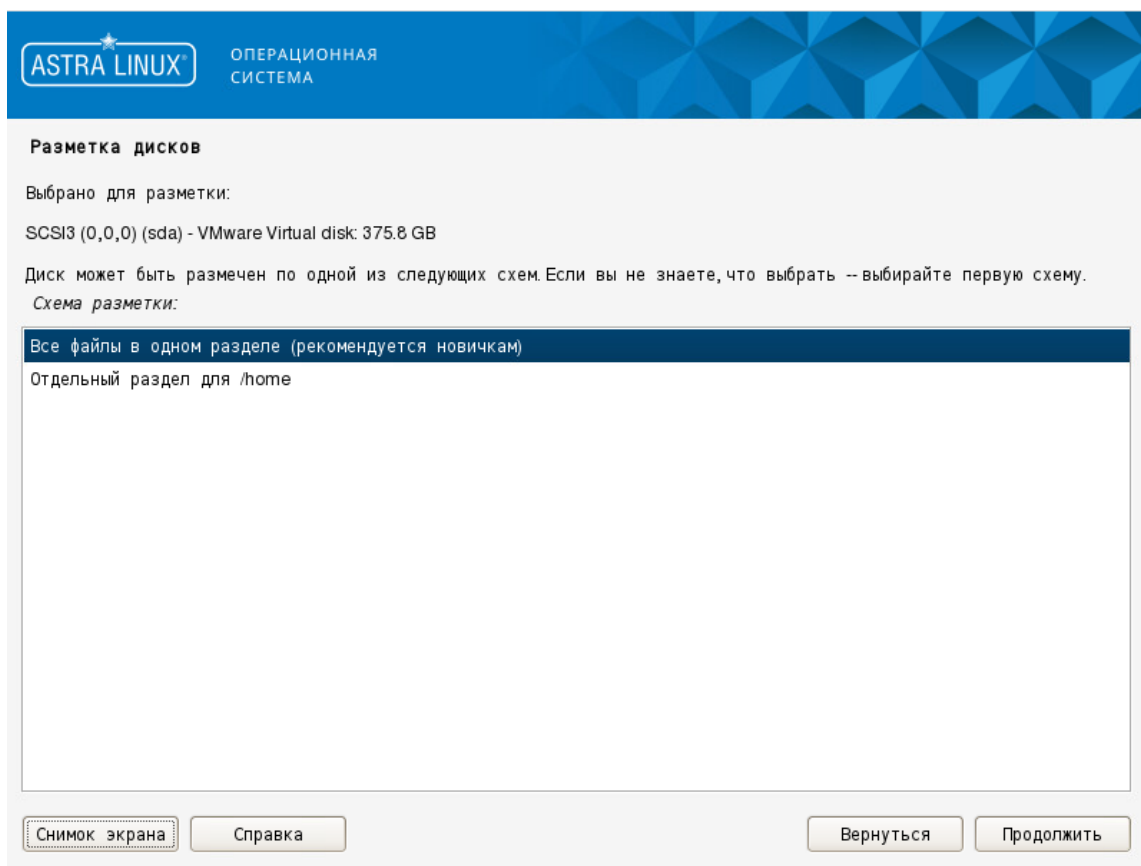


Рисунок 11.2 – Выбор схемы разметки

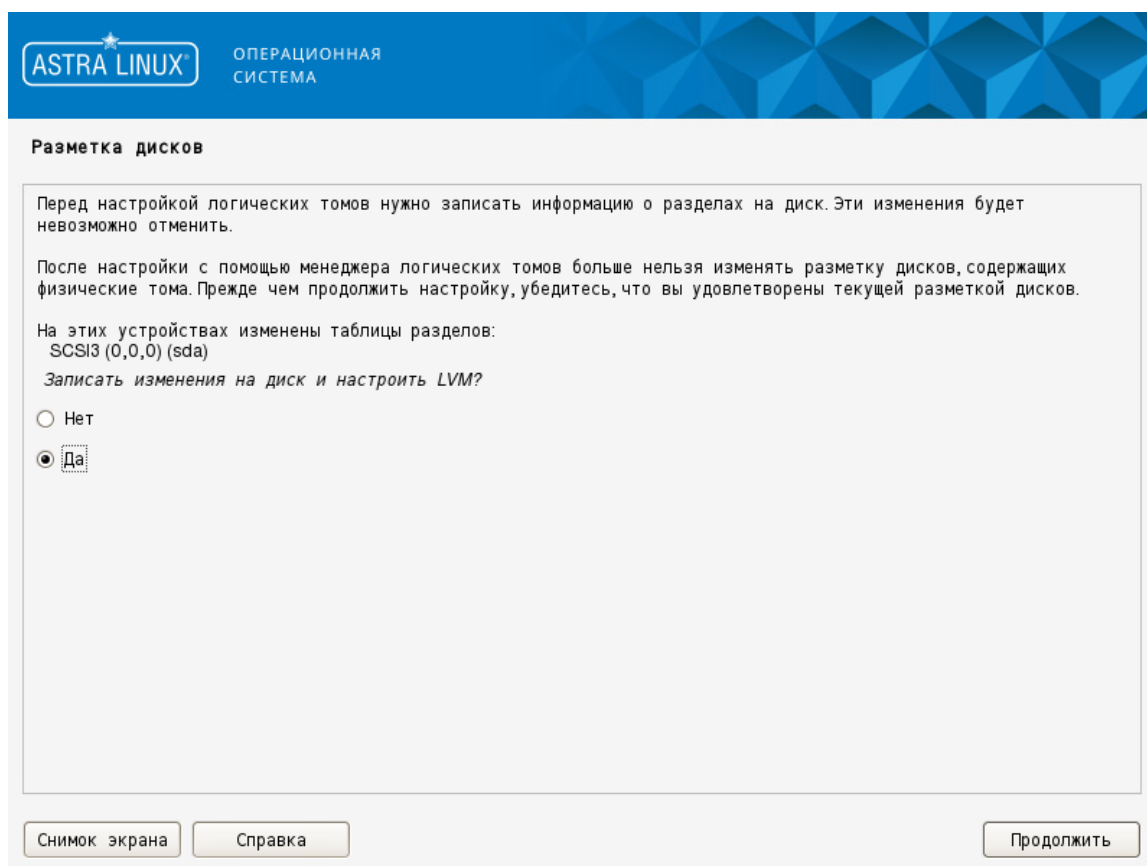


Рисунок 11.3 – Подтверждение выбранных параметров

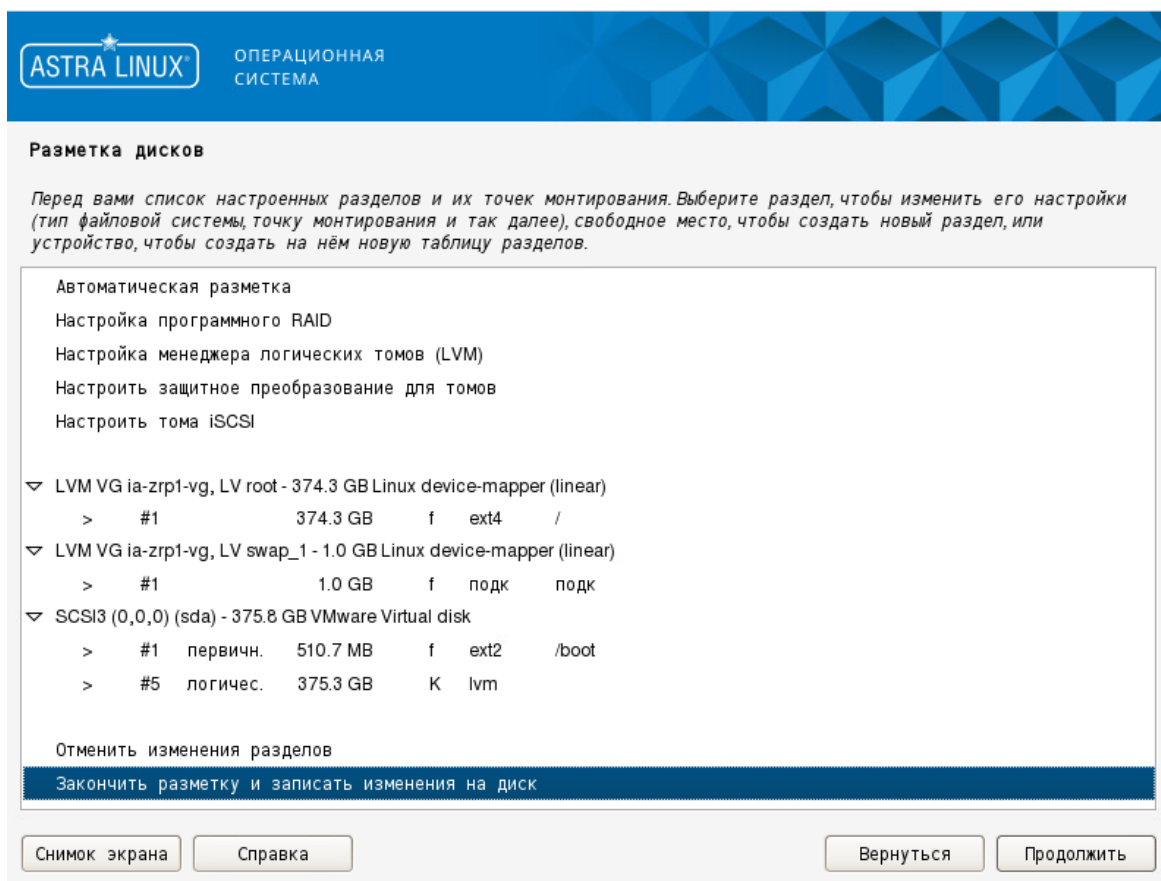


Рисунок 11.4 – Завершение разметки дисков

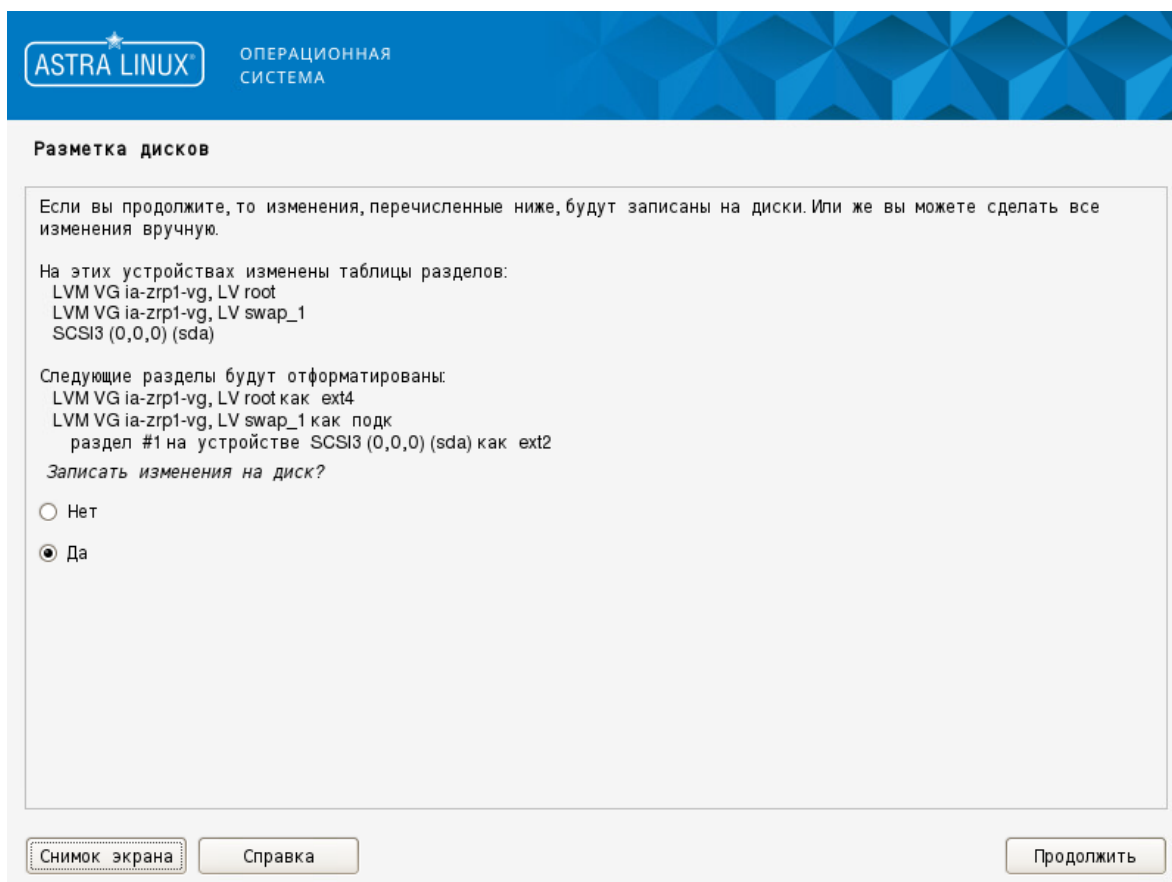


Рисунок 11.5 – Запись изменений по разметке дисков

2. Выбор ядра установки (Рисунок 11.6).

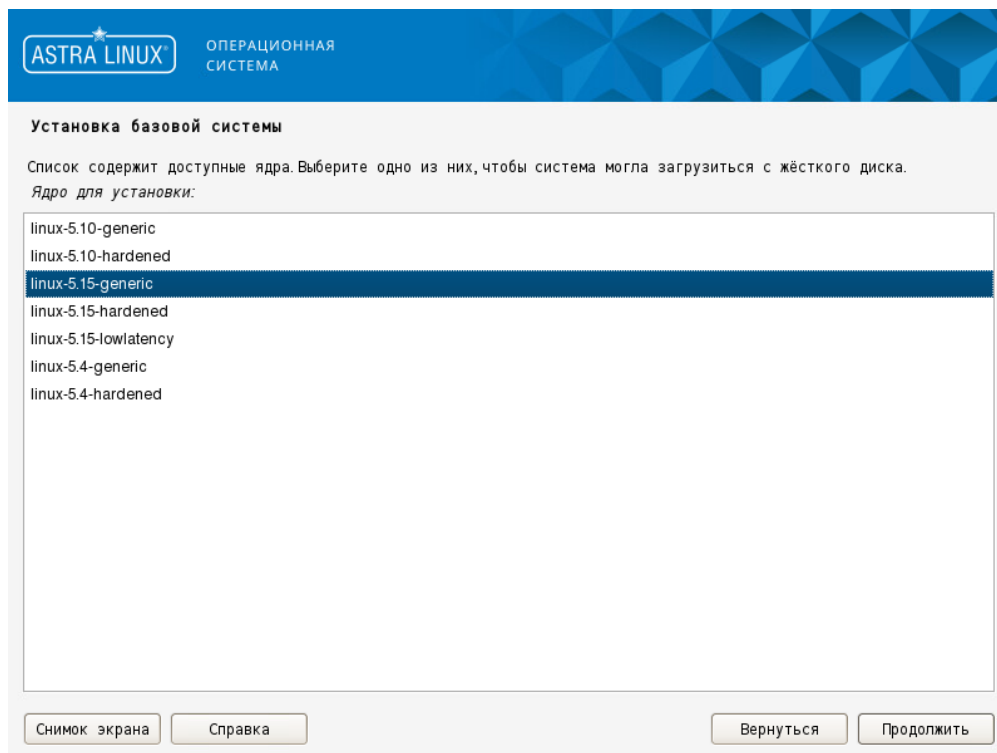


Рисунок 11.6 – Выбор ядра для установки

3. Выбор дополнительного ПО. Необходимо установить флаги «Консольные утилиты», «Средства удаленного подключения SSH» (Рисунок 11.7).

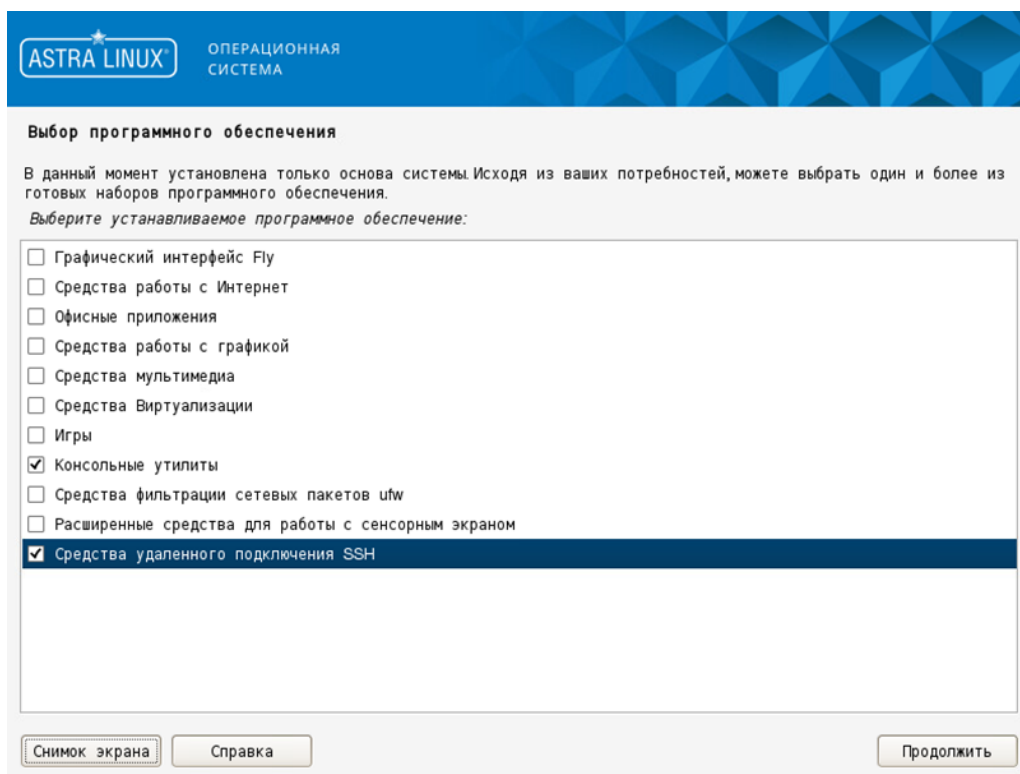


Рисунок 11.7 – Выбор дополнительного ПО

4. Дополнительные настройки ОС. Необходимо выбрать уровень защищенности, как минимум указать «Базовый уровень защищенности «Орел» (Рисунок 11.8).

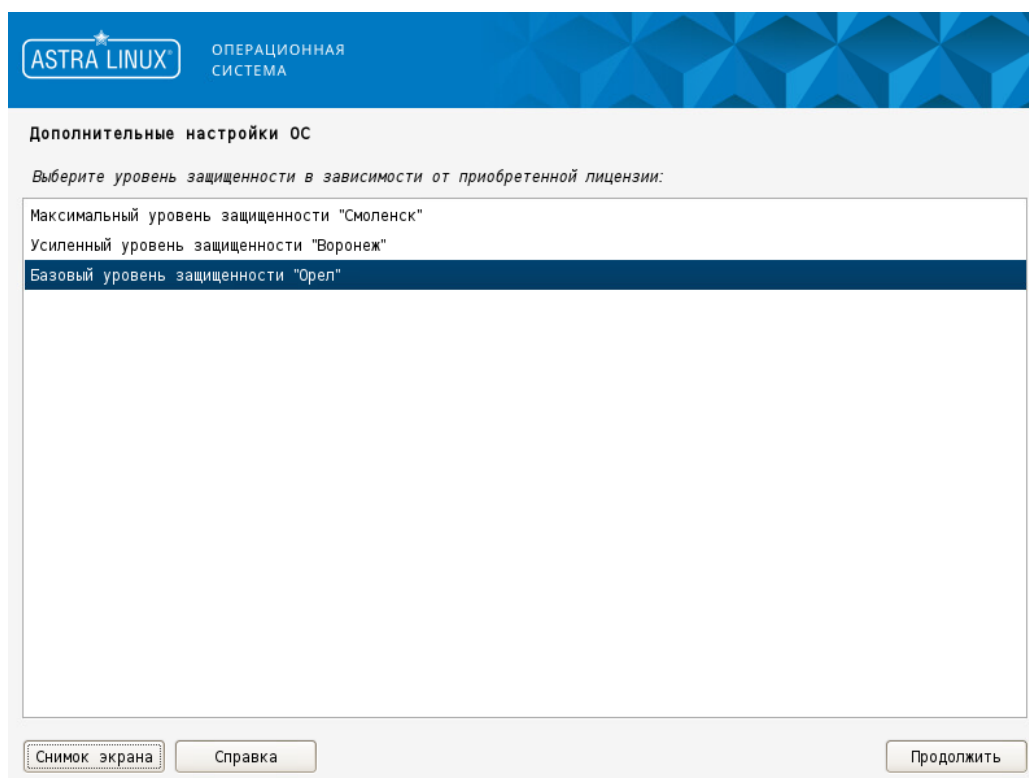


Рисунок 11.8 – Выбор уровня защищенности

На следующем шаге можно выбрать дополнительные настройки ОС. По умолчанию не требуются (Рисунок 11.9).

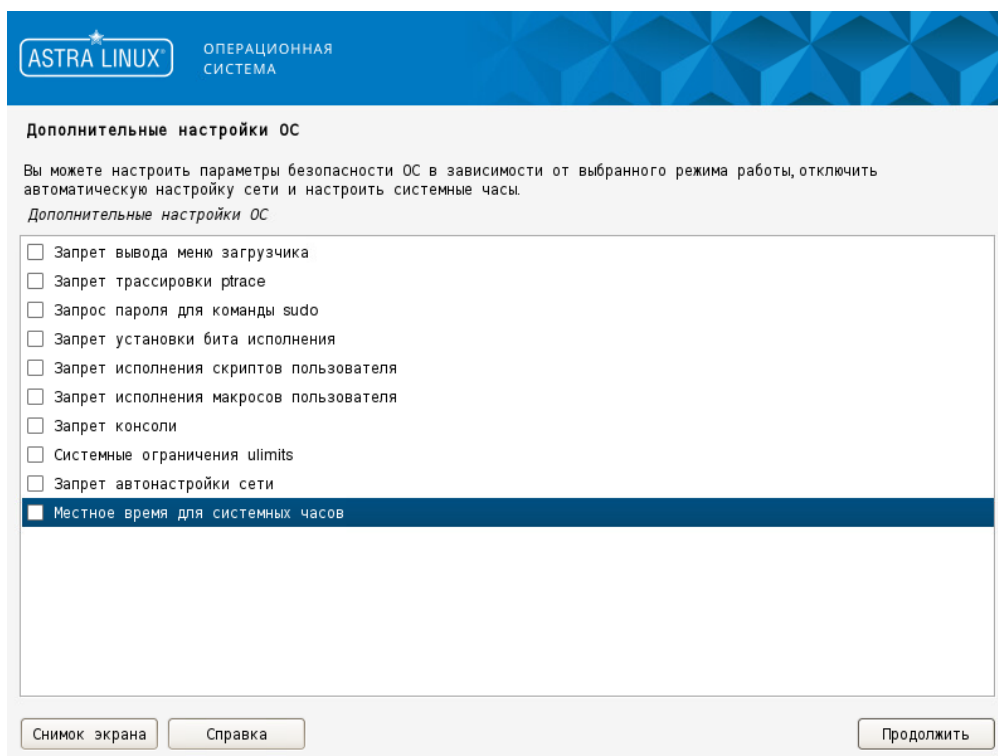


Рисунок 11.9 – Выбор дополнительных настроек

11.2 Обновление ОС Astra Linux

Для обновления с одной мажорной версии на другую требуется установка пакета обновления «astra-full-upgrade»:

sudo apt install astra-full-upgrade

После установки пакета обновления, требуется провести ряд манипуляций для успешного запуска обновления.

Если требуется обновление на минорную версию 1.8.x (где x - номер минорной версии), то необходимо отредактировать файл `/usr/lib/python3/dist-packages/astra_upgrade/configs/upgrade.conf.yaml` и указать репозитории данной версии в параметре `sources`.

Если требуется обновление на последнюю версию Astra Linux, предыдущий шаг можно пропустить.

Обязательная предварительная настройка:

1. Установить последнюю доступную версию ядра ОС:
sudo apt install linux-image-latest
2. Перезагрузить ОС с использованием последней версии ядра.
3. Если есть пакеты, которые не должны обновляться, необходимо добавить их в раздел `packages -> whitelist` конфигурационного файла.
4. Если есть пакеты `nginx` и `postgresql`, то необходимо выполнить `systemctl stop + systemctl disable`:
sudo systemctl disable nginx
sudo systemctl stop nginx
sudo systemctl disable postgresql
sudo systemctl stop postgresql
5. Выполнить проверку возможности обновления:
sudo astra-full-upgrade check
6. После выполнения предыдущей команды, будет предоставлен отчет, в котором можно увидеть, можно ли обновиться, или же что-либо мешает.
7. Если в отчете получаем сообщение, что все готово к обновлению, выполняем команду:
sudo astra-full-upgrade force

Обращаем внимание, что в отчете также указываются пакеты, которые после обновления могут некорректно работать или вовсе быть удалены.

8. По результатам обновления проверить, что все хорошо. При переходе на Astra 1.8.3 были проблемы с docker-compose и PostgreSQL 15. Для решения проблемы с docker-compose достаточно выполнить переустановку на версию 2:

sudo apt remove docker-compose

sudo apt install docker-compose-v2

Убрать настройку astra-sec-level 6 в docker (если была). Если есть проблемы с юнитом PostgreSQL 15 проверить, нет ли в конфигурации строки `ac_audit_mode = 'internal'`. При наличии – удалить или закомментировать.

9. После обновления пакеты PostgreSQL PRO могут быть перезаписаны, даже в случае указания их в whitelist'e, требуется переустановка БД после успешного обновления (перед обновлением ОС рекомендуется создание резервной копии БД).

11.3 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.io docker-compose-v2

3. Проверить работу docker:

systemctl status docker

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

11.4 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`

11.5 Настройка сети docker

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

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

1. `sudo 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. При этом значение "bip" должно быть уникальным для каждого сервера.

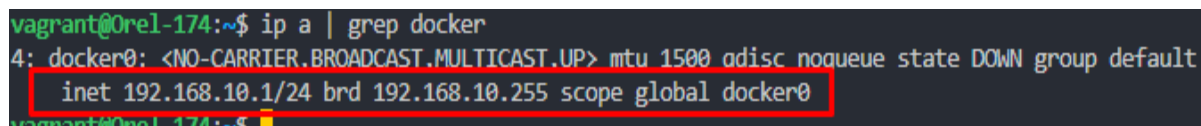
Сохранить и перезапустить службу docker.

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 11.10).

A terminal window showing the command 'ip a | grep docker' being executed. The output line is '4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 adisc noqueue state DOWN group default' followed by 'inet 192.168.10.1/24 brd 192.168.10.255 scope global docker0'. The IP address '192.168.10.1/24' is highlighted with a red rectangle.

```
vagrant@Orel-174:~$ ip a | grep docker
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 adisc noqueue state DOWN group default
   inet 192.168.10.1/24 brd 192.168.10.255 scope global docker0
```

Рисунок 11.10 – Измененный ip

Для предотвращения неконтролируемого роста логов контейнеров рекомендуется настроить политику ротации на уровне docker-демона.

Для этого необходимо выполнить следующие рекомендации:

1. Подготовка конфигурационного файла.

Отредактировать файл конфигурации docker-демона `/etc/docker/daemon.json`. Если файл не существует, его необходимо создать.

Внимание! Если файл уже существует, добавьте новые параметры в существующий JSON-объект, не нарушая его структуры.

2. Добавление параметров ротации логов.

Для использования драйвера `json-file` с ограничением максимального размера лога каждого контейнера до 2 ГБ, добавить или убедиться в наличии следующей секции в файле `daemon.json`:

```
json
{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "2g"
  }
}
```

Примечание: Параметр `"max-size"` также поддерживает единицы измерения `m` (мегабайты) и `k` (килобайты). Например, `"10m"` или `"500k"`.

3. Применение изменений.

После сохранения файла конфигурации необходимо применить изменения. Выполните следующие команды:

```
# Перезагрузить конфигурацию systemd-демонов
```

```
sudo systemctl daemon-reload
```

```
# Перезапустить службу docker для применения новой конфигурации
```

```
sudo systemctl restart docker
```

4. Проверка работоспособности.

После перезапуска `docker` проверить состояние всех системных служб и работу ваших контейнеров.

- Убедиться, что `docker`-демон работает: `sudo systemctl status docker`
- Проверить, что все необходимые контейнеры запущены: `docker ps`
- Если какие-либо контейнеры не запустились автоматически, перезапустить их вручную: `docker restart <имя_или_id_контейнера>`

11.6 Подготовка веб-сервера nginx и настройка конфигурационного файла default.conf

Для работы Системы на ОС семейства Linux используется веб-сервер nginx.

Для автоматизированного запуска web-сервера nginx с использованием docker-контейнеров и docker-compose необходимо выполнить следующие действия:

1. Если на сервере отсутствует доступ к внешним серверам Docker Hub, то необходимо вручную загрузить на сервер образ nginx:alpine из внутреннего репозитория docker registry организации, либо получить файл с данным образом и загрузить его командой:

```
docker load -i <имя_файла_образа>.tar.
```

2. Открыть файл «nginx.conf» из комплекта поставки на редактирование.

Файл «nginx.conf» содержит общие настройки nginx, описание upstream-серверов и подключение конфигурационного файла «default.conf».

Пример файла «nginx.conf»:

```
user www-data;
```

```
worker_processes auto;
```

```
error_log /var/log/nginx/error.log notice;
```

```
pid /var/run/nginx.pid;
```

```
#load_module /etc/nginx/modules-enabled/nginx_http_auth_spnego_module.so; # Раскомментировать  
для spnego
```

```
events {
```

```
    worker_connections 1024;
```

```
}
```

```
http {
```

```
    map $http_upgrade $connection_upgrade {
```

```

default upgrade;
"";
}

upstream web_requests_5000 {
    server asunet:5000;

    keepalive 32;

    keepalive_timeout 60s;

    keepalive_requests 100;
}

upstream web_app_5001 {
    server asunet:5001;

    keepalive 32;

    keepalive_timeout 60s;

    keepalive_requests 100;
}

upstream web_configurator_5002 {
    server asunet:5002;

    keepalive 16;

    keepalive_timeout 60s;

    keepalive_requests 100;
}

upstream asu_appsite_9880 {
    server localhost:9880;
}

```

```
    keepalive 32;

    keepalive_timeout 60s;

    keepalive_requests 100;
}

upstream asu_appservice_8625 {

    server localhost:8625;

    keepalive 32;

    keepalive_timeout 60s;

    keepalive_requests 100;
}

include /etc/nginx/conf.d/default.conf;
}
```

При редактировании файла «nginx.conf» необходимо скорректировать адреса и порты upstream-серверов в соответствии с фактической схемой развертывания:

- «web_requests_5000» — сервер веб-заявок, по умолчанию «asunet:5000»;
- «web_app_5001» — сервер авторизации веб-версии, по умолчанию «asunet:5001»;
- «web_configurator_5002» — сервер веб-конфигуратора, по умолчанию «asunet:5002»;
- «asu_appsite_9880» — сервер приложений Delphi, по умолчанию «localhost:9880», при необходимости заменить порт в адресе и наименовании upstream'a;
- «asu_appservice_8625» — SOAP-сервис Delphi, по умолчанию «localhost:8625», при необходимости заменить порт в адресе и наименовании upstream'a.

Параметр «map \$http_upgrade \$connection_upgrade» используется для корректной передачи заголовков «Upgrade» и «Connection» при проксировании запросов, требующих обновления HTTP-соединения.

При необходимости использования SPNEGO-модуля необходимо раскомментировать строку:

```
load_module /etc/nginx/modules-enabled/ngx_http_auth_spnego_module.so;
```

3. Открыть файл «default.conf» из комплекта поставки на редактирование.

Файл «default.conf» содержит настройки виртуальных серверов nginx для веб-заявок, сервера авторизации, веб-конфигуратора и Delphi-заявок.

- default.conf для .Delphi + .Net

При редактировании необходимо скорректировать:

- имя сервера в директиве «server_name»;
- внешние HTTP- и HTTPS-порты;
- пути к сертификату и закрытому ключу;
- при необходимости — правила перенаправления HTTP на HTTPS;
- правила проксирования к upstream-серверам, указанным в «nginx.conf».

Пример конфигурации для сервера веб-заявок:

Настройки для веб заявок

```
server {  
  
    listen    81;  
  
    listen [::]:81;  
  
    server_name cluster;  
  
  
  
    listen 443 ssl;  
  
    listen [::]:443 ssl;  
  
  
  
    ssl_certificate /etc/nginx/ssl/mycert.crt;  
    ssl_certificate_key /etc/nginx/ssl/mycert.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;
```

```
# Если нужен редирект с http на https, то напомним этот параметр в этом же контексте.
```

```
if ($scheme = "http") {
```

```
    return 308 https://$server_name:443$uri;
```

```
}
```

```
location / {
```

```
    proxy_pass http://web_requests_5000/;
```

```
    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;
```

```
    proxy_set_header    Upgrade       $http_upgrade;
```

```
    proxy_set_header    Connection    $connection_upgrade;
```

```
    proxy_http_version  1.1;
```

```
}
```

```
}
```

Пример конфигурации для сервера авторизации веб-версии:

```
server {
```

```
    listen 82;
```

```
    listen [::]:82;
```

```
    server_name cluster;
```

```
    listen 444 ssl;
```

```
    listen [::]:444 ssl;
```

```
ssl_certificate /etc/nginx/ssl/mycert.crt;

ssl_certificate_key /etc/nginx/ssl/mycert.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;


# Если нужен редирект с http на https, то напишем этот параметр в этом же контексте.
if ($scheme = "http") {
    return 308 https://$server_name:444$uri;
}


location / {

    proxy_read_timeout 60s;

    proxy_connect_timeout 60s;

    proxy_pass http://web_app_5001/;

    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;

    proxy_set_header    Upgrade             $http_upgrade;

    proxy_set_header    Connection         $connection_upgrade;

    proxy_http_version  1.1;

}
```

```
}
```

```
...
```

Пример конфигурации для веб-конфигуратора:

```
```nginx
```

```
Настройки для веб конфигуратора
```

```
server {
```

```
 listen 83;
```

```
 listen [::]:83;
```

```
 listen 445 ssl;
```

```
 listen [::]:445 ssl;
```

```
 server_name cluster;
```

```
 ssl_certificate /etc/nginx/ssl/mycert.crt;
```

```
 ssl_certificate_key /etc/nginx/ssl/mycert.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;
```

```
Если нужен редирект с http на https, то напишем этот параметр в этом же контексте.
```

```
if ($scheme = "http") {
```

```
 return 308 https://$server_name:445$uri;
```

```
}
```

```
location / {
```

```
 proxy_read_timeout 60s;
```

---

```
proxy_connect_timeout 60s;

proxy_pass http://web_configurator_5002/;

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;

proxy_set_header Upgrade $http_upgrade;

proxy_set_header Connection $connection_upgrade;

proxy_http_version 1.1;

}

}

...

```

Пример конфигурации для Delphi-заявок:

```
``nginx

Настройки для дэлфи заявок

server {

 listen 80;

 listen [::]:80;

 listen 445 ssl;

 listen [::]:445 ssl;

 server_name cluster;

 ssl_certificate /etc/nginx/ssl/mycert.crt;

 ssl_certificate_key /etc/nginx/ssl/mycert.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;

location /zvk/ {

 # Раскомментируйте alias, если nginx на хосте

 # alias /etc/nginx/www/;

 try_files $uri $uri =404;

}

location ~ ^/zvk/appsrv/proxy.dll/help/(.*)$ {

 rewrite ^/zvk/appsrv/proxy.dll/help/(.*)$ /appservice/help/$1;

}

location ~ ^/zvk/appsrv/(proxy.dll)?(.*)$ {

 if ($http_user_agent ~* 'RemObjects') {

 rewrite ^/zvk/appsrv/(proxy.dll)?(.*)$ /appservice/$2;

 }

 if ($arg_service ~* CIMIntegrationService) {

 rewrite ^/zvk/appsrv/(proxy.dll)?(.*)$ /zvk/auth/$2;

 }

 rewrite ^/zvk/appsrv/(proxy.dll)?(.*)$ /appsite/$2;

}
```

---

```
location ~ \.application {
```

```
 types {
```

```
 application/x-ms-application application;
```

```
 application/x-ms-manifest manifest;
```

```
 application/octet-stream deploy;
```

```
 }
```

```
}
```

```
location /appsite/ {
```

```
 proxy_pass http://asu_appsite_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://asu_appservice_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;
```

```
}
```

```
location / {
```

---

```
 return 301 /zvк/index.html;
 }

 location ~ ^/zvк/ZVK_NET {
 return 301 http://$host:81;
 }

 location ~ ^/zvк/CONFIGURATOR_NET {
 return 301 http://$host:83;
 }
}
```

**Внимание!** При одновременном использовании веб-конфигуратора и Delphi-заявок необходимо убедиться, что HTTPS-порты в соответствующих «server»-блоках не конфликтуют. Если для веб-конфигуратора используется порт «445 ssl», то для Delphi-заявок должен быть указан другой свободный HTTPS-порт, либо наоборот. Использование одного и того же сочетания «listen» и «server\_name» в нескольких «server»-блоках может привести к некорректной обработке запросов.

4. При необходимости отредактировать mapping портов в «docker-compose.yml» в секции с веб-сервером.

Пример mapping портов для nginx:

*services:*

*webserver:*

*image: nginx:alpine*

*restart: always*

*container\_name: webserver*

*ports:*

*- "80:80"*

*- "81:81"*

*- "82:82"*

- 
- "83:83"
  - "443:443"
  - "444:444"
  - "445:445"

volumes:

- ./nginx-config/nginx.conf:/etc/nginx/nginx.conf
- ./nginx-config/conf.d:/etc/nginx/conf.d
- ./nginx-config/www:/etc/nginx/www
- ./nginx-config/ssl/mycert.crt:/etc/nginx/ssl/mycert.crt
- ./nginx-config/ssl/mycert.key:/etc/nginx/ssl/mycert.key

Если для какого-либо сервиса используется другой внешний порт, его необходимо дополнительно указать в секции «ports».

5. После изменения конфигурационных файлов необходимо проверить корректность конфигурации nginx командой:

```
docker exec webserver nginx -t
```

Если проверка завершилась успешно, необходимо перечитать конфигурацию nginx:

```
docker exec webserver nginx -s reload
```

Либо перезапустить контейнер веб-сервера:

```
docker-compose restart webserver
```

Если изменялись настройки контейнеров или mapping портов, необходимо выполнить перезапуск контейнеров:

```
docker-compose down
```

```
docker-compose up -d
```

После запуска необходимо проверить доступность:

- Delphi-заявок: «http://<имя\_сервера>/zvkk/index.html»;
- веб-заявок: «http://<имя\_сервера>:81» или «https://<имя\_сервера>:443»;
- сервера авторизации веб-версии: «http://<имя\_сервера>:82» или «https://<имя\_сервера>:444»;

- 
- веб-конфигуратора: «http://<имя\_сервера>:83» или соответствующий HTTPS-порт.

## 11.7 Настройка HTTPS для веб-сервера nginx

Процесс настройки HTTPS:

1. На веб-сервере назначается закрытый ключ, с помощью которого генерируется запрос сертификата (открытого ключа).

2. Получение подписанного сертификата.

Если в соответствии с политиками безопасности требуется использовать заверенные сертификаты, то необходимо получить его в центре сертификации вашей организации или же другим разрешённым политиками способом. Ниже приводится команда для создания самоподписанного сертификата на 365 дней и закрытого ключа:

```
sudo openssl req -x509 -nodes -addext "subjectAltName = IP:ip_сервера,
DNS:имя_сервера" -days 365 -newkey rsa:2048 -keyout private.key -out private.crt
```

3. Подготовка конфигурационных файлов.

В случае использования веб-сервера nginx установка подписанного сертификата и настройка сервера заключается в подключении закомментированных секций с конфигурациями HTTPS в default.conf. При этом особенность веб-версии Системы заключается в обязательном использовании HTTPS-соединения при работе с сайтами сервера приложений и сервера авторизации.

4. Установка подписанного сертификата на сервере.

Для этого необходимо загрузить закрытый ключ и сертификат на сервер, после чего в файле docker-compose.yml настроить mapping данных файлов. Например, если на сервере файлы лежат в директории /opt/zvk/nginx-config/certs/, то в секцию volumes для контейнера веб-сервера добавить строки:

- ./nginx-config/certs/private.crt:/etc/nginx/ssl/private.crt
- ./nginx-config/certs/private.key:/etc/nginx/ssl/private.key

Также mapping сертификата и корневого сертификата при его наличии нужно добавить в секцию volumes и для контейнера веб-версии:

- ./nginx-config/certs/root.crt:/etc/ssl/certs/root.crt
- ./nginx-config/certs/private.crt:/etc/ssl/certs/private.crt

---

## 11.8 Настройка basic-авторизации для комплекса на ОС Linux

### 11.8.1 Общие сведения

Общая информация по принципам и преимуществам basic-авторизации описаны в пункте 10.5.1 данного руководства.

### 11.8.2 Настройка web-сервера nginx на ОС Linux

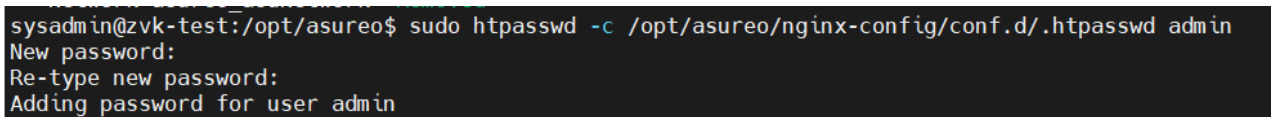
В первую очередь необходимо создать файл с логином и паролем (в хэшированном виде) для доступа к сервису обмена заявок. Для этого используется утилита `htpasswd`, входящая в состав пакета `apache2-utils`. Для начала необходимо загрузить данный пакет:

```
sudo apt update && sudo apt install apache2-utils
```

Далее необходимо создать сам файл. При этом возможно заменить имя пользователя админ на своё:

```
sudo htpasswd -c /opt/zvk/nginx-config/conf.d/.htpasswd admin
```

После ввода команды нужно будет ввести пароль для данного пользователя и повторить его (Рисунок 11.11).



```
sysadmin@zvk-test:/opt/asureo$ sudo htpasswd -c /opt/asureo/nginx-config/conf.d/.htpasswd admin
New password:
Re-type new password:
Adding password for user admin
```

Рисунок 11.11 – Выполнение команды `htpasswd`

Далее получившийся файл нужно передать в контейнер с веб-сервером. Для этого в конфигурационном файле `docker-compose.yml` для контейнера `webserver` в секцию `volumes` добавить строчку:

```
/nginx-config/conf.d/.htpasswd:/etc/nginx/conf.d/.htpasswd
```

А также необходимо настроить basic-авторизацию в конфигурационном файле `default.conf` самого веб-сервера `nginx`. В том числе необходимо отделить доступ внутренних пользователей и интеграций без пароля и внешних с паролем. Для этого в секцию с сайтом делфи-заявок нужно добавить дополнительный `location` параллельно с имеющимся `/appservice/` и `/appsite/`. Имя может быть произвольное, в данном примере он назван `/protectservice/`. Главным отличием от `/appservice/` является наличие секций `auth_basic`

```
location /protectservice/ {
 auth_basic "Enter password!";
 auth_basic_user_file /etc/nginx/conf.d/.htpasswd;
 proxy_pass http://192.168.1.135:8625/;
```

```

 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;
 }

```

```

location /appsite/ {
 proxy_pass http://192.168.1.135:9880/;
 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://192.168.1.135:8625/;
 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;
}

location /protectservice/ {
 auth_basic "Enter password!";
 auth_basic_user_file /etc/nginx/conf.d/.htpasswd;
 proxy_pass http://192.168.1.135:8625/;
 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;
}

```

Рисунок 11.12 – Дополнительный location для basic-авторизации

### 11.8.3 Настройка ПК в части basic-авторизации

Также необходимо настроить ПК предприятий, осуществляющих обмен с данным, для авторизации по логину и паролю при обмене сообщениями. Настройка аналогична разделу 10.5.3 данного руководства. В данном случае в качестве URL-ссылки для обмена будет выступать ссылка вида

<http://192.168.1.135/protectservice/SOAP>

В качестве же логина и пароля соответственно указываются логин и пароль, зафиксированные в файле .htpasswd.

---

## 11.9 Настройка basic authentication для защиты SOAP-сервисов в nginx

Аутентификация позволяет ограничить доступ к SOAP-сервисам предприятия по логину и паролю.

Для настройки базовой аутентификации (Basic Authentication) для защиты SOAP с использованием веб-сервера nginx необходимо выполнить следующие действия:

1. Установить утилиту htpasswd для создания и управления файлами паролей. Данная утилита входит в состав пакета apache2-utils.

Установка пакета:

```
bash
```

```
sudo apt install apache2-utils
```

При возникновении ошибок (проблемы с кэшем или зависимостями):

```
bash
```

```
sudo apt update --fix-missing
```

```
sudo apt install --fix-broken
```

Альтернативная установка (только необходимая утилита без рекомендуемых зависимостей):

```
bash
```

```
sudo apt install --no-install-recommends apache2-utils
```

2. Для создания нового файла паролей используется команда htpasswd с ключом -c (create).

```
bash
```

```
htpasswd -c <путь_к_файлу>/.htpasswd <имя_пользователя>
```

где <путь\_к\_файлу> - директория для сохранения файла паролей,

<имя\_пользователя> - логин для basic-авторизации (произвольное имя).

Например, итоговая команда может выглядеть так:

```
bash
```

```
htpasswd -c /home/vagrant/Desktops/Desktop1/.htpasswd asureo
```

Действия после выполнения:

- Система запросит ввод пароля.
- Подтвердить пароль повторным вводом.
- После успешного выполнения в указанной папке появится файл .htpasswd

**Примечание:** Для просмотра созданного файла в файловом менеджере необходимо включить отображение скрытых файлов.

- 
3. Готовый файл `.htpasswd` необходимо поместить в папку `nginx-config/conf.d` экземпляра `nginx`, где настраивается `basic`-авторизация.

Путь: `./nginx-config/conf.d/.htpasswd`

**Важно:** Убедитесь, что файл скопирован именно в эту директорию — путь будет использован при настройке монтирования в `docker`.

4. В файл `default.conf` в раздел настроек для сервиса (Delphi) добавить новый блок `location`:

```
location /rusgidro/ {
 proxy_pass http://10.3.34.27:8638/;

 proxy_redirect off;
 proxy_set_header Host $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;

 auth_basic "Close SOAP!";
 auth_basic_user_file /etc/nginx/conf.d/.htpasswd;
}
```

где `rusgidro` - логин предприятия для обмена по SOAP,

`http://10.3.34.27:8638/` - ip и http порт экземпляра.

5. В файл `docker-compose.yml` в раздел `volumes` для сервиса `nginx` добавить строку маппинга, например:

```
- ./nginx-config/conf.d/.htpasswd:/etc/nginx/conf.d/.htpasswd
```

6. Если необходимо добавить ещё одного пользователя в существующий файл, используется команда `htpasswd` без ключа `-c`:

```
bash
```

```
htpasswd <путь_до_файла>/.htpasswd <новый_пользователь>
```

Пример:

```
bash
```

```
htpasswd ./nginx-config/conf.d/.htpasswd user2
```

**Важно:** При добавлении нового пользователя не требуется создавать отдельный блок `location` в файле `default.conf`. Все пользователи, перечисленные в файле `.htpasswd`, имеют доступ к одним и тем же защищённым `location`. Ключ `-c` используется только

при создании нового файла — применение его при добавлении пользователя приведёт к удалению всех существующих записей.

- После внесения всех изменений необходимо перезапустить контейнеры:

```
bash
```

```
docker-compose down
```

```
docker-compose up -d
```

Или, если изменялась только конфигурация nginx:

```
bash
```

```
docker-compose restart nginx
```

- В Интерфейсе оборудования адрес SOAP для предприятия будет выглядеть следующим образом (Рисунок 11.13):

The screenshot shows a configuration window titled 'Принадлежность к задаче' (Task Affiliation). It contains two sections, each with a checked checkbox and a dropdown menu. The first section is for 'ПК Заявки' (Request PC) with format 'XML'. The second section is for 'Планы ремонтов' (Repair Plans) with format 'XML\_RP'. Both sections have a 'SOAP' checkbox checked and a table of parameters.

Параметр	Значение
URL веб-сервиса	https://10.3.34.27:500/rusgidro/SOAP
Логин	asureo
Пароль	*****
EMAIL	

Параметр	Значение
URL веб-сервиса	https://10.3.34.27:500/rusgidro/SOAP?SubscriberId=РусГидро
Логин	asureo
Пароль	*****
EMAIL	

Рисунок 11.13 – Отображение адреса SOAP

## 11.10 Настройка Kerberos авторизации для Системы

### 11.10.1 Общие сведения

В случае необходимости использования доменной авторизации в Системе на ОС Linux используется Kerberos авторизация, требующая помимо ввода сервера в домен дополнительной настройки.

### 11.10.2 Ввод в домен

- Ввести сервер для СП в домен Active Directory с помощью **astra-ad-sssd-client** (для использования необходимо установить соответствующий пакет)
- Убедиться, что сервер введен в домен корректно. Для проверки успешности ввода в домен можно выполнить следующие команды:

Получить билет Kerberos от имени администратора домена:

---

```
kinit admin@dc01.example.com
```

Проверить статус подключения: `sudo astra-ad-sssd-client -i`

Вывод команды будет примерно следующим: *Обнаружен настроенный клиент в домене example.com.* Это говорит, что сервер получил информацию о текущем домене.

### 11.10.3 Настройка доменной авторизации для .Delphi

После успешного ввода сервера в домен в `/etc/` должны появиться файлы `krb5.conf` и `krb5.keytab`. Необходимо проверить, что в файле `/etc/krb5.conf` находится актуальная информация о домене, в файле `/etc/hosts` должны быть указаны контроллер(ы) домена.

В `docker-compose.yml` необходимо раскомментировать или добавить маппинг этих файлов в контейнер `.Delphi` в секцию `volumes`:

- `/etc/krb5.keytab:/etc/krb5.keytab`
- `/etc/krb5.conf:/etc/krb5.conf`

На этом настройка окончена. После установки и запуска СП необходимо настроить учетные записи под доменные.

### 11.10.4 Настройка доменной авторизации для веб-версии Системы

Для организации доменной авторизации также в веб-версии Системы необходимо организовать SPN для данного сервиса, а также сформировать `spnego.keytab`.

На контроллере домена Windows создать учетную запись AD именно для того хостового компьютера, на котором будет развернут `nginx` в составе Системы с параметрами (при работе в кластере учетная запись AD создается для общего имени кластера и используется на обоих узлах):

- пользователь не может менять пароль (User cannot change password);
- пароль никогда не устаревает (Password never expires);

В консоли контроллера домена создать `keytab`-файл следующей командой:

```
ktpass /princ HTTP/full_server_name@DOMAIN.LOCAL /mapuser spnego@DOMAIN.LOCAL
/crypto ALL /ptype KRB5_NT_PRINCIPAL /out C:\spnego.keytab /pass <пароль_учётной_записи>
```

где:

- `full_server_name` — полное имя сервера с учетом домена, например, `vmzvk-host.domain.local` — т.е. с указанием домена после имени компьютера;
- `DOMAIN.LOCAL` — наш домен;

- 
- `spnego@DOMAIN.LOCAL` — учетная запись в AD для выполнения запросов (которую ранее создали на контроллере домена);
  - `pass` — пароль, который будет задан пользователю (должен соответствовать требованию AD). Система запросит его ввод дважды.

Учетная запись в AD должна быть размещена по пути, в котором присутствуют названия только на латинице. Подразделения и контейнеры не должны быть на кириллице. В противном случае, при выполнении команды выше мы получим ошибку «Password set failed! 0x00000020».

Готовый `keytab`-файл необходим для контейнера `.Net`, поэтому нужно перенести его на сервер, например, по пути `/etc/spnego.keytab`, а также добавить `mapping` данного файла в контейнер `.Net` в секцию `volumes`.

- `/etc/spnego.keytab:/etc/krb5.keytab`

Также требуется дополнительная настройка самого сервера `.Net`. В том числе указание необходимости доменной авторизации, уникальный идентификатор (SPN), домен и его возможные алиасы. Всё это может быть настроено с помощью конфигулятора после установки самого комплекса. Более подробно см. в пункте 12.5.3 данного руководства.

### **11.10.5 Настройка клиентов для доменной авторизации в веб-версии Системы**

Для веб-версии Системы возможна доменная авторизация двух видов:

- Непрозрачная;
- Сквозная.

В случае непрозрачной авторизации клиенту будет предложено ввести NT-логин и пароль. При этом логин вводится в следующем виде `login@domain.local` (Рисунок 11.14)

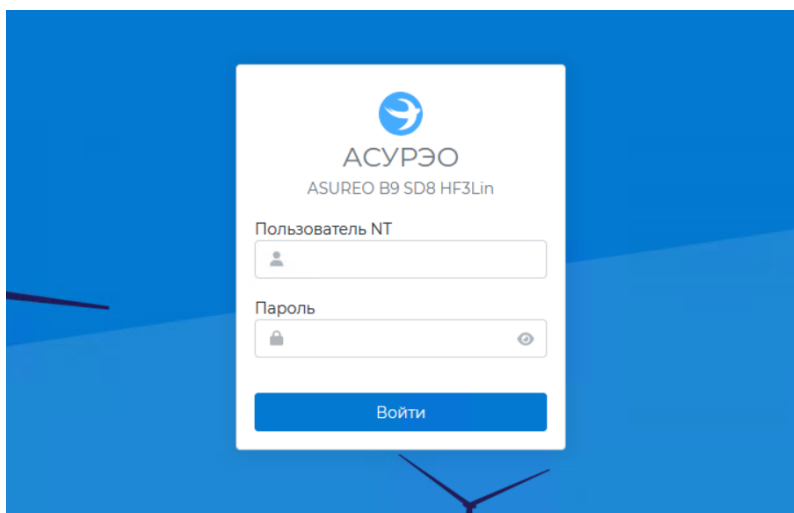


Рисунок 11.14 – Непрозрачная авторизация

После ввода данных сервер пытается авторизоваться под этими данными на KDC и получить билет для доступа к данному SPN. После чего проверяет билет и авторизовывает пользователя в системе

Сквозная же авторизация не требует никакого ввода дополнительных данных. Клиент сам получает билет на доступ к SPN веб-версии Системы, после чего отправляет его серверу, и после проверки билета сервер авторизовывает пользователя

Непрозрачная авторизация будет использоваться всегда, когда недоступна прозрачная. При этом для прозрачной авторизации необходимо несколько дополнительных условий:

- возможность распознать доменное имя пользователя по его ip-адресу (например, через обратную зону просмотра DNS);
- доверие к данному серверу со стороны ОС и браузера клиента (также доверие может быть ограничено другими средствами безопасности).

Стандартные настройки и политики со стороны браузера клиента описаны в разделе «5.4.5 Настройка доверенных сайтов». В случае же наложения дополнительных ограничений в связи с политиками безопасности по вопросам организации сквозной авторизации необходимо консультироваться со специалистами информационной безопасности вашей организации.

## 11.11 Установка и настройка СУБД на ОС семейства Linux

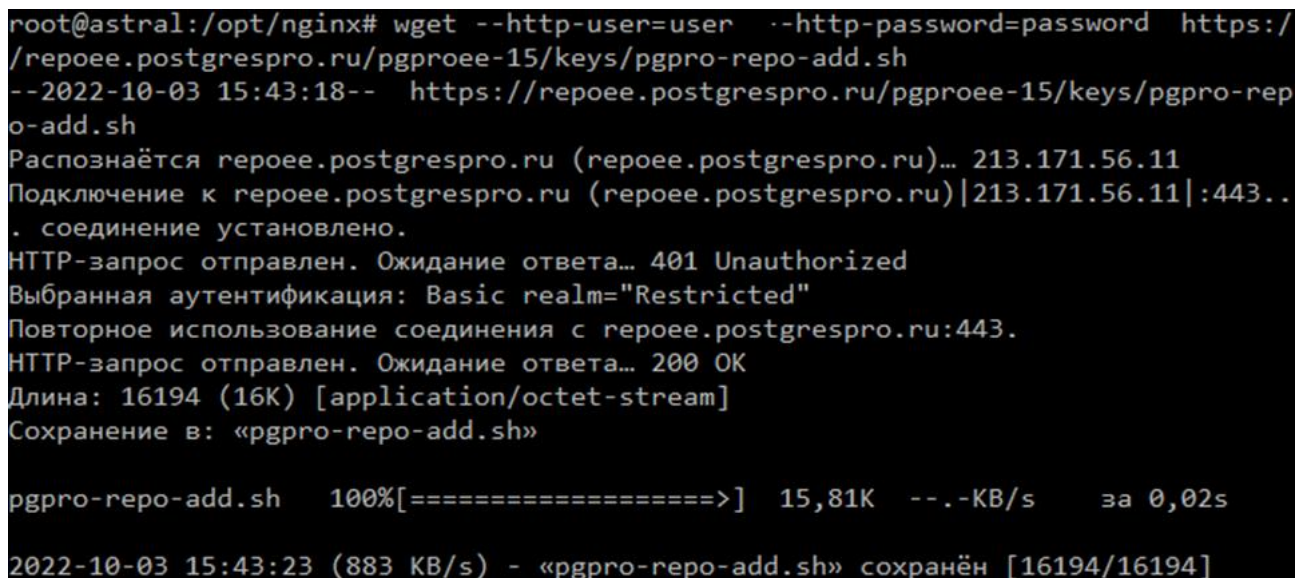
### 11.11.1 Установка СУБД на ОС семейства Linux

Для хранения данных в Системе 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://repoe.postgrespro.ru/pgproee-15/keys/pgpro-repo-add.sh` (Рисунок 11.15).



```
root@astral:/opt/nginx# wget --http-user=user --http-password=password https://repoe.postgrespro.ru/pgproee-15/keys/pgpro-repo-add.sh
--2022-10-03 15:43:18-- https://repoe.postgrespro.ru/pgproee-15/keys/pgpro-repo-add.sh
Распознаётся repoe.postgrespro.ru (repoe.postgrespro.ru)... 213.171.56.11
Подключение к repoe.postgrespro.ru (repoe.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 repoe.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 11.15 – Выполнение команды `wget - -http-user=user - -http-password=password https://repoe.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 11.16).

```

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

Ошибка аутентификации пользователя/пароля.
Repository https://repoe.e.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://repoe.e.postgrespro.ru/pgproee-15/astra-smolensk
/1.7/dists/1.7_x86-64/main/binary-amd64/Release
Распознаётся repoe.e.postgrespro.ru (repoe.e.postgrespro.ru)... 213.171.56.11
Подключение к repoe.e.postgrespro.ru (repoe.e.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 repoe.e.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/repoe.e.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 АПТ смог распознать данный CD-ROM. apt-get update
не используется для добавления новых CD-ROM
Пол:3 https://repoe.e.postgrespro.ru/pgproee-15/astra-smolensk/1.7 1.7_x86-64 InR

```

Рисунок 11.16 – 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 pgproee-15.list расположенный по пути /etc/apt/sources.list.d и в явном виде указать учётные данные подключения к репозиторию (Рисунок 11.17).

```

GNU nano 3.2 /etc/apt/sources.list.d/pgproee-15.list Изменён
Repository for 'PostgresPro Enterprise'
deb https://YOURLOGIN:YOURPASS@repoe.e.postgrespro.ru/pgproee-12/astra-smolensk/1.7 1.7_x86$

```

Рисунок 11.17 – Указание учетных данных подключения к репозиторию

4. Запустить установку СУБД postgrespro-ent-15, выполнив команду:

`apt-get install postgrespro-ent-15` (Рисунок 11.18).

```

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 пакетов,
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/ap
t/sources.list:6 и в /etc/apt/sources.list:7

```

Рисунок 11.18 – Выполнение команды apt-get install postgrespro-ent-15

При окончании установки также в автоматическом режиме будет произведена инициализация базы данных (Рисунок 11.19).

```

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
Initializing 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 11.19 – Инициализация базы данных

5. Проверить, что СУБД в активном режиме, выполнив команду:

`systemctl status postgrespro-ent-15.service` (Рисунок 11.20).

```

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 11.20 – Выполнение команды проверки статуса СУБД

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

6.1 Перейти на учётную запись postgres и войти в консоль psql, выполнив команду:

`su postgres` (Рисунок 11.21).

```

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

postgres=# █

```

Рисунок 11.21 – Выполнение команды su postgres

6.2 Задать пароль, выполнив команду:

`ALTER USER postgres WITH PASSWORD 'SecretPass';` (Рисунок 11.22),

где ‘SecretPass’ – новый пароль, который необходимо задать.

```

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

```

Рисунок 11.22 – Выполнение команды задания пароля

Для выхода из консоли psql необходимо ввести команду: `\q`

### 11.11.2 Настройка СУБД на ОС семейства Linux

Если сервер приложений расположен не на том же самом компьютере, что и СУБД, 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 11.23).

```
#-----
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 = '' # comma-separated list of directories
 # (change requires restart)
```

Рисунок 11.23 – 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 11.24.

```
#-----
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 11.24 – 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 11.25).

```
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 11.25 – Указание IP

3. В основном файле конфигурации postgresql.conf, который расположен по пути /var/lib/pgpro/ ent-15/data задать региональные настройки, соответствующие локали ru\_RU. Установить следующие параметры:

- datestyle = 'iso, dMY' – гарантирует корректное отображение и обработку дат в формате «День-Месяц-Год».
- timezone = 'Europe/Moscow' – устанавливает правильную временную зону для всех операций с датой и временем.

Для полного соответствия региональным стандартам также рекомендуется установить следующие параметры локали:

*# Дополнительные рекомендуемые параметры локали*

*lc\_messages = 'ru\_RU.UTF-8' # Локализация системных сообщений об ошибках*

*lc\_monetary = 'ru\_RU.UTF-8' # Локализация форматирования денежных единиц (руб.)*

*lc\_numeric = 'ru\_RU.UTF-8' # Локализация форматирования чисел (разделитель дробной части - запятая)*

*lc\_time = 'ru\_RU.UTF-8' # Локализация названий дней недели и месяцев*

**Примечание:** Для применения этих настроек необходимо, чтобы локаль ru\_RU.UTF-8 была сгенерирована в операционной системе сервера баз данных. Проверить список доступных локалей можно командой: *locale -a*.

4. Перезапустить сервис postgrespro-ent-15.service, выполнив команду:

```
systemctl restart postgrespro-ent-15.service.
```

## 11.12 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.

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`

---

## 12 Установка и первоначальная настройка Системы

### 12.1 Создание и настройка БД MS SQL

#### 12.1.1 Создание базы данных

Перед установкой ПК на сервере баз данных MS SQL Server должна быть создана база данных, создана учетная запись пользователя (см. раздел «12.1.2 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 «12.1.3 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 12.1).

**Внимание!** Не допускается использование специальных символов в именах БД.

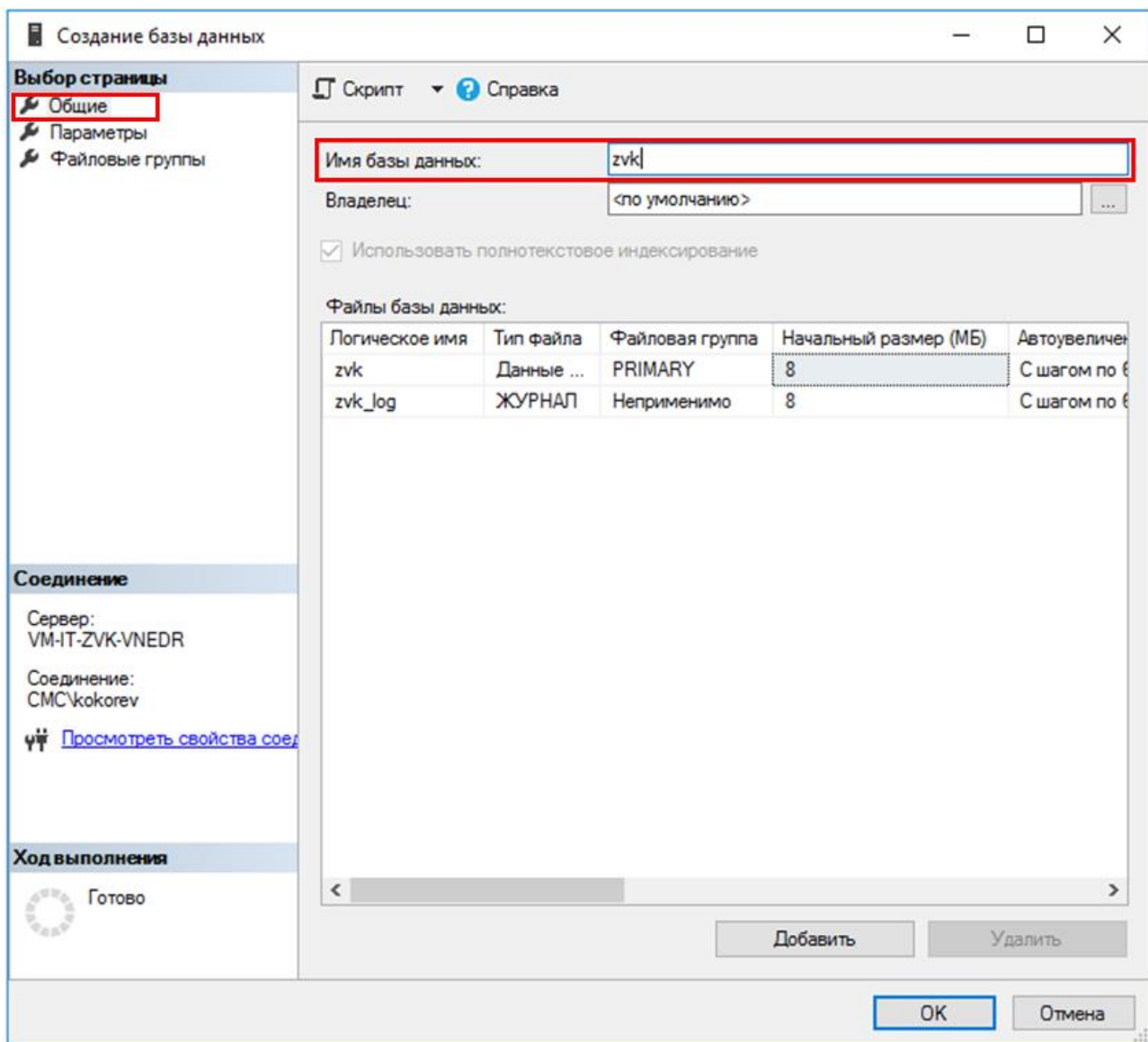


Рисунок 12.1 – Указание имя БД

3. На вкладке «*Параметры*» (*Options*) для элемента «*Параметры сортировки*» (Collation name) установить значение «Cyrillic\_General\_CI\_AS» (Рисунок 12.2).

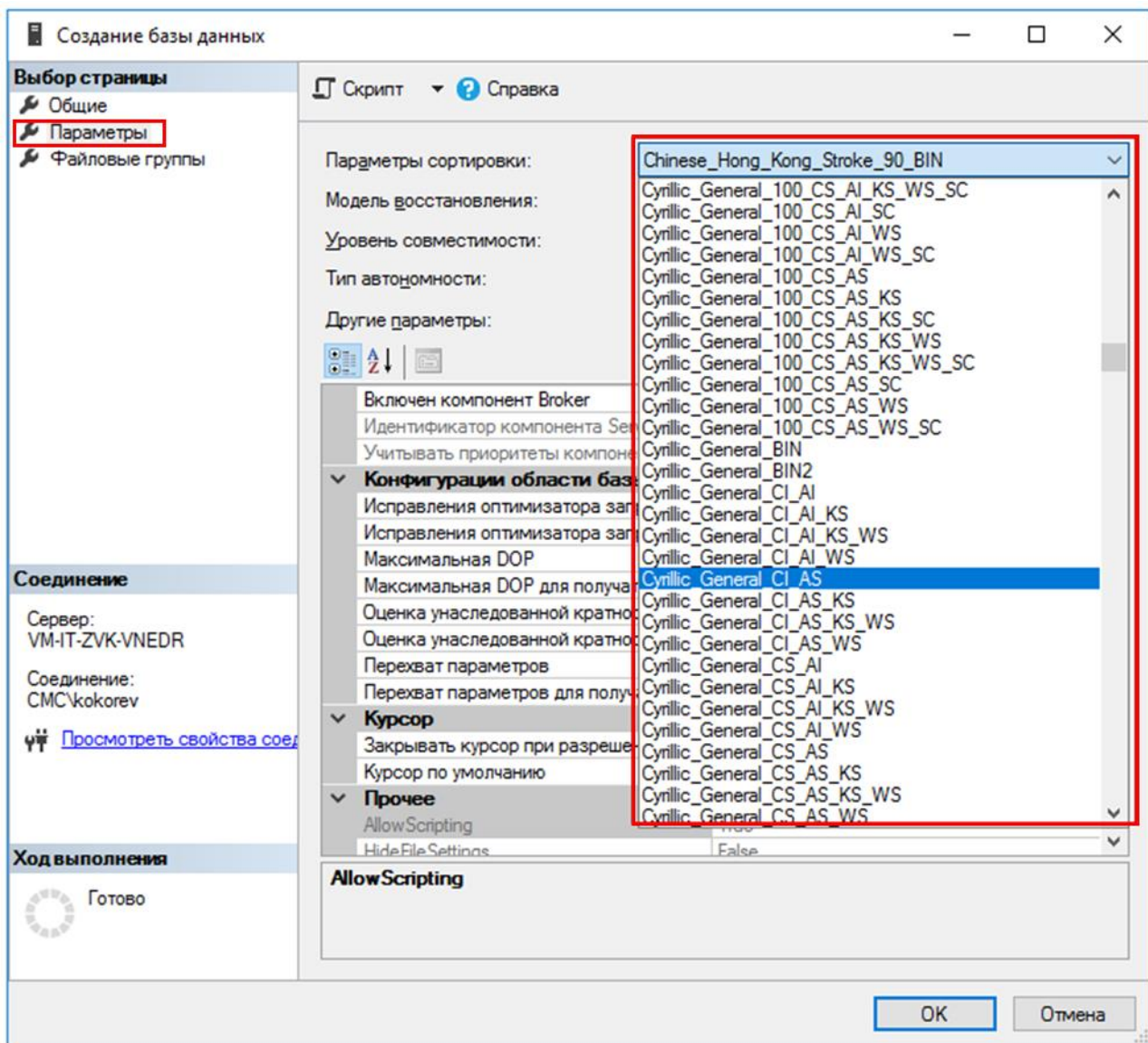


Рисунок 12.2 – Значение Cyrillic\_General\_CI\_AS для элемента «Параметры сортировки» (Collation name)

4. На вкладке «Параметры» (Options) для элемента «Модель восстановления» (Recovery Model) установить значение «Полная» (Full) (Рисунок 12.3).

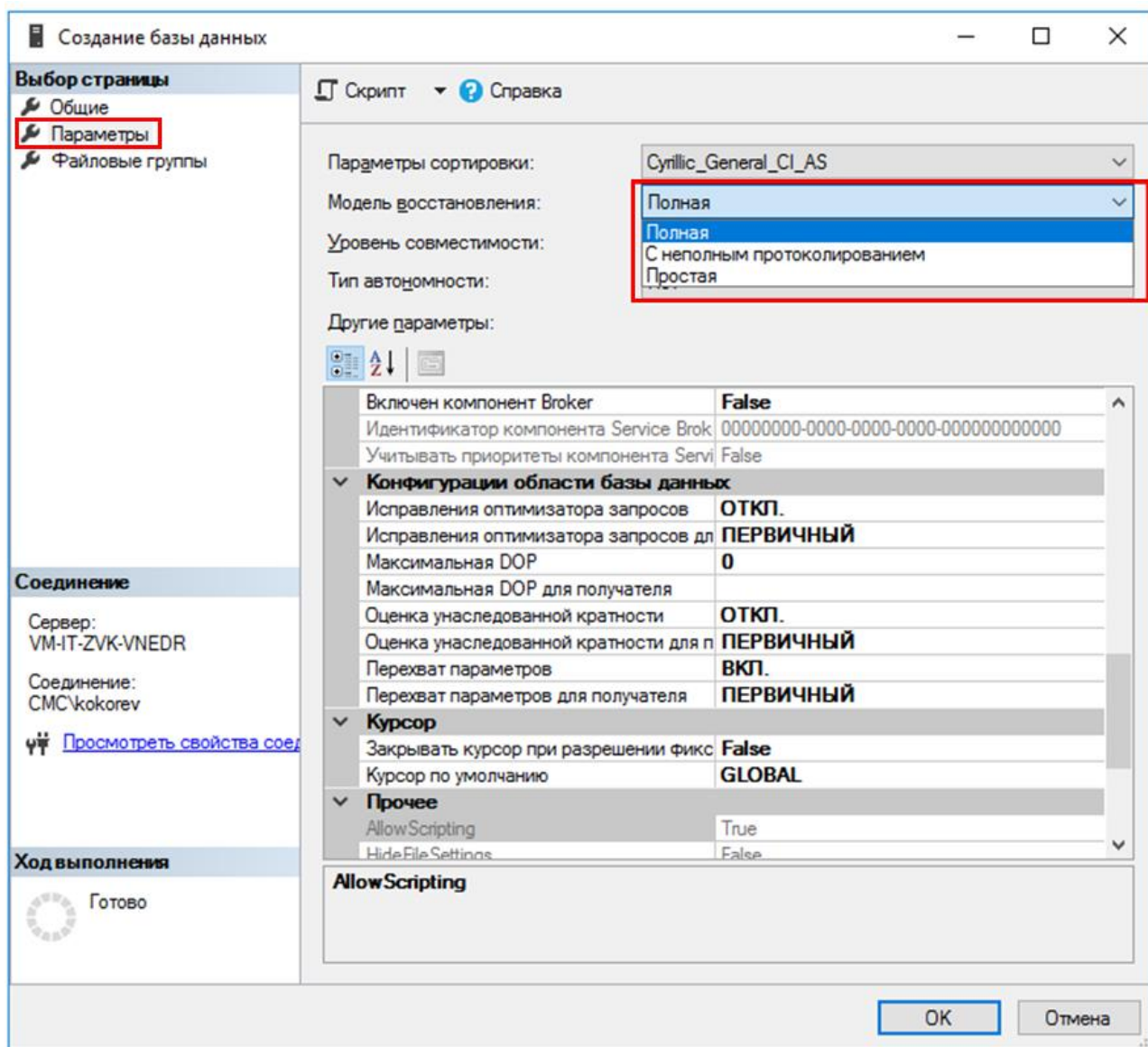


Рисунок 12.3 – Значение *Cyrillic\_General\_CI\_AS* для элемента «Модель восстановления» (*Recovery Model*)

### 12.1.2 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 12.4). Также следует указать созданную ранее базу данных в качестве базы данных по умолчанию для этого пользователя.

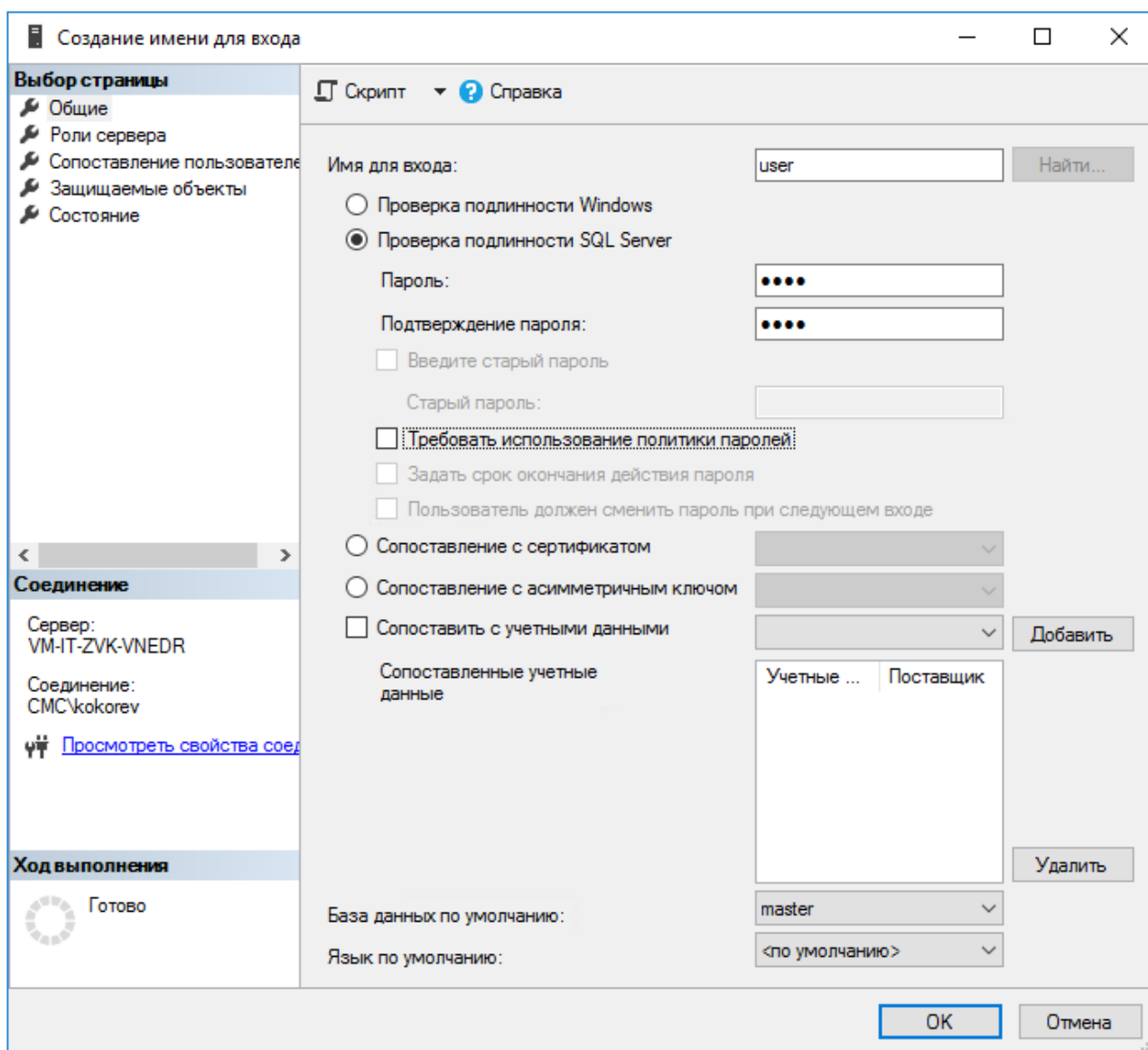


Рисунок 12.4 – Создание учетной записи пользователя

### 12.1.3 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 12.5).

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

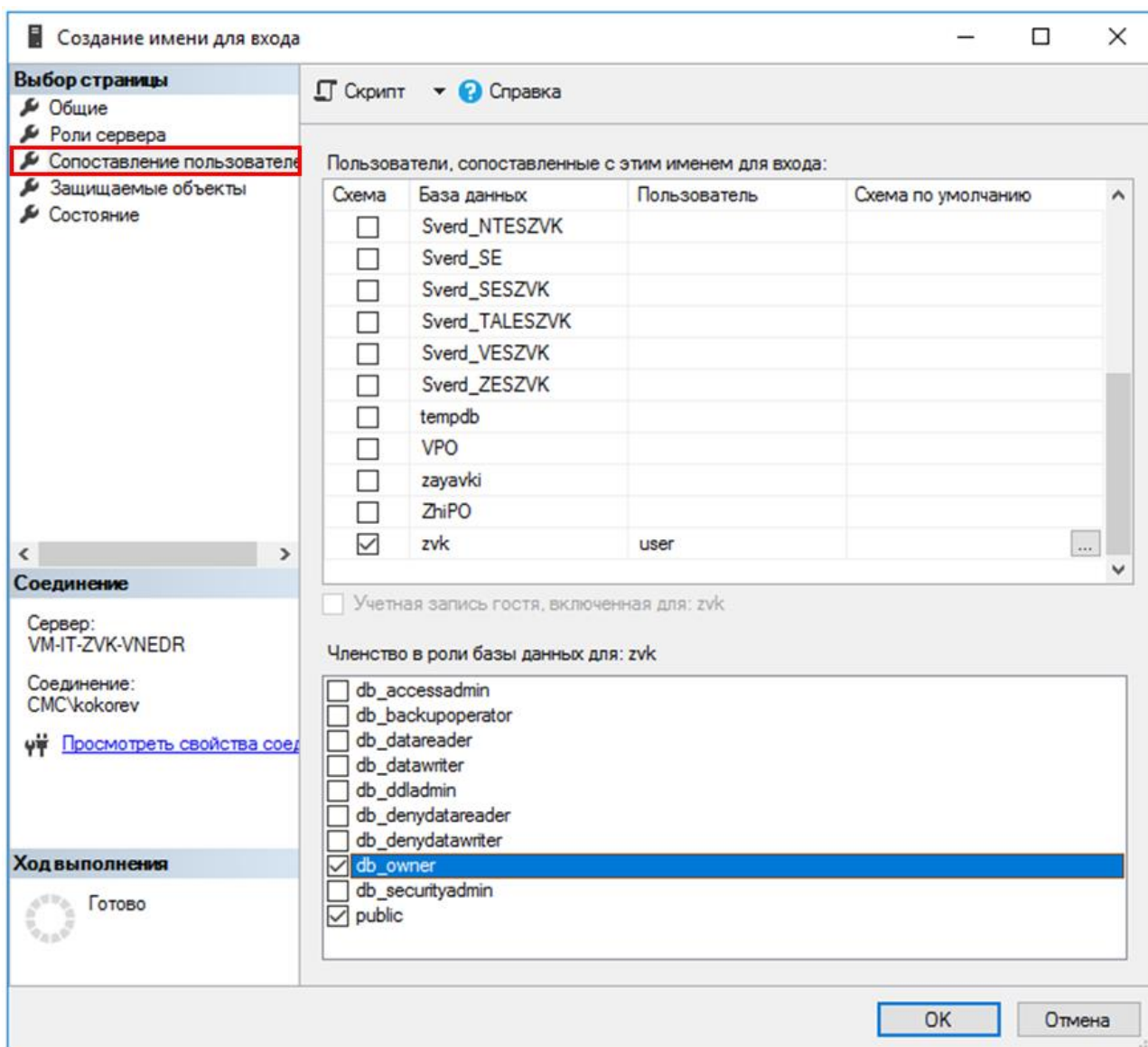


Рисунок 12.5 – Настройка прав учетной записи пользователя

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 12.6).

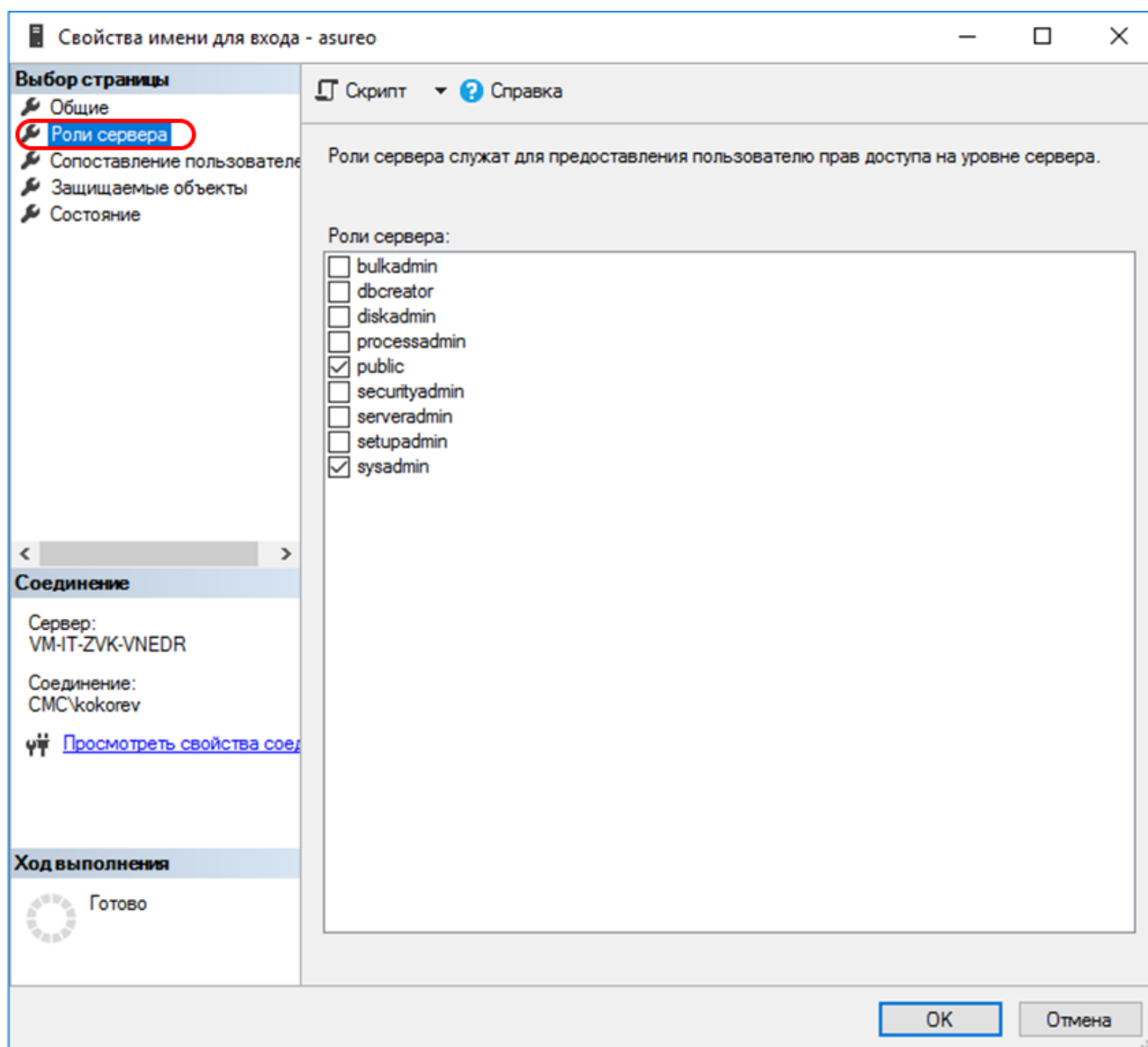


Рисунок 12.6 – Назначение роли sysadmin в разделе «Роли сервера»

## 12.2 Создание БД PostgreSQL

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

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

### 12.2.1 Создание БД с использованием «SQL Shell (psql) в MS Windows»

Для создания базы данных в PostgreSQL на сервере БД, предназначенном для развертывания Системы на ОС MS Windows 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 zvktest;») нажать «Enter». Далее в строке postgres=# ввести «\l» нажать «Enter» (Рисунок 12.7).

**Внимание!** Не допускается использование специальных символов в именах БД.

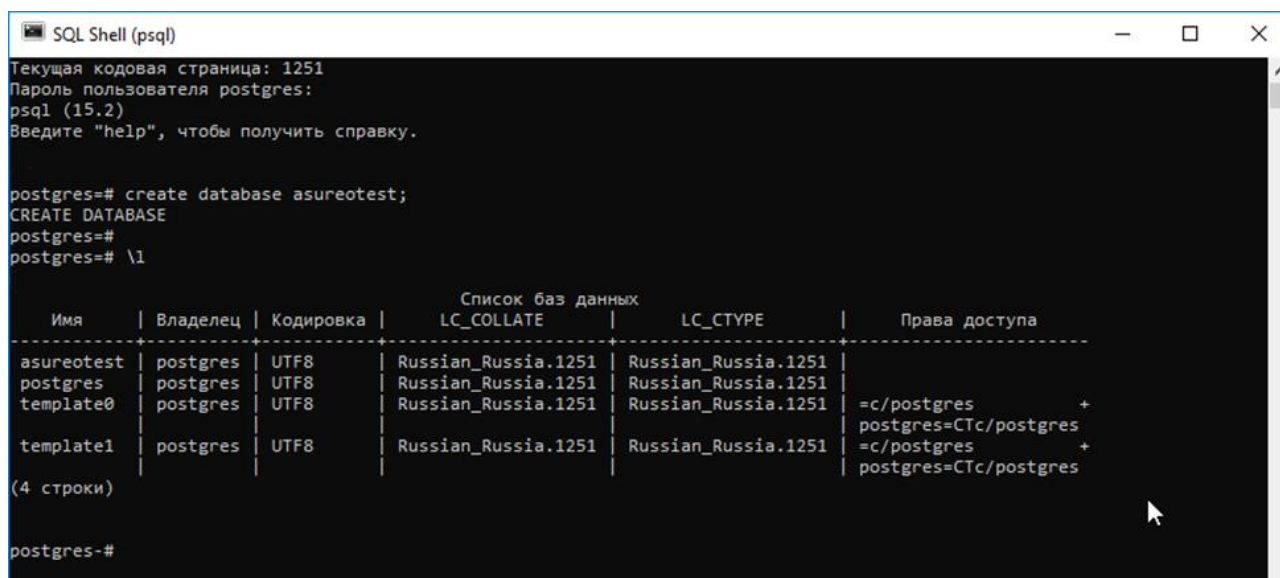


Рисунок 12.7 – Создание новой БД

## 12.2.2 Создание БД с использованием «SQL Shell (psql) в Linux»

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

1. Войти в psql под пользователем postgres. Если команды вводятся прямо на сервере СУБД, то ввести:

```
sudo -u postgres psql
```

Если же БД создаётся с удалённого хоста, на котором установлен клиент postgres, то необходимо ввести команду

```
psql -U postgres -h <ip адрес СУБД> -p <порт СУБД>
```

2. Далее в консоли необходимо вписать «create database <имя БД>» (например, «create database zvktest;») нажать «Enter». Далее в строке postgres=# ввести «\l» нажать «Enter» (Рисунок 12.8).

```
sysadmin@zvk-test:/opt/asureo$ psql -U postgres -h 192.168.1.135 -p 5432
Пароль пользователя postgres:
psql (15.12)
Введите "help", чтобы получить справку.

postgres=# create database asureotest;
CREATE DATABASE
postgres=# \l
```

Имя	Владелец	Кодировка	LC_COLLATE	LC_CTYPE	локаль	ICU	Провайдер локали	Права доступа
asureotest	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	
chelyab	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	
postgres	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	
stavropol	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	
template0	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	=c/postgres + postgres=Ctc/postgres
template1	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	=c/postgres + postgres=Ctc/postgres
test	postgres	UTF8	ru_RU.UTF-8	ru_RU.UTF-8	ru-RU		icu	

(7 строк)

```
postgres=#
```

Рисунок 12.8 – Подключение к серверу

**Внимание!** Не допускается использование специальных символов в именах БД.

3. Из контекстного меню пункта «Базы Данных» выбрать «Создать – База Данных». В открывшейся форме «Создание Базы данных» указать имя базы данных, например, ZVKTEST и нажать кнопку «Сохранить» (Рисунок 12.9).

**Внимание!** Не допускается использование специальных символов в именах БД.

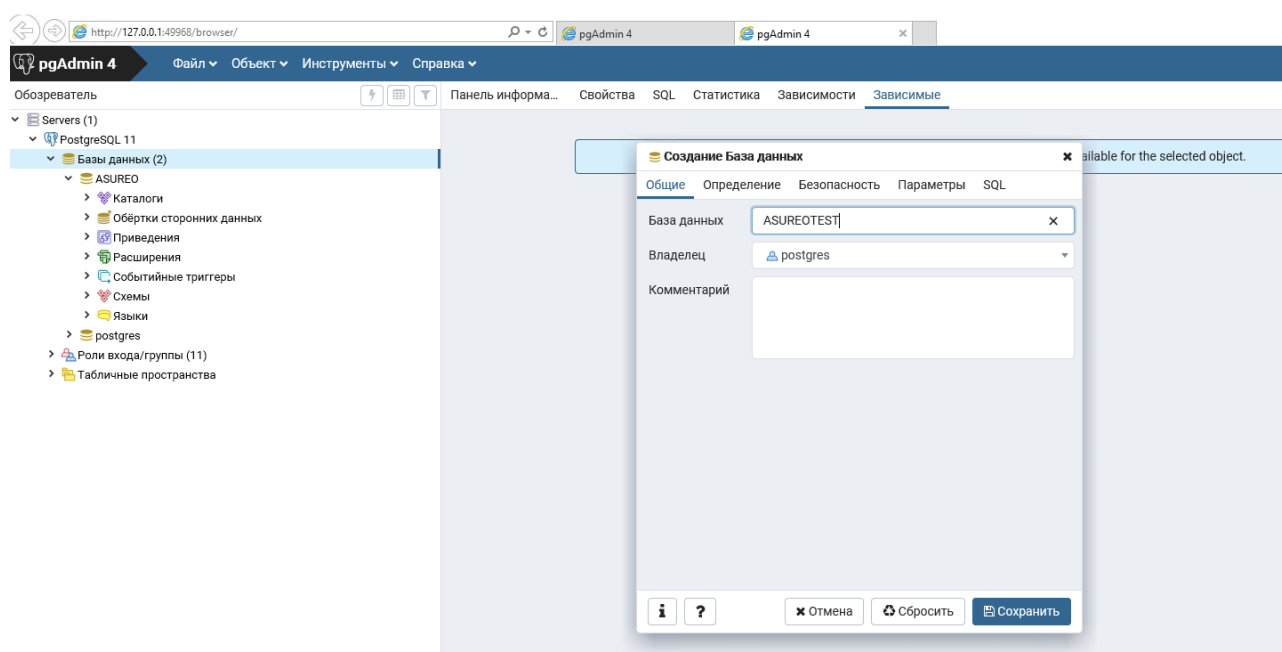


Рисунок 12.9 – Создание базы данных

### 12.2.3 Создание БД с использованием инструментария PGAdmin

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

1. В меню «Пуск» выбрать пункт «PGAdmin 4» – «PGAdmin 4 v 4». Либо же перейти по адресу PGAdmin и авторизоваться в случае, если он установлен в контейнере на сервере Linux.

2. Подключиться к серверу СУБД, указав пароль пользователя «postgres» (Рисунок 12.10), который был указан при установке СУБД (см. Рисунок 10.20).

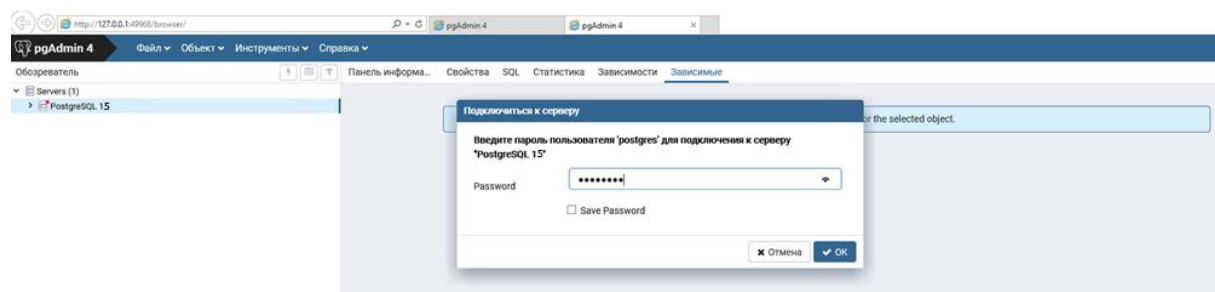


Рисунок 12.10 – Подключение к серверу

3. Из контекстного меню пункта «Базы Данных» выбрать «Создать – База Данных». В открывшейся форме «Создание Базы данных» указать имя базы данных, например, ZVKTEST и нажать кнопку «Сохранить» (Рисунок 12.13).

**Внимание!** Не допускается использование специальных символов в именах БД.

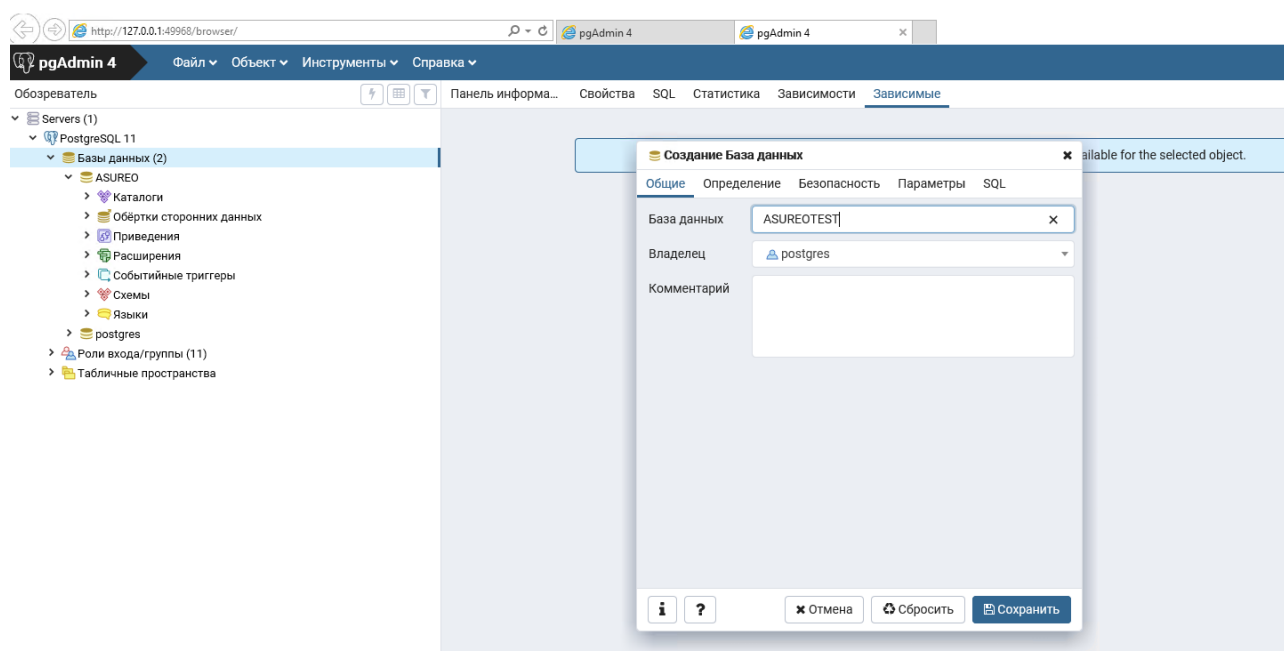


Рисунок 12.11 – Создание базы данных

#### 12.2.4 Создание учетной записи пользователя в инструментарии PGAdmin

При создании учетной записи пользователя, подключающегося к БД, в диалоговом окне «Роль входа» на вкладке «Права» необходимо создать пользователя отличного от postgres без права «Superuser» (Рисунок 12.12).

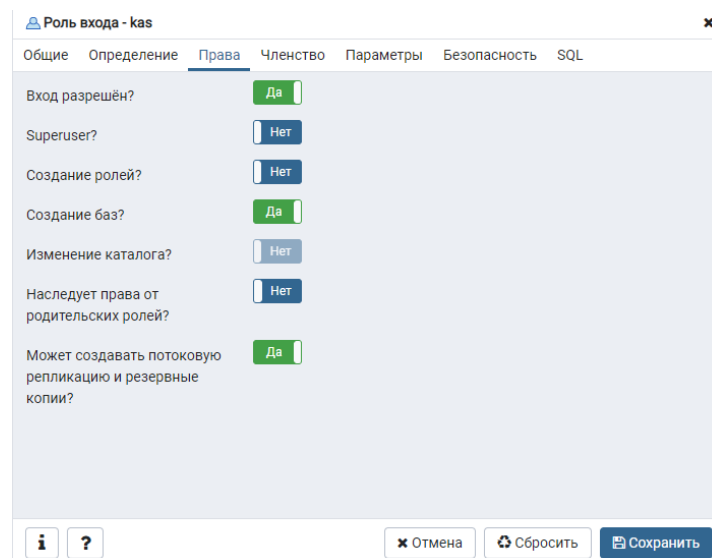


Рисунок 12.12 – Создание пользователя отличного от postgres без права «Superuser»

### 12.2.5 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 12.13).

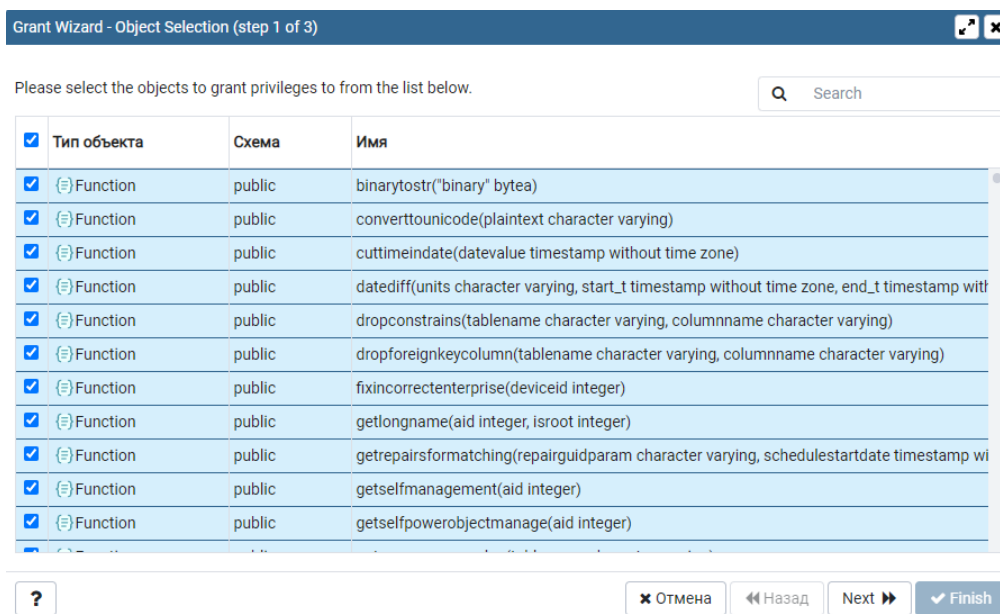


Рисунок 12.13 – Мастер назначения прав

Далее для пользователя, созданного в разделе «12.2.4 Создание учетной записи пользователя в инструментарии PGAdmin», необходимо добавить субъект и выбрать все права (Рисунок 12.14).

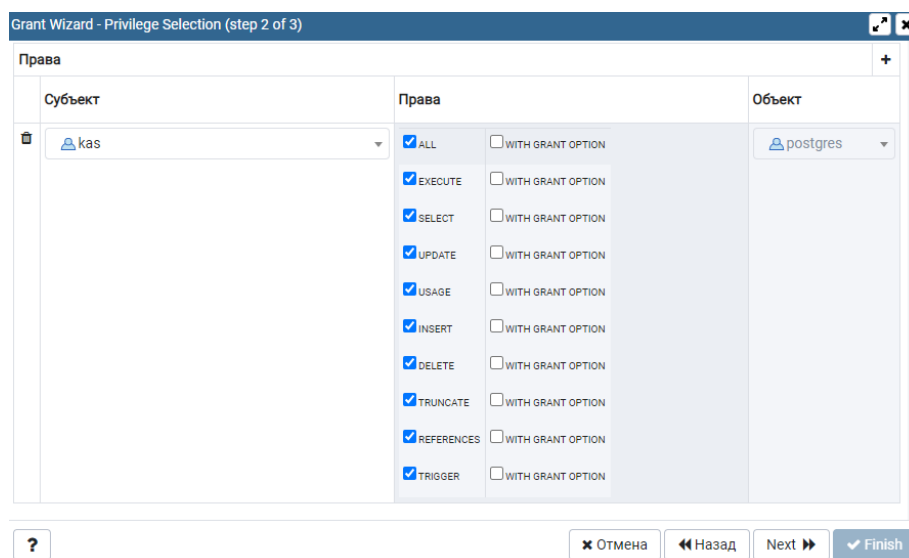


Рисунок 12.14 – Добавление субъекта

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

**Внимание!** При обновлении ПК необходимо включить для пользователя опцию «Superuser» (Рисунок 12.15). После завершения обновления опция должна быть выключена.

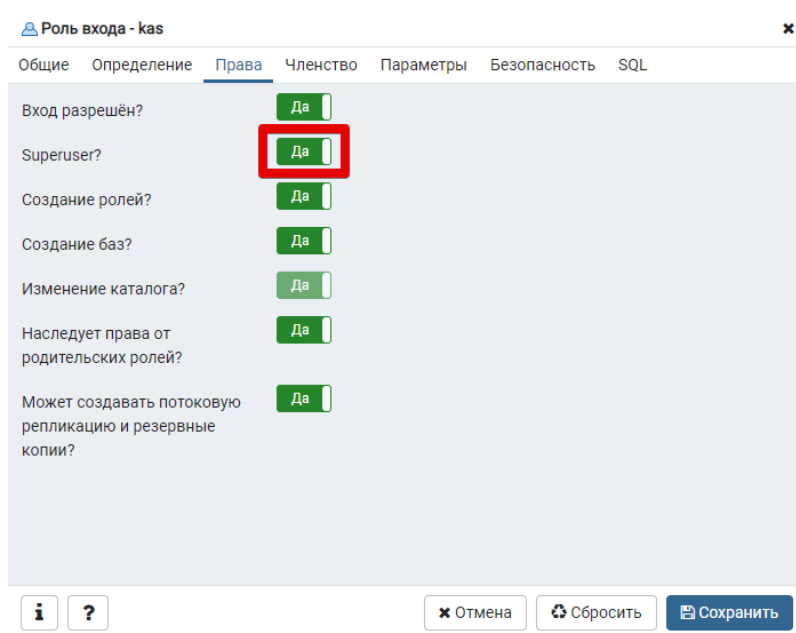


Рисунок 12.15 – Включение опции «superuser»

## 12.3 Установка Системы на СУБД MSSQL/PostgreSQL на ОС Windows

**Внимание!** При установке Системы на СУБД PostgreSQL на ОС Windows необходимо включить для пользователя опцию «Superuser». Для СУБД MS SQL Server также рекомендуется для пользователя включить роль «sysadmin». После завершения установки опция должна быть выключена.

Установка Системы осуществляется с помощью установщика дистрибутива, что позволяет вводить необходимую информацию пошагово (Рисунок 12.16). Для открытия установщика необходимо запустить под правами администратора файл «Setup.exe» из каталога «install» установочного диска ПК.

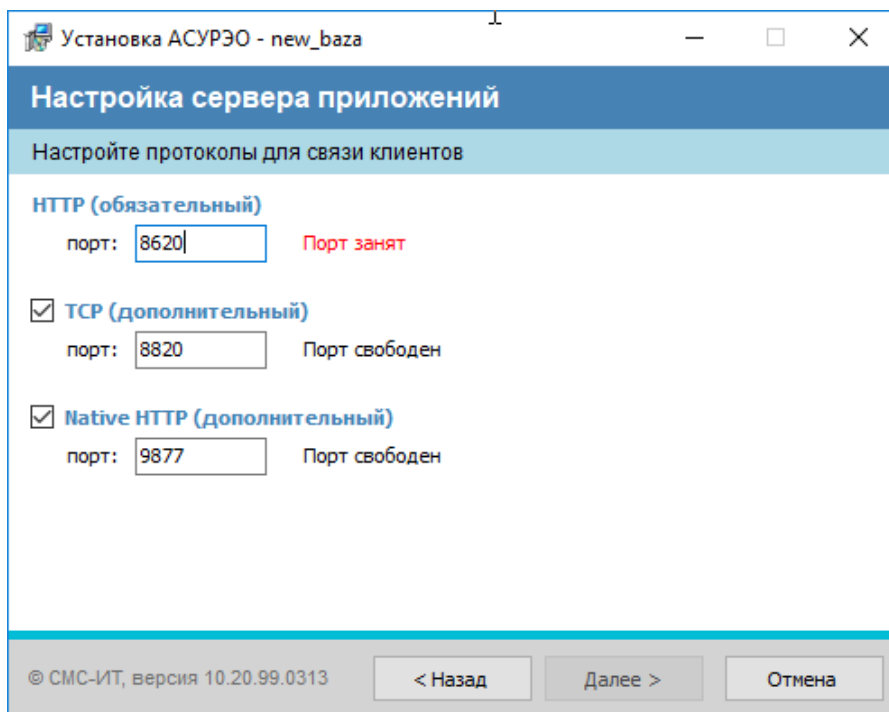


Рисунок 12.16 – Мастер установки

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 12.17).

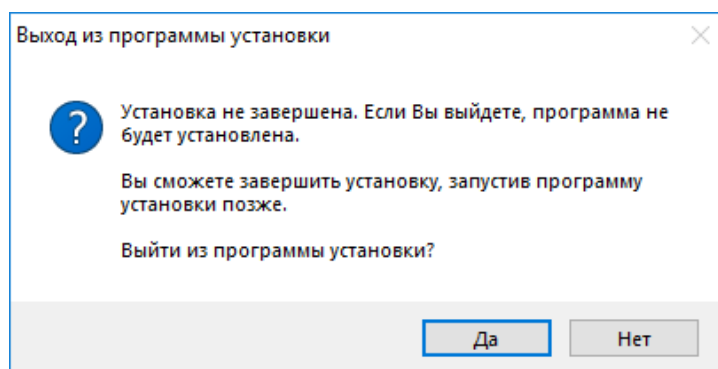


Рисунок 12.17 – Подтверждение отмены установки

В стартовом окне установщика «*Выбор производимых действий*» необходимо выбрать одно из действий (Рисунок 12.18):

- «**Новый экземпляр**». Для установки нового экземпляра.
- «**Обновить экземпляры**». Для обновления экземпляров, уже существующих на сервере (см. раздел «12.10 Обновление на ОС MS Windows»).
- «**Удалить экземпляры**». Для удаления установленных экземпляров.

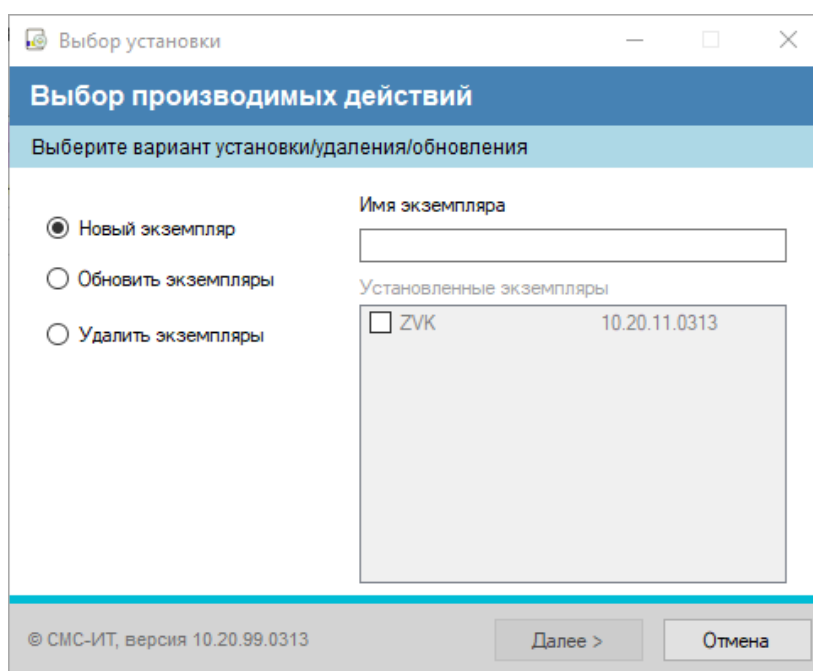


Рисунок 12.18 – Стартовое окно мастера установки

### 12.3.1 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 12.19).

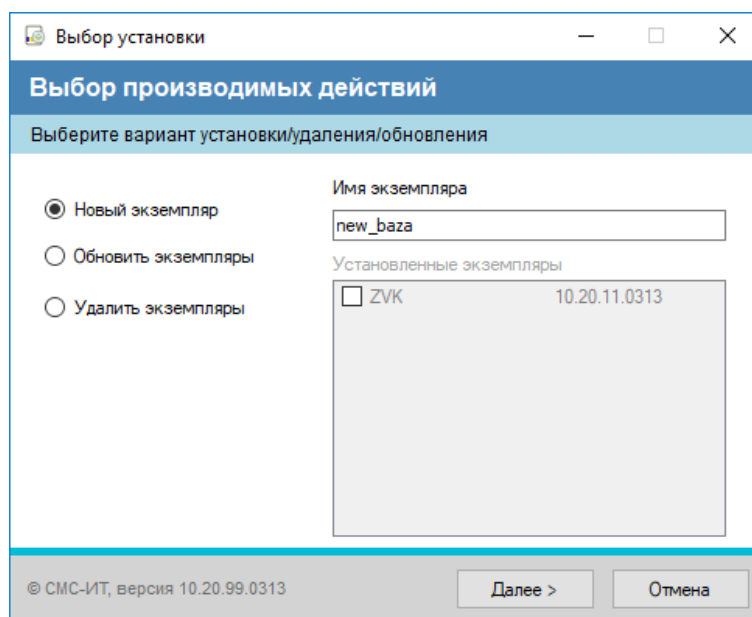


Рисунок 12.19 – Ввод имени экземпляра

При нажатии на кнопку «Далее >» открывается шаг «Проверки системных требований» (Рисунок 12.20).

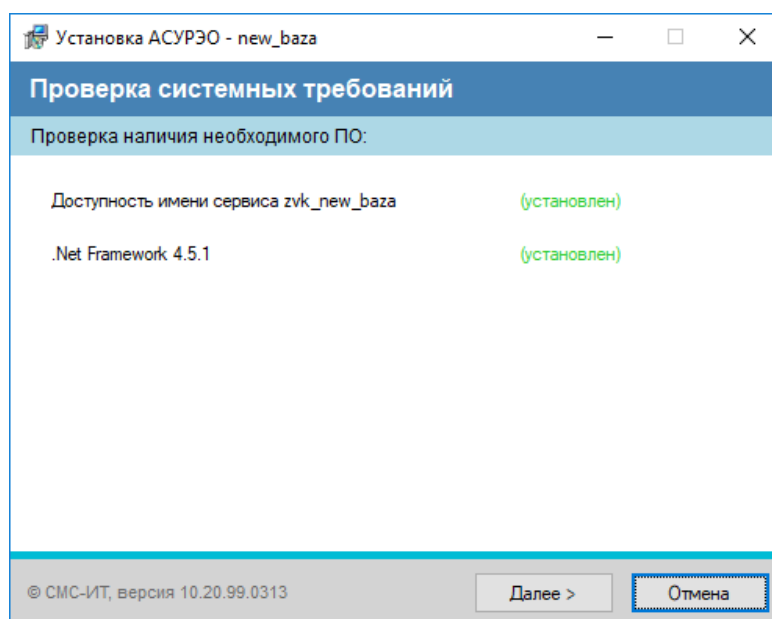


Рисунок 12.20 – Проверка системных требований

При установке первого экземпляра ПК в окне мастера «Выбор папки установки» (Рисунок 12.21) 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.).

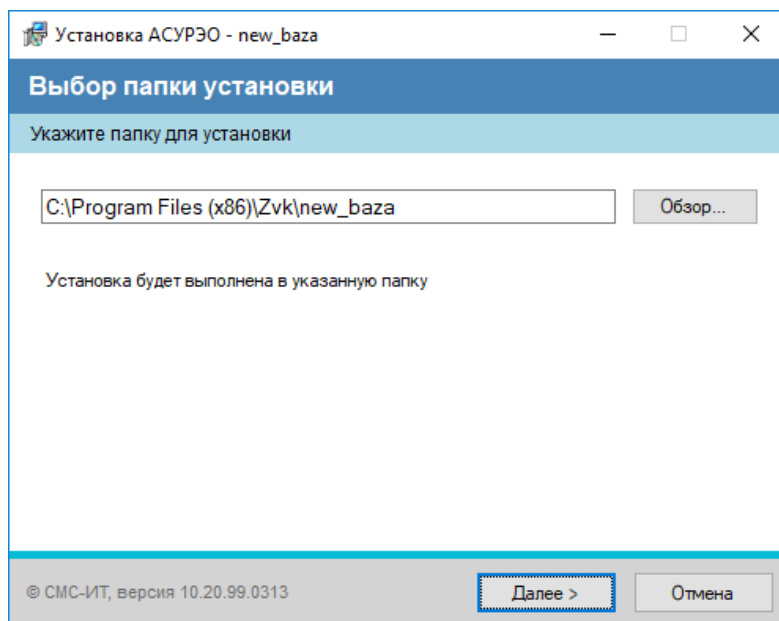


Рисунок 12.21 – Выбор папки установки

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

### 12.3.2 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 12.22).

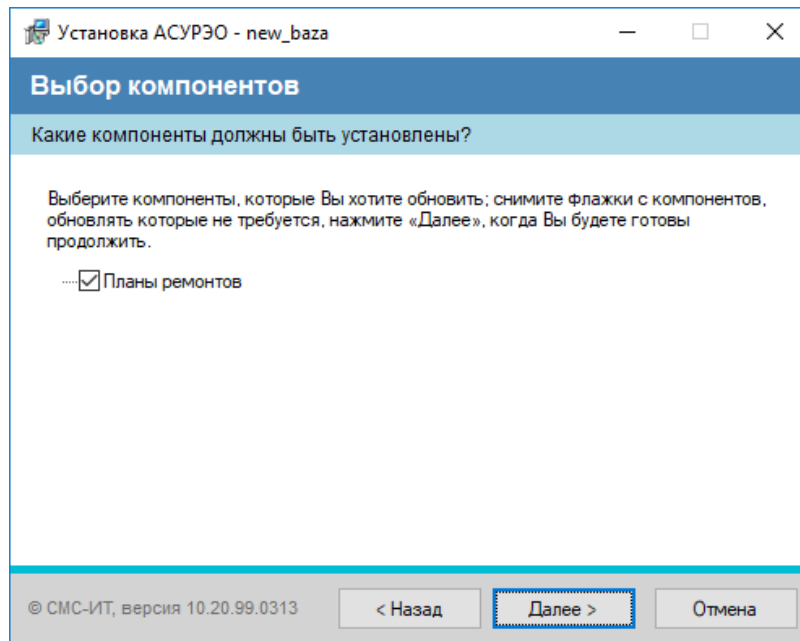


Рисунок 12.22 – Выбор компонентов

### 12.3.3 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 12.23).

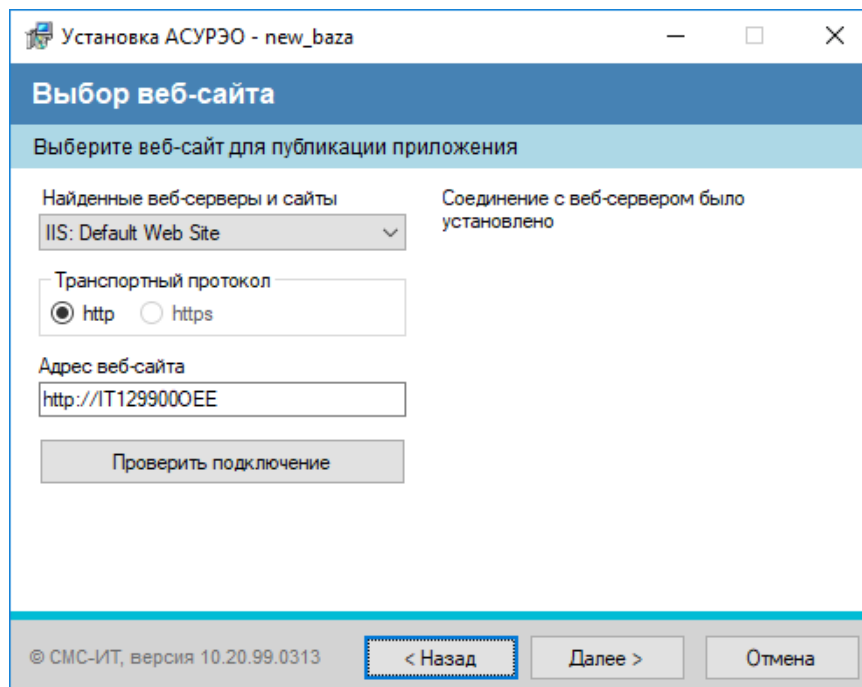


Рисунок 12.23 – Выбор версии веб-сервера

**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 12.24).

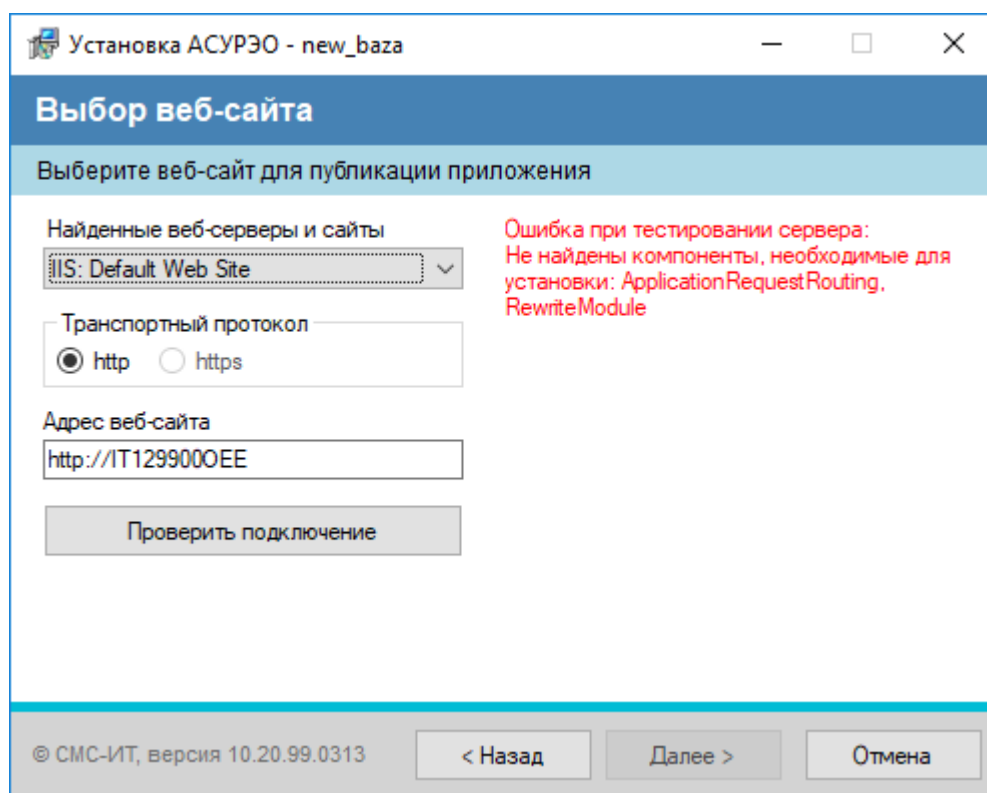


Рисунок 12.24 – Установка дополнительных компонентов IIS

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](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](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](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](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».

### 12.3.4 Настройка сервера приложений

На данном шаге производится настройка протоколов для связи с клиентами (Рисунок 12.25). 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.

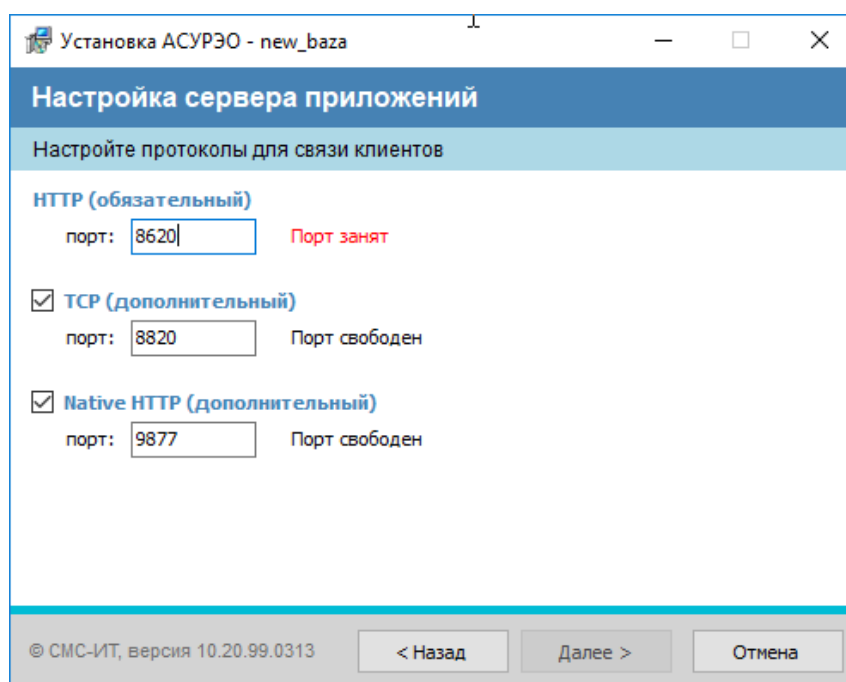


Рисунок 12.25 – Настройка протоколов для связи клиентов

Мастер установки автоматически проверяет, занят ли указанный порт (например, другим экземпляром), и выводит соответствующее сообщение напротив поля ввода номера порта (Рисунок 12.25). Кнопка «Далее >» становится активной, если все указанные порты свободны (Рисунок 12.26).

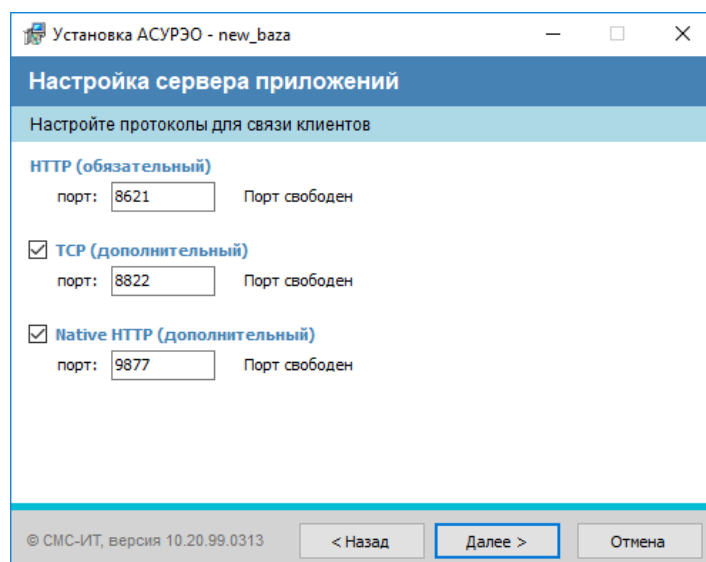


Рисунок 12.26 – Проверка портов

**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 12.27).

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

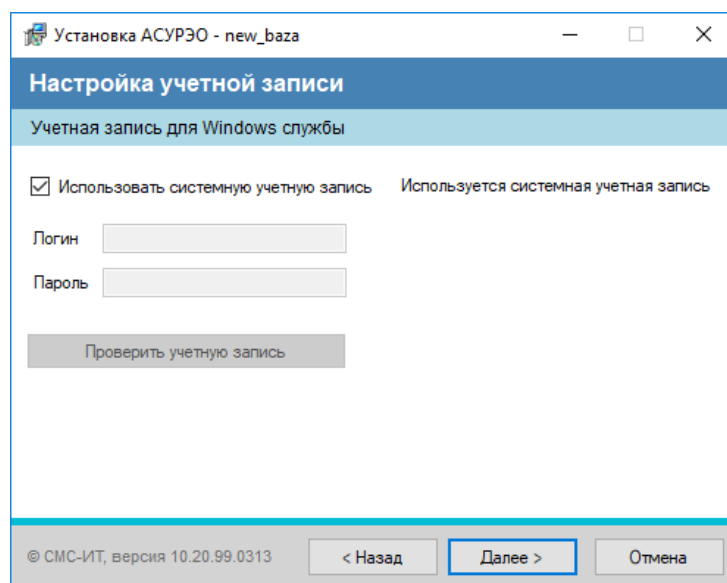


Рисунок 12.27 – Использование системной учетной записи

### 12.3.5 Выбор базы данных

На следующем шаге необходимо выбрать поддерживаемую базу данных «MSSQL» или «PostgreSQL» (Рисунок 12.28).

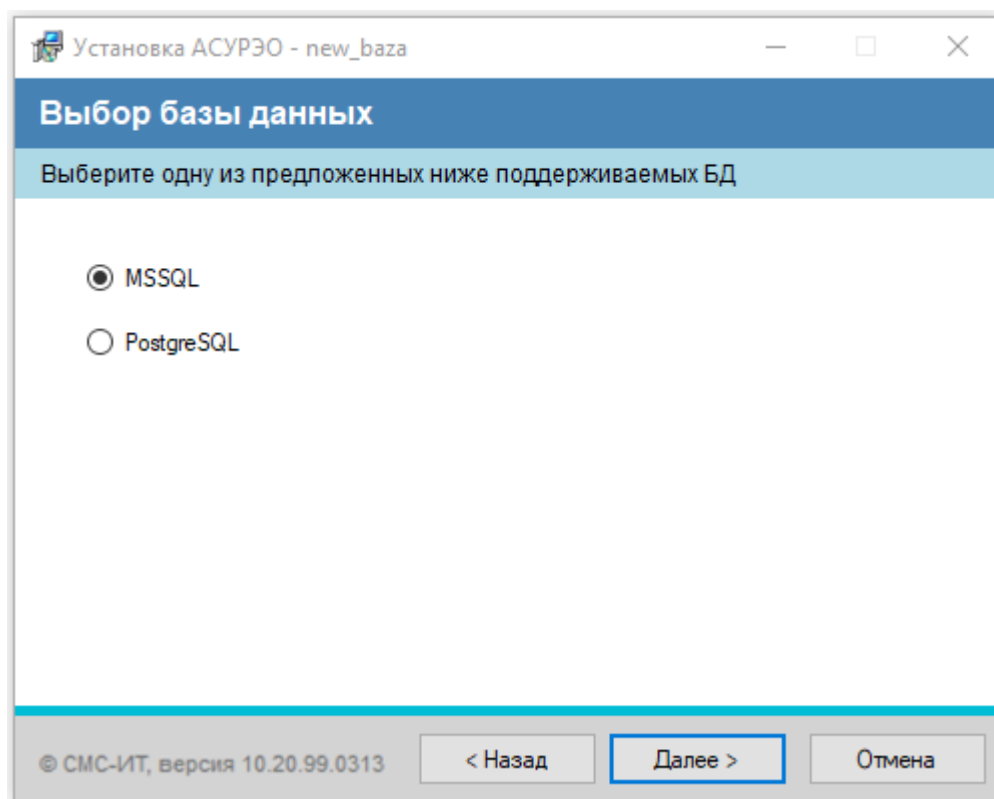


Рисунок 12.28 – Выбор базы данных

### 12.3.6 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 12.29).

Данные о пользователе должны соответствовать настройкам созданной ранее учетной записи пользователя (см. разделы «12.1.3 Настройка прав учетной записи пользователя» и «12.2.5 Настройка прав учетной записи пользователя»).

Установка АСУРЭО - new\_baza

### Настройка подключения к MSSQL

Введите необходимые параметры соединения с СУБД

Адрес сервера:

Базы данных:

Обновить

Логин:

Пароль:

Проверить соединение

☐ Использовать доменную авторизацию ☐ Установить на существующую БД

© СМС-ИТ, версия 10.20.99.0313

< Назад Далее > Отмена

Рисунок 12.29 – 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 12.30).

Установка АСУРЭО - new\_baza

### Настройка подключения к MSSQL

Введите необходимые параметры соединения с СУБД

Адрес сервера:

Базы данных:

Обновить

Логин:

Пароль:

Проверить соединение

☐ Использовать доменную авторизацию ☐ Установить на существующую БД

A network-related or instance-specific error occurred while connecting to the SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that the server is running. (Microsoft SQL Server, Error: 26)

© СМС-ИТ, версия 10.20.99.0313

< Назад Далее > Отмена

Рисунок 12.30 – 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 12.31). 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».

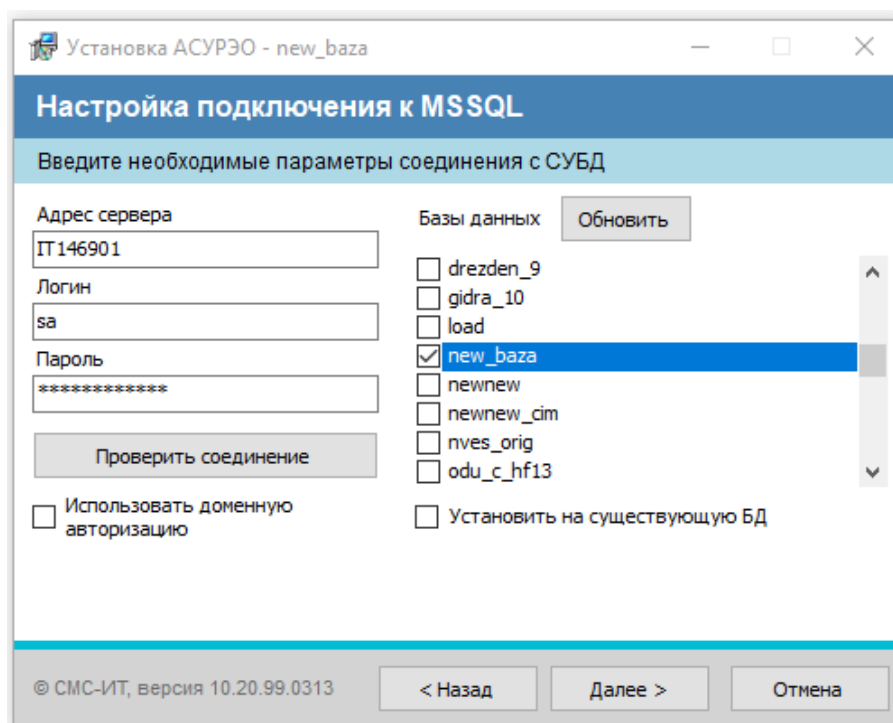


Рисунок 12.31 – Выбор базы данных для установки

БД для установки ПК создается заранее (см. раздел «12.1 Создание и настройка БД MS SQL»).

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.

### 12.3.7 Настройка параметров ключа защиты

На следующем шаге требуется ввести идентификатор электронного ключа защиты, поставляемого вместе с ПК (Рисунок 12.32).

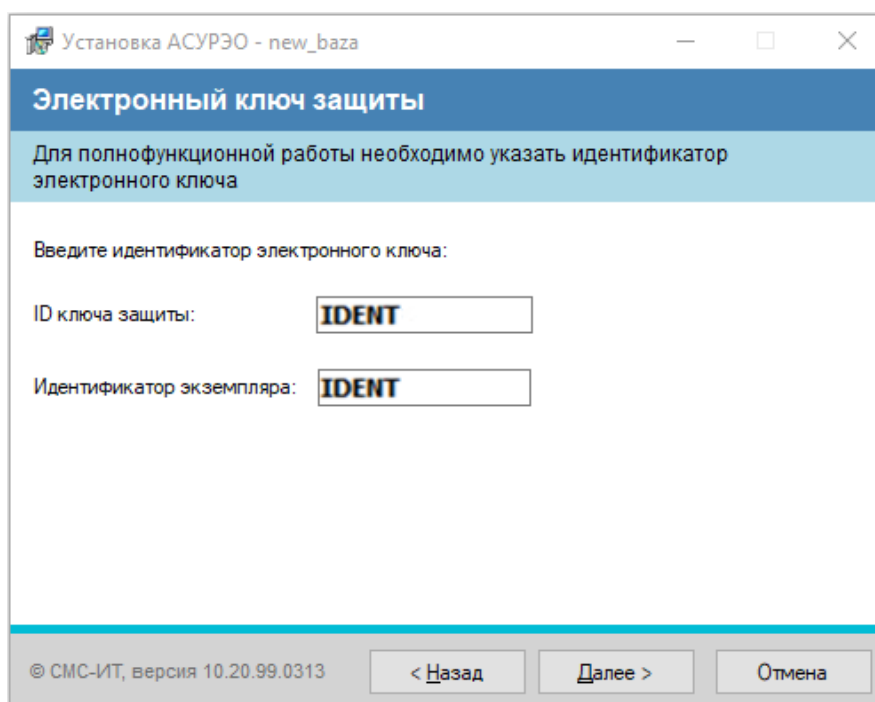


Рисунок 12.32 – Ввод идентификатора электронного ключа

### 12.3.8 Завершение сбора информации

На следующем шаге в окне мастера отображается вся информация, полученная программой установки (Рисунок 12.33). В случае необходимости можно вернуться на предыдущие шаги установки и внести изменения.

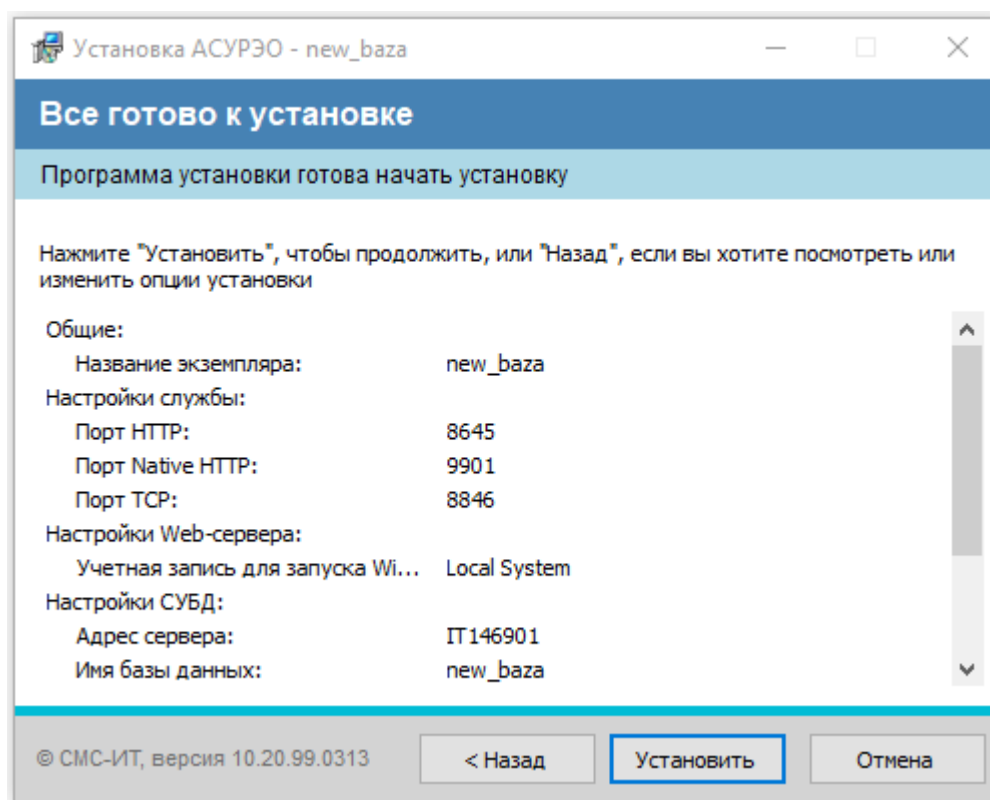


Рисунок 12.33 – Завершение сбора информации

Последним этапом является процесс копирования файлов и настройка системы (Рисунок 12.34).

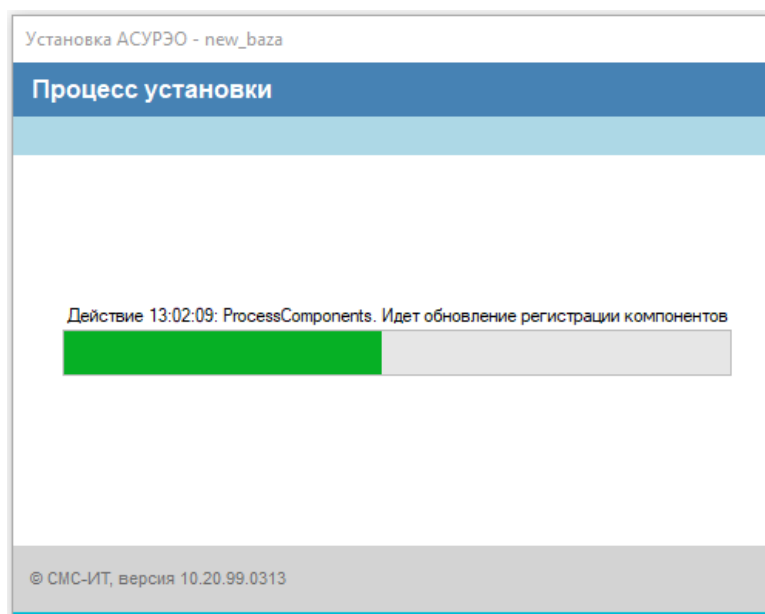


Рисунок 12.34 – Копирование файлов и настройка системы

По окончании процесса установки появляется окно завершения мастера установки, в котором отображается адрес доступа к ПК (Рисунок 12.35). 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.

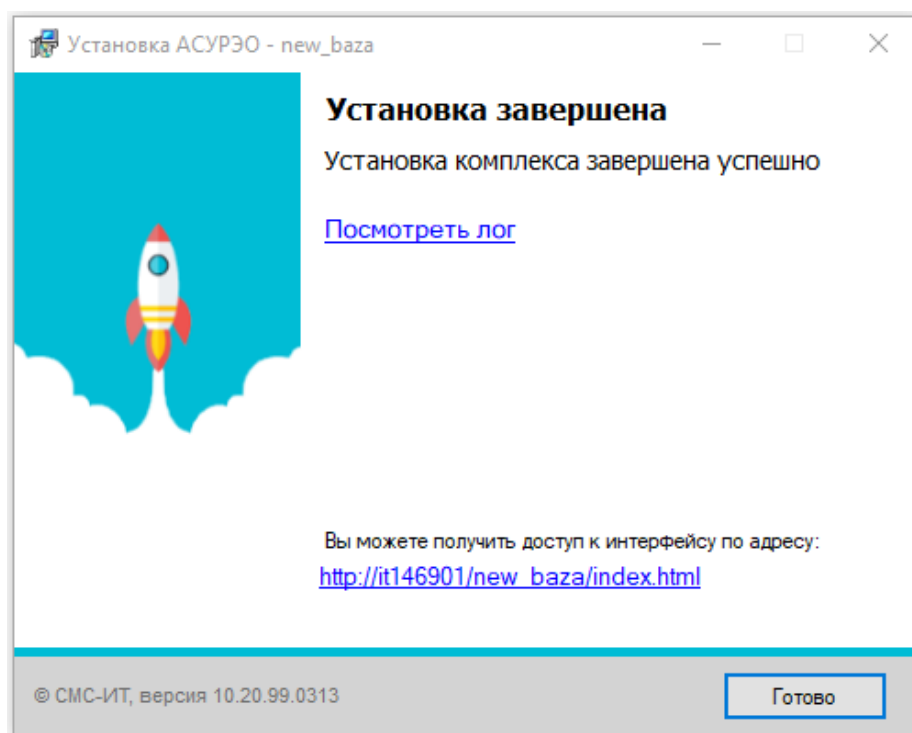


Рисунок 12.35 – Завершение установки

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

## 12.4 Установка Системы на ОС семейства Linux

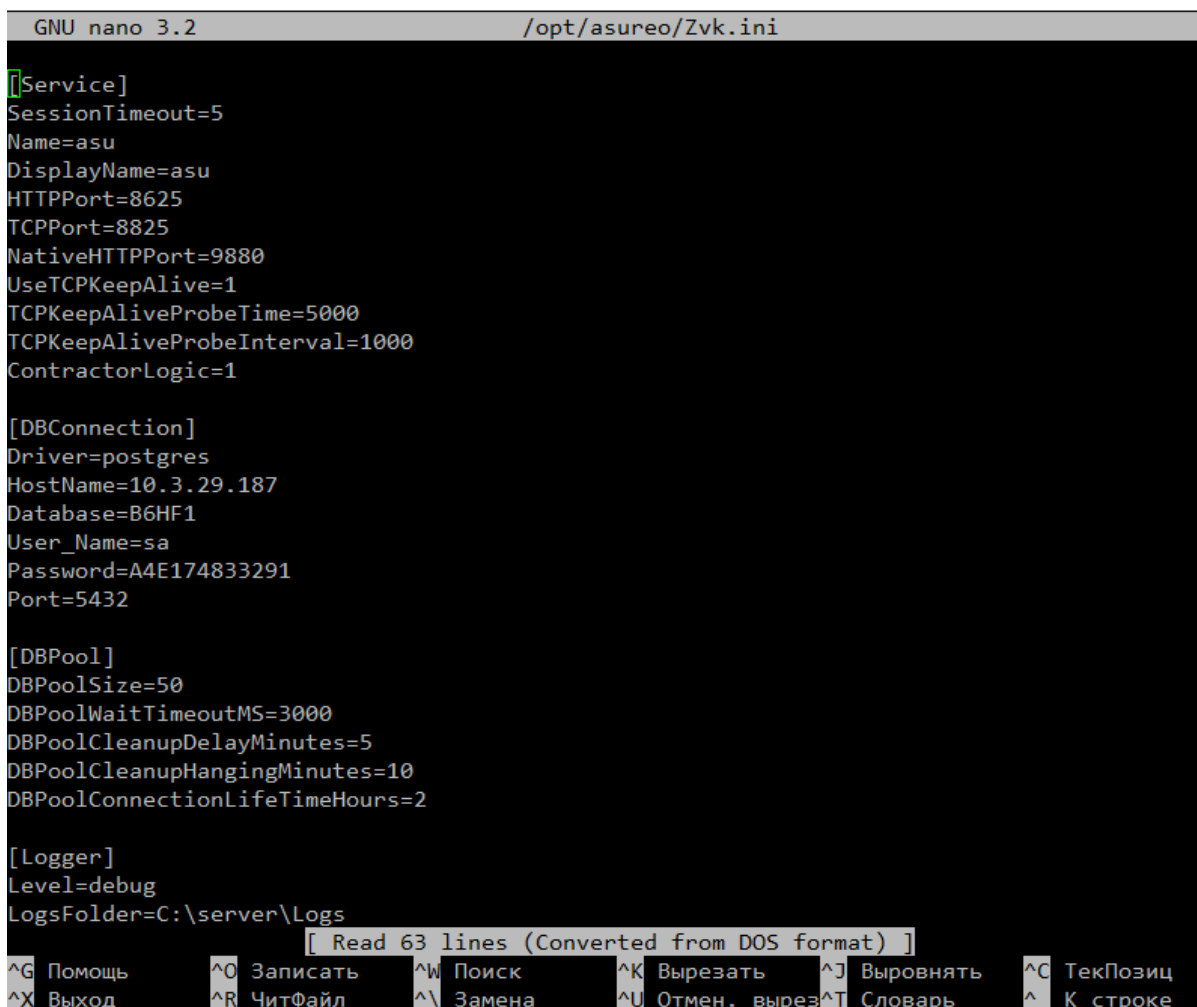
Установка Системы на ОС семейства Linux осуществляется с помощью docker контейнеров. Для выполнения установки необходимо выполнить следующие действия:

1. Создать каталог. Выполнить команду: `mkdir /opt/asureo` (Рисунок 12.36).

```
sysadmin@ClusterPG-1:/opt/asureo$ mkdir /opt/asureo
```

Рисунок 12.36 - Выполнение команды `mkdir /opt/asureo`

2. Скопировать в каталог `/opt/asureo` файлы из комплекта поставки:
  - `docker-compose.yml` файл с образами Системы и веб-сервера `nginx`;
  - конфигурационный файл `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 12.37.



```
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 Выводить ^C ТекПозиц
^X Выход ^R ЧитФайл ^\ Замена ^U Отмен. выр ^T Словарь ^_ К строке
```

Рисунок 12.37 – Правки в секции `[DBConnection]`

4. В файл конфигурации мигратора БД (`config.json`) внести правки подключения к СУБД (Рисунок 12.38).

```
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 12.38 – Правки подключения к СУБД

5. В файл конфигурации confighost.txt внести правки: изменить адрес на ip хост сервера (Рисунок 12.39).

```
GNU nano 3.2 confighost.txt
ApplicationUrl=http://192.168.242.20/SMSITLoader
Version=11.22.8308.0719
```

Рисунок 12.39 – Правки confighost.txt

6. В nginx-config/conf.d/default.conf указать корректный ip хост сервера (Рисунок 12.40).

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

location ~ ^/appsrv/(proxy.dll/)?(.*)$ {
 if ($http_user_agent ~* 'RemObjects') {
 rewrite ^/appsrv/(proxy.dll/)?(.*)$ /appservice/$2;
 }
 rewrite ^/appsrv/(proxy.dll/)?(.*)$ /appsite/$2;
}

location /appsite/ {
 proxy_pass http://10.3.34.34:9880/;
 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://10.3.34.34:8625/;
 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;
```

Рисунок 12.40 – Корректировки default.conf

7. Перейти в каталог. Выполнить команду: `cd /opt/asureo/` (Рисунок 12.41).

```
sysadmin@ClusterPG-1: cd /opt/asureo/
```

Рисунок 12.41 – Выполнение команды `cd /opt/asureo/`

8. Загрузить образы Системы из файла на диске с помощью docker команды.

Выполнить команду: *docker load* (Рисунок 12.42).

```
sysadmin@ClusterPG-1:/opt/asureo$ docker load < asu_v9sd9wine10.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
C454e21f5600: Loading layer 3.032MB/3.032MB
547b32605171: Loading layer 4.608kB/4.608kB
Loaded image: asu:v9sd9hf2
```

Рисунок 12.42 – Выполнение команды docker load

9. Проверить успешную загрузку образов Системы, отобразив список образов.

Выполнить команду: *docker image ls* (Рисунок 12.43).

```
sysadmin@ClusterPG-1:/opt/asureo$ docker images ls
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
asu	v9sd9wine10	e397f47dfbf0	1 week ago	4.13GB

Рисунок 12.43 – Выполнение команды docker image ls

10. Запустить контейнеры Системы и nginx с помощью docker-compose команды.

Выполнить команду: *docker-compose up -d* (Рисунок 12.44).

```
sysadmin@ClusterPG-1:/opt/asureo$ sudo docker-compose up -d
Creating volume "asureo_www" with default driver
Creating asureo ... done
```

Рисунок 12.44 – Выполнение команды docker-compose up -d

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

Выполнить команду: *docker ps* (Рисунок 12.45).

```
sysadmin@ClusterPG-1:/opt/asureo$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
98ad1e703e50	asu:v9sd9 wine10	"/home/root/docker-e..."	9 seconds ago	Up 8 seconds	0.0.0.0:8625->8625/tcp	asureo

Рисунок 12.45 – Выполнение команды docker ps

---

## 12.5 Настройка Системы с помощью конфигуратора

Конфигуратор позволяет вносить изменения в конфигурации сервера приложений и сервера авторизации веб-версии Системы.

**Важно!** При настройке Системы через конфигуратор необходимо осуществлять сохранение настроек на каждой вкладке конфигуратора.

Открытие конфигуратора осуществляется на стартовой странице комплекса по нажатию на пункт «Конфигуратор» (Рисунок 12.46).

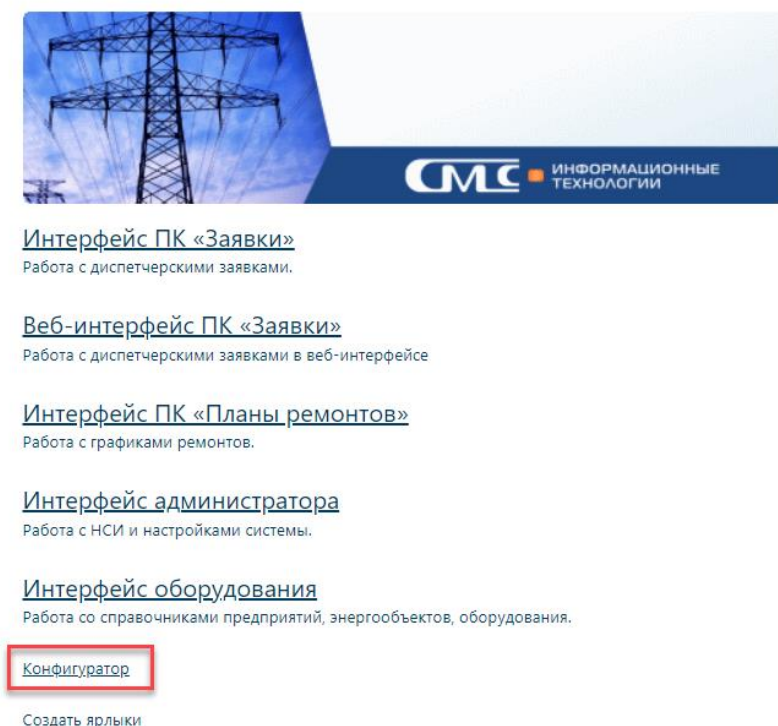


Рисунок 12.46 – Открытие конфигуратора

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 «12.5.1 Дополнительные настройки») по нажатию кнопки «Сменить пароль». После нажатия кнопки открывается окно «Смена пароля», где необходимо указать старый и новый пароли (Рисунок 12.47).

Данные логин и пароль необходимо запомнить, так как в дальнейшем они должны использоваться пользователем для авторизации в конфигураторе.

---

Сервер приложений   Сервер авторизации   Доп.настройки   [Выход](#)

---



### Смена пароля

Старый пароль

 ..... 

Новый пароль

 ..... 

Сменить пароль

Рисунок 12.47 – Окно «Смена пароля»

### 12.5.1 Дополнительные настройки

Для настройки веб-конфигуратора необходимо перейти в раздел «Доп.настройки», где отображаются следующие параметры (Рисунок 12.48):

- «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» – название контейнера . Указанный в данном параметре контейнер перезапускается по нажатию на кнопку «Перезапустить контейнеры и сервисы».

Сервер приложений Сервер авторизации Сервер приложений Delphi

Доп.настройки

Доп. настройки

Системные настройки

Уровень логирования: Information

Сервер авторизации: /identity/app/web/AuthServer.settings.json

Сервер приложений: /zrp/app/web/Sms.ZRP.WebApi.settings.json

Сервер приложений Delphi: /home/root/wine/drive\_c/server/Zvk.ini

Контейнеры для перезагрузки:

Имя контейнера с Delphi заявками ZR\_E

Сменить пароль

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.48 – Настройка веб-конфигуратора

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

### 12.5.2 Настройка Сервера приложений

После изменения пароля откроется страница настроек Сервера приложений.

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

- «Разрешенные хосты» – указывается фильтр допустимых имен хоста, которые может иметь сервер.
- «Адрес аутентификации» – указывается адрес сервера авторизации. Если внешний адрес сервера авторизации недоступен со стороны веб-сервера приложений, то в данном поле необходимо указать внутренний адрес сервера авторизации, а в поле «Внешние адреса сервера авторизации» – внешний адрес. Адрес необходимо указать в формате: `https://<адрес_сервера>:444`, где порт 444 – https порт, указанный в `default.conf`.
- «Базовый адрес сервера приложений» – указывается базовый адрес сервера приложений, который обращается к серверу авторизации, указанному в поле «Адрес сервера авторизации».
- «Адрес сервера авторизации» – указывается адрес сервера авторизации в привязке к базовому адресу сервера приложений, указанному в поле «Базовый адрес сервера приложений».

- «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.
- «Префикс экземпляра BasePath» – указывается общий префикс для всех эндпоинтов API. Значение необходимо указать в формате '/<префикс>/web/'. Пример: /zvkdev/web/. Подробнее в разделе «14.5.17 Настройка префикса для маршрутизации запросов внутри одного порта».

Для удаления пары полей «Базовый адрес сервера приложений:» и «Адрес сервера авторизации:» необходимо нажать кнопку [-] около поля «Адрес сервера авторизации».

По нажатию кнопки «Добавить» добавляется новая пара полей «Базовый адрес сервера приложений:» и «Адрес сервера авторизации:».

При необходимости пользователь может включить логирование для настроек к БД, установив соответствующие флаги (Рисунок 12.49). По умолчанию логирование выключено.

Сервер приложений Сервер авторизации Сервер приложений Delphi Доп.настройки

### Настройки

Системные настройки

Настройка оповещений

Настройка интеграций

Разрешенные хосты: \*

Адрес аутентификации: http://srv-it-zvk-lin.stand.local:467

Внешний адрес аутентификации: https://external.web.address.com:4443

Провайдер БД: PostgreSQL

Date Source=VM-IT-ZVK-ANALY  
Initial Catalog=real\_cdu  
User ID=sa  
Password=sa

**Логирования настроек к БД:**

Включить: ☒

Дополнительное логирование запросов: ☐

Дополнительное логирование команд: ☒

Префикс экземпляра BasePath: /zvkdev/web/

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.49 – Системные настройки сервера приложений

В разделе «Настройка оповещений» настраиваются оповещения о заявках и пользовательские оповещения. Параметры настройки оповещений задаются в виде стандартного

Сtop – выражения. По умолчанию установлено значение с периодом обновления в 1 минуту - \*/1 \* \* \* \* (Рисунок 12.50).

Сервер приложений   Сервер авторизации   Сервер Delphi приложений   Доп.настройки

### Настройки

Системные настройки

Настройка оповещений

Настройка интеграций

#### Оповещения о заявках

Оповещения о заявках: \*/1 \* \* \* \*

---

#### Пользовательские оповещения

Пользовательские оповещения: \*/1 \* \* \* \*

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.50 – Настройка оповещений

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:superhttp-порт/SOAP`, где `superhttp-порт` – порт из `zvk.ini` (по умолчанию 9890). Также возможно указать ссылку в следующем виде `http://имя сервера:http-порт/appsrv/SOAP`, где `http-порт` – порт для веб-сервера заявок из `default.conf` (по умолчанию 80). Использование протокола HTTPS не допускается! (Рисунок 12.51).

Флаг «Проксировать запросы создания/редактирования заявки в сервер приложений Delphi» установлен по умолчанию. Если флаг не установлен, то необходимо его установить.

Флаг «Проксировать запросы предопределенных маршрутов в сервер приложений Delphi» не должен быть установлен. Установка может потребоваться только при возникновении критичных ошибок в функционале создания/редактирования заявки и предопределенных маршрутов на сервере приложений Системы.

Начиная с версии ПК «АСУРЭО» B9SD10 для работы с веб-интерфейсом необходимо указать параметры лицензионного ключа в секции «Лицензирование» и нажать кнопку «Сохранить». Значение поля «Идентификатор лицензионного ключа» должно соответствовать значению параметра «Instance» в секции [Key] файла `zvk.ini`.

При наличии функционала лицензирования для корректной работы Системы при перезапуске сервера приложений веб-интерфейса необходимо обязательно осуществить перезапуск сервера приложения delphi-интерфейса.

---

Для настройки взаимодействия с внешними сервисами необходимо установить флаг «Включено» в разделе «Настройка взаимодействия с внешними сервисами» и в поле «Канал» выбрать канал через который будет выполняться внешняя коммуникация (etcd или База данных) (Рисунок 12.51). Если выбрано значение «etcd»:

- в конфигурационном файле `Sms.ZRP.WebApi.settings.json` в разделе `ExternalCommunicationSettings` настройка `Channel` заполняется значением `etcd` (подробнее в разделе «14.5 Описание параметров файла `sms.ZRP.WebApi.settings.json`»);
- в конфигурационном файле `zvk.ini` в секции `MessageServerConnection` настройка `ChannelType` заполняется значением `etcd` (подробнее в разделе «14.2 Описание параметров файла `zvk.ini`»).

Если выбрано значение «База данных»:

- в конфигурационном файле `Sms.ZRP.WebApi.settings.json` в разделе `ExternalCommunicationSettings` настройка `Channel` заполняется значением `database` (подробнее в разделе «14.5 Описание параметров файла `sms.ZRP.WebApi.settings.json`»);
- в конфигурационном файле `zvk.ini` в секции `MessageServerConnection` настройка `ChannelType` заполняется значением `database` (подробнее в разделе «14.2 Описание параметров файла `zvk.ini`»).

Поле «Канал» отображается, если установлен флаг «Включено». Также в данном разделе необходимо установить флаг «Разрешить повторную отправку».

Сервер приложений

Сервер авторизации

Сервер приложений Delphi

Доп.настройки

Настройки

Системные настройки

Настройка оповещений

Настройка интеграций

Подключаемые функции

Сервис интеграции с сервером приложений Delphi

Включить интеграцию с сервером приложений Delphi:

☒

Проксировать запросы создания/редактирования заявки в сервер приложений Delphi:

☒

Проксировать запросы predefined маршрутов в сервер приложений Delphi:

☐

URL к интеграции:

Лицензирование

Идентификатор лицензионного ключа:

Имя файла лицензионного ключа:

Настройка взаимодействия с внешними сервисами

Включено:

☒

Канал:

Разрешить повторную отправку:

☒

Возраст сообщения для переправки в секундах:

Настройка интеграции через etcd

Строка подключения:

Группа клиентов:

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.51 – Пример настройки интеграций

**Примечание.** Ниже идет описание взаимодействия через канал etcd. Канал etcd на данный момент не используется и не требует подключения, коммуникации между серверами приложений происходят только по каналу БД.

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

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": {
```

Руководство системного администратора

```
"Enable": false,
"ConnectionString": "http://<IP-адрес сервера>:2379"
},
```

В конфигурационном файле `zvk.ini` меняются следующие параметры:

**Пример:**

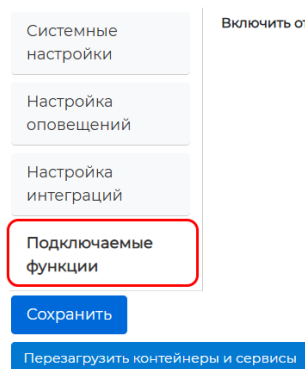
```
[MessageServerConnection]
ServerType=ETCD
Host=<IP-адрес сервера>
Port=2379
GroupID=
ConnectTimeout=1
ReadTimeout=1
MessageEncryption=0
PingIntervalSec=60
UseResendExpired=1
ResendExpiredIntervalSec=60
UseEtdChannel=0
UseDatabaseChannel=1
```

Etcd не должен влиять на правильную работу веб-версии Системы. 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. 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).

В разделе «Подключаемые функции» настраивается отображение сообщений СУПА в Журнале сообщений (Рисунок 12.52). 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`.

## Настройки



Включить отображение сообщений СУПА в ЖС:



Рисунок 12.52 – Настройка подключаемых функций

После внесения изменений необходимо нажать кнопку «Сохранить».

### 12.5.3 Настройка Сервера авторизации

Для настройки сервера авторизации необходимо перейти в раздел «Системные настройки» (Рисунок 12.53). 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 доступна переадресация на сервер авторизации. Доступно указание нескольких данных параметров в конфигураторе.

Стандартно для данного параметра необходимо указать адрес сервера приложений веб-версии Системы в виде `https://<адрес_сервера>:443`, где 443 – порт сервера приложений веб-заявок из `default.conf`.

- «RedirectUris» – набор допустимых адресов, которые может прислать клиент как точки возврата пользователя после завершения аутентификации. Доступно указание нескольких таких параметров в конфигураторе в разных полях ввода «RedirectUris».

- «Префикс экземпляра BasePath» – базовый путь в URL, определяющий маршрутизацию запросов внутри одного порта. Необходимо указать значение в формате '/<префикс>/identity/'. Пример: /zvkdev/identity/. Данное поле заполняется при необходимости. Подробнее в разделе «14.5.17 Настройка префикса для маршрутизации запросов внутри одного порта».

Сервер приложений
Сервер авторизации
Сервер приложений Delphi
Доп. настройки

## Настройки

Системные настройки
Домены

Разрешенные хосты: \*
NT Аутентификация: ☐
Уникальный идентификатор: HTTP/srv-it-zvk-lin.stand.local
Домен: STAND.LOCAL
AllowedCorsOrigins: https://srv-it-zvk-lin.stand.local
AllowedCorsOrigins: http://srv-it-zvk-lin
AccessTokenLifetime: 3600
RedirectUri: /zvkdev/zvk/auth-callback
RedirectUri: /zvkdev/web/zvk/auth-callback
Префикс экземпляра BasePath: /zvkdev/identity/

Сохранить
Перезагрузить контейнеры и сервисы

Рисунок 12.53 – Настройка сервера авторизации

В разделе «Домены» настраивается доменная авторизация (Рисунок 12.54). При осуществлении авторизации с нескольких доменов необходимо указать имена всех доменов и их возможные алиасы (псевдонимы).

Поле ввода «Домен»:

- отображается всегда. Доступно для редактирования всегда;
- обязательно для заполнения;
- заполняется вручную;
- в поле допускается ввод букв, цифр, символов;
- ограничение по количеству символов отсутствует;
- хинт: «Полное имя домена, включающее в себя доменную зону»;

- заполняет настройку DomainAliasMap / domain в конфигурационном файле AuthServer.settings.json.

Поле ввода «Полное имя домена»:

- отображается всегда. Доступно для редактирования всегда;
- обязательно для заполнения;
- заполняется вручную;
- в поле допускается ввод букв, цифр, символов;
- ограничение по количеству символов отсутствует;
- заполняет настройку DomainAliasMap / realm в конфигурационном файле AuthServer.settings.json.

Сервер приложений Сервер авторизации Сервер приложений Delphi Доп.настройки

Настройки

Системные настройки Домены

Домен

cmc

Полное имя домена

domain.local

Алиасы:

mail.sms-samara.ru

+

+

+

Добавить алиас

Домен

stand

Полное имя домена

domain.local

Алиасы:

stand.local

+

+

Добавить алиас

Сохранить

Перезагрузить контейнеры

Рисунок 12.54 – Настройка доменной авторизации

### 12.5.4 Настройка Сервера Delphi приложений

Для настройки сервера Delphi приложений необходимо перейти в раздел «Системные настройки» (Рисунок 12.55). 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 первого зондирующего TCPKeepAlive-пакета. По умолчанию 5000 мсек.
- «TCPKeepAliveProbeInterval» – указывается период отправки зондирующих TCPKeepAlive-пакетов. По умолчанию 1000 мсек.

Сервер приложений	Сервер авторизации	Сервер приложений Delphi
-------------------	--------------------	--------------------------

Настройки

Системные настройки

Соединение с БД

Пул

Логирование

Планировщик

Автоматическая очистка журнала

Таймаут сессии на веб-сервере:

5

Имя экземпляра:

asu

Отображаемое имя экземпляра:

asu

HTTPPort экземпляра:

8625

TCPPort экземпляра:

8825

NativeHTTPPort экземпляра:

9880

UseTCPKeepAlive:

1

TCPKeepAliveProbeTime:

5000

TCPKeepAliveProbeInterval:

1000

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.55 – Системные настройки сервера Delphi приложений

Для настройки соединения с БД необходимо перейти в раздел «Соединение с БД», где отображаются следующие параметры (Рисунок 12.56):

- «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.

Сервер приложений Сервер авторизации Сервер приложений Delphi Доп.настройки

### Настройки

- Системные настройки
- Соединение с БД**
- Пул
- Логирование
- Планировщик
- Автоматическая очистка журнала

**Провайдер БД:** PostgreSQL ▼

**HostName:** 10.3.29.42

**Наименование базы данных:** zre

**Логин пользователя в СУБД:** postgres

**Пароль:** A7EF039E2B9CCD698A0D0257

**Порт СУБД:** 5432

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.56 – Настройки соединения с БД

Для настройки пула необходимо перейти в раздел «Пул», где отображаются следующие параметры (Рисунок 12.57):

- «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).

## Настройки

Системные настройки	Размер пула: 50
Соединение с БД	Время ожидания при получении соединения: 3000
Пул	Время удаления из пула свободных соединений: 5
Логирование	Время принудительного удаления из пула: 10
Планировщик	Время жизни соединения в пуле : 2
Автоматическая очистка журнала	
Сохранить	
Перезагрузить контейнеры и сервисы	

Рисунок 12.57 – 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, warn, 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 ЗРП.
- «ShedulerTasks.FileName» – включает логирование расширенной информации по работе задач планировщика. По умолчанию присутствует в zvz.ini в формате ShedulerTasks.FileName=ShedulerTasks.

Для настройки планировщика необходимо перейти в раздел «Планировщик», где отображаются следующие параметры (Рисунок 12.58):

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

[Сервер приложений](#) [Сервер авторизации](#) [Сервер Delphi приложений](#)

[Доп.настройки](#)

## Настройки

Системные настройки	Частота опроса планировщика:	500
Соединение с БД	Пауза перед первым запуском:	10000
Пул		
Логирование		
<b>Планировщик</b>		
Автоматическая очистка журнала		
Сохранить		
Перезагрузить контейнеры и сервисы		

Рисунок 12.58 – Настройка планировщика

Для настройки автоматической очистки журнала необходимо перейти в раздел «Автоматическая очистка журнала», где отображаются следующие параметры (Рисунок 12.59):

- «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).

## Настройки

Системные настройки	Задача отправки сообщений:	60
Соединение с БД	Задача приема сообщений:	60
Пул	Задача проверки квитанций:	60
Логирование	Задача архивации очистки данных и автоудаления диспетчерских заявок:	86400,01:00
Планировщик	Архивации заявок по сроку давности с интервалом:	86400,01:30
Автоматическая очистка журнала		

Сохранить

Перезагрузить контейнеры и сервисы

Рисунок 12.59 – 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.

При старте перезагрузки отображается шторка с текстом «Начинаем перезагрузку контейнера Delphi и сервисов Web». Далее отображается результат перезагрузки:

1. **Результат перезагрузки контейнера Delphi** (т.е Docker-контейнера, в котором работает Сервер приложений Delphi заявок):

- При ошибке:
  - Если поле «Имя контейнера с Delphi заявками» **не заполнено**, то отображается шторка красного цвета с текстом «Контейнер Delphi не задан. Перезагрузите Сервер приложений Delphi вручную».
  - Если поле «Имя контейнера с Delphi заявками» **заполнено некорректно**, то отображается шторка красного цвета с текстом «Контейнер '<имя контейнера из поля "Имя контейнера с Delphi заявками">' не найден».

*Пример:* «Контейнер 'zvк-11r8-zvк' не найден»

- 
- Если произошла **другая ошибка** при перезапуске контейнера Delphi, то отображается шторка красного цвета с текстом: «Произошла ошибка при перезагрузке контейнера Delphi: <текст ошибки>».
  - При успешной перезагрузке:
    - Отображается шторка с текстом «Контейнер '<Имя контейнера с Delphi заявками>' успешно перезапущен».
  - 2. **Результат перезагрузки Сервисов Web** (т.е Сервера приложений Web заявок и Сервера авторизации):
    - При ошибке:
      - Если Сервер приложений Web-заявок развернут на Windows, то отображается шторка красного цвета с текстом: «Не доступна перезагрузка сервисов Web. Перезагрузите Сервер приложений Web заявок вручную.»
      - Если произошла **другая ошибка** при перезапуске сервисов Web, то отображается шторка красного цвета с текстом: «Произошла ошибка при перезагрузке сервисов Web: <текст ошибки>».
    - При успешной перезагрузке:
      - Отображается шторка с текстом «Сервисы Web успешно перезапущены».

## 12.6 Добавление шаблонов отчетов для ЗРП.Net

Добавление шаблонов отчетов для ЗРП.Net осуществляется путем обновления БД через мигратор ЗРП.Delphi (при работе в кластере на любом одном из узлов кластера, где установлен сервер приложений).

Для этого необходимо:

1. Скопировать файлы, содержащие скрипты отчетов в директорию /home/root/.wine/drive\_c/migrator/\_data/Templates внутри docker контейнера.
2. Перезапустить контейнер, выполнив команду:  
`docker-compose up --build --force-recreate -d`

## 12.7 Запуск приложения Системы

Для запуска Системы клиентского рабочего места необходимо на рабочем столе пользователя в строке браузера ввести адрес *http://xx.xxx.xx.xxx:yy/index.html*, где xx.xxx.xx.xxx – ip адрес, либо имя сервера ПС, yy – порт сайта приложения (Рисунок 12.60) и выполнить переход по данной строке. Далее необходимо выбрать интерфейс и дождаться загрузки интерфейса (Рисунок 12.61).

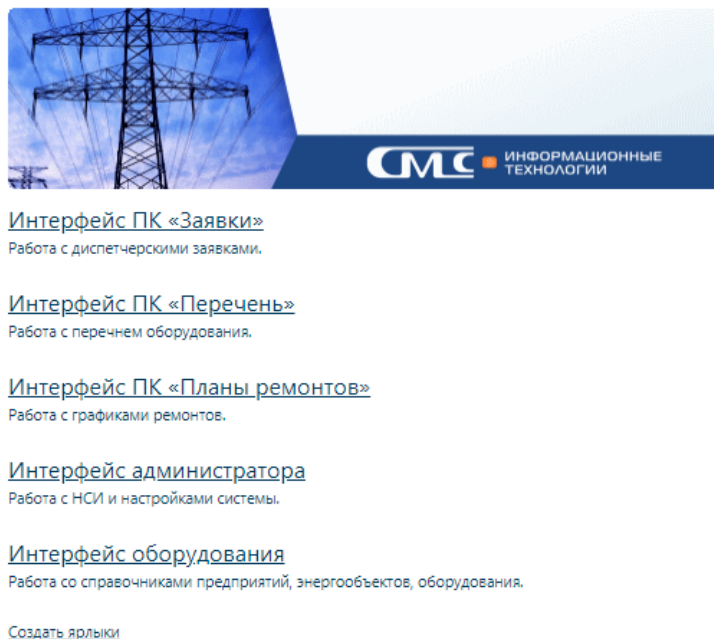


Рисунок 12.60 – Web-страница приложения Системы

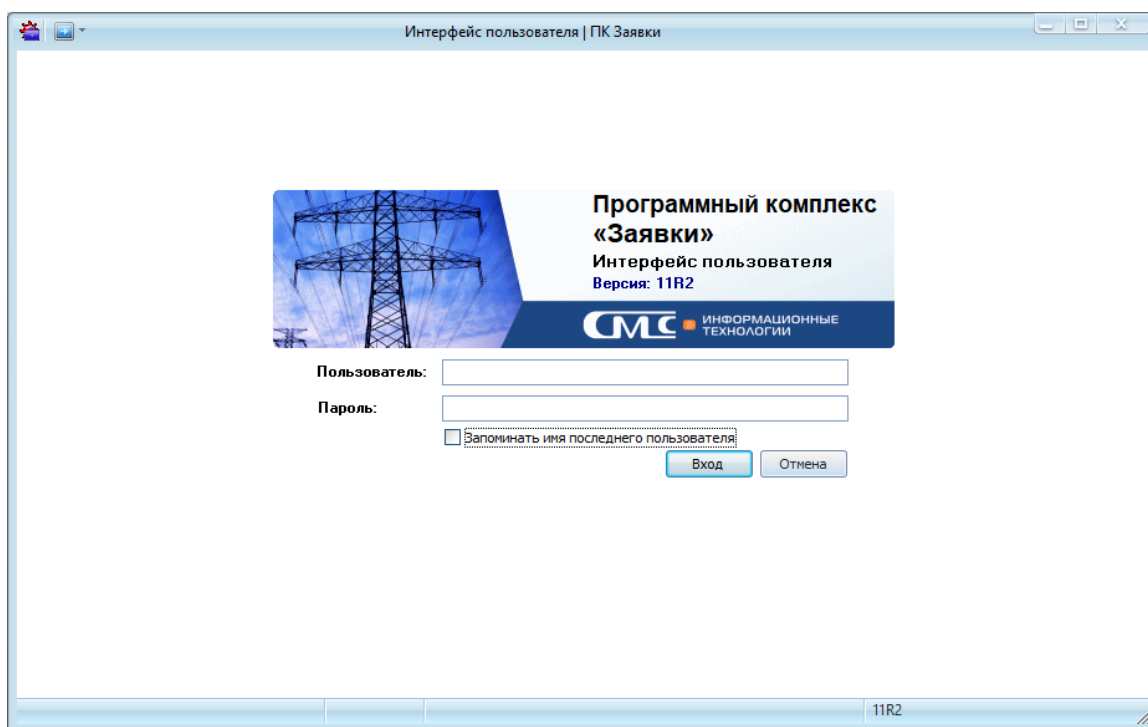


Рисунок 12.61 – Интерфейс пользователя

При запуске ЗРП.Net произойдет перенаправление на https и откроется окно авторизации (Рисунок 12.62).

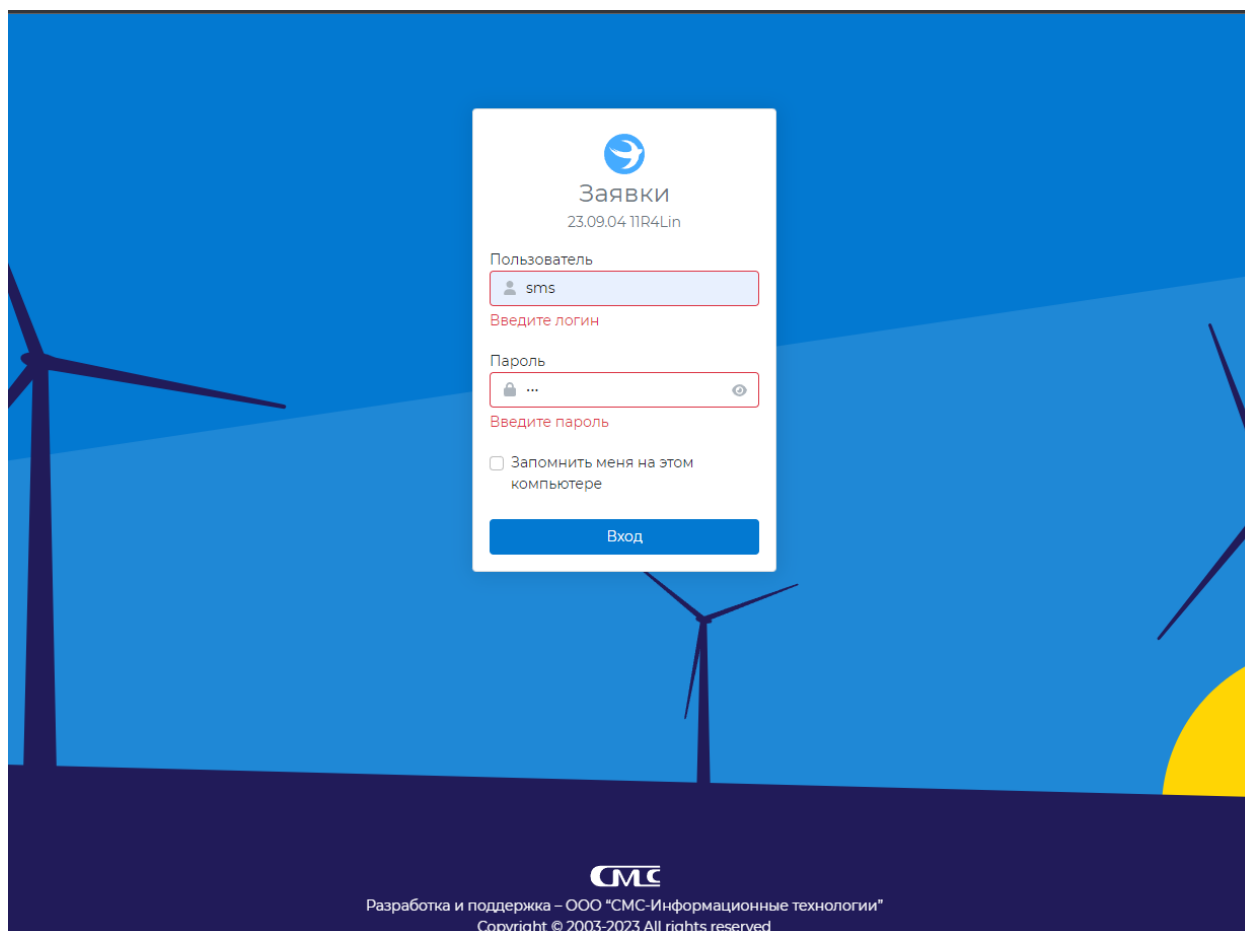


Рисунок 12.62 – Запуск ЗРП.Net

Если у пользователя настроена NT-авторизация, то после перехода на экран входа осуществляется автоматическая попытка авторизации в системе.

Если на сервере настроена NT-авторизация, но у пользователя указаны доменный логин и пароль (которые не соответствуют настройкам), то отображается окно NT-авторизации (Рисунок 12.63) по нажатию на кнопку «Войти» пользователь не может авторизоваться. В данном случае пользователю отображается окно с вводом логина и пароля (Заголовки полей ввода на форме: «Пользователь NT», «Пароль»). Пользователю необходимо ввести доменные логин и пароль (логин и пароль NT-авторизации) для авторизации в системе.

Пример NT-авторизации:

- на Linux:
  - <логин>@<домен>;
  - <домен>\<логин> – если домен настроен в конфигурационном файле AuthServer.settings.json настроены домены.
- на Windows: <домен>\<логин>

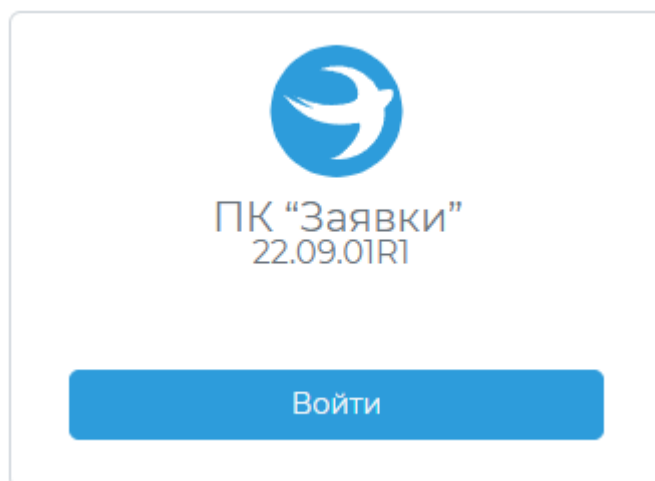


Рисунок 12.63 – Авторизация при настроенной NT-авторизации

Если на сервере настроена NT-авторизация, но у пользователя не указаны доменный логин в поле «Пользователь NT» в Интерфейсе администратора в справочнике «Службы и пользователи», то отображается окно NT-авторизации (Рисунок 12.63) по нажатию на кнопку «Войти» пользователь не может авторизоваться. В данном случае пользователю отображается окно с вводом логина и пароля (Заголовки полей ввода на форме: «Пользователь NT», «Пароль»). Пользователь вводит доменные логин и пароль, но не может авторизоваться, отображается окно авторизации с текстом ошибки: «Неправильный логин и пароль».

Если у пользователя настроена NT-авторизация, то его авторизация в системе происходит по нажатию на кнопку «Войти» на форме авторизации. Ввод логина и пароля при этом не требуется.

## 12.8 Обновление на ОС семейства Linux

В состав дистрибутива для обновления входят docker образы: **.Delphi** и **.Net (поставляется при наличии лицензий для веб-версии)**. Обновление на ОС семейства Linux производится путём замены соответствующих docker образов на новые и запуском docker контейнеров. Для обновления необходимо выполнить следующие действия:

1. Выполнить остановку сервера приложений 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 «20.3 Рекомендации по штатному останову серверов приложений».

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

```
sudo docker volume rm assureo_www
```

Для удаления docker томов веб-версии Системы выполнить команды:

```
sudo docker volume rm asuteo_config
```

```
sudo docker volume rm asureo_sqlite
```

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

```
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 12.64 полное имя *asu:v9sd7\_release* и *asu-web:latest* для веб-версии Системы.

**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 12.64 – 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 12.65):

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

Рисунок 12.65 – Команда удаления docker образа

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

```
ls /opt/asureo
```

Пример представлен на рисунке 12.66.

```
sysadmin@zvk-test:/opt/asureo$ ls /opt/asureo
```

asu_v9sd8_release.tar	asu_web_v9sd8	docker-compose.yml	Zvk.ini
-----------------------	---------------	--------------------	---------

Рисунок 12.66 – Выполнение команды `ls /opt/asureo`

6. Убедиться, что в файле `nginx-config/conf.d/default.conf` указан корректный `ip` хост сервера, а конфигурационном файле `zvk.ini` – корректные данные подключения к СУБД (в секции `[DBConnection]`) и Instance (в секции `[Key]`).
7. В случае обновления с ASUREO B9 SD2 HF3 удалить файл `RP.sms` из папки с файлами для новой версии. Убедиться, что в `docker-compose.yml` отсутствует строка пути маппинга для `RP.sms`.
8. 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 12.67.

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

Рисунок 12.67 – Команды для загрузки новых образов `docker load`

*Примечание: при загрузке образа могут возникнуть ошибки, если название файла содержит скобки, тире и т.д. В таком случае потребуется переименовать файл и заново попробовать загрузить образ.*

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

```
sudo docker image ls
```

Пример представлен на рисунке 12.68.

```
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 12.68 – 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)*

10. Изменить имя образа в `docker-compose.yml`. Убедиться, что:

- неиспользуемые `config.json` и `confighost.txt` закомментированы либо отсутствуют;
- присутствует строка пути маппинга для `zvkkey.lic` (Рисунок 12.69).

```

ZVK:
 image: asureo_linux:B9SD6_release
 container_name: asureo
 restart: always
network_mode: "host"
ports:
 - "8628:8628"
 - "8828:8828"
 - "9888:9888"
tty: true
volumes:
 - ./zvkkey.lic:/home/root/.wine/drive_c/server/zvkkey.lic
 - ./Logs:/home/root/.wine/drive_c/server/Logs
 - www:/home/root/.wine/drive_c/www
 - ./Zvk.ini:/home/root/.wine/drive_c/server/Zvk.ini
 - ./ckzv.ini:/home/root/.wine/drive_c/server/Events/ckzv/ckzv.ini
- ./config.json:/home/root/.wine/drive_c/migrator/config.json
- ./confighost.txt:/home/root/.wine/drive_c/www/SMSITLoader/confighost.txt
 - /etc/timezone:/etc/timezone:ro
 - /etc/localtime:/etc/localtime:ro
 - ./version.info:/home/root/.wine/drive_c/server/version.info
 - /etc/krb5.keytab:/etc/krb5.keytab
 - /etc/krb5.conf:/etc/krb5.conf

```

Рисунок 12.69 – Внесение корректировок в docker-compose.yml

11. Начиная с версии **ASUREO B9 SD10** для работы с интерфейсом веб-заявок необходим обязательный маппинг лицензионного ключа в docker контейнер веб-приложения и его последующее подключение в веб-конфигураторе.

Отредактировать файл docker-compose.yml, добавить строку с монтированием ключа \*.lic в контейнер веб-заявок (Рисунок 12.70).

```

services:
 asuweb:
 image: asu_web:v9sd10
 container_name: ASUREO-Net
 restart: always
network_mode: "host"
 networks:
 - asuNetwork
 tty: true
 extra_hosts:
 - "asuweb:10.111.11.13"
 environment:
 ASPNETCORE_ENVIRONMENT: Production
 TZ: Europe/Samara
 depends_on:
 - asu
 volumes:
 - sqlite:/configurator/app/web/sqlite
 - config:/zrp/app/web/wwwroot/Content/assets/config
 - ./zrpNet/appsettings.json:/configurator/app/web/appsettings.json
 - ./zrpNet/Sms.ZRP.WebApi.settings.json:/zrp/app/web/Sms.ZRP.WebApi.settings.json
 - ./zrpNet/AuthServer.settings.json:/identity/app/web/AuthServer.settings.json
 - ./Zvk.ini:/home/root/.wine/drive_c/server/Zvk.ini
 - ./zvkkey.lic:/zrp/app/web/zvkkey.lic
 - ./nginx-config/certs/nginx.crt:/etc/ssl/certs/ca-certificates.crt
 - ./zrpNet/Logs:/configurator/app/web/Logs
 - ./zrpNet/Logs:/zrp/app/web/logs
 - ./zrpNet/Logs:/identity/app/web/logs
 - /var/run/docker.sock:/var/run/docker.sock:ro
если нужны кейтабы - т.е. доменная аутентификация через Kerberos
- /etc/krb5.keytab:/etc/krb5.keytab

```

Рисунок 12.70 – Монтирование ключа в контейнер веб-заявок

12. Запустить docker контейнеры новой версии Системы, выполнив команду:

```
sudo docker-compose up -d
```

13. Проверить успешный запуск docker контейнеров путём вывода списка активных контейнеров, выполнив команду:

```
sudo docker ps
```

Пример представлен на рисунке 12.71.

```
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		ZVK-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	ZVK
d4179730ec58	nginx:alpine	"/docker-entryptoint...."	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 12.71 – Выполнение команды docker ps

14. Перейти на главную страницу Системы в браузере и открыть «Конфигуратор» (Рисунок 12.72).

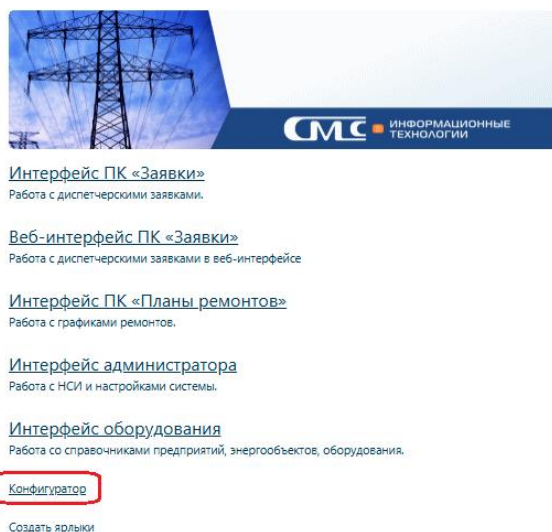


Рисунок 12.72 – Переход в конфигуратор веб-заявок

15. Перейти в раздел конфигуратора «Сервер приложений – Настройка интеграции», указать параметры лицензионного ключа в секции «Лицензирование» и нажать кнопку «Сохранить» (Рисунок 12.73). Параметры лицензионного ключа соответствуют таковым в секции [Key] файла Zvk.ini.

## Настройки

Системные настройки	Сервис интеграции с сервером приложений Delphi
Настройка оповещений	Включить интеграцию с сервером приложений Delphi: <input checked="" type="checkbox"/>
Настройка интеграций	Проксировать запросы создания/редактирования заявки в сервер приложений Delphi: <input checked="" type="checkbox"/>
Подключаемые функции	Проксировать запросы predetermined маршрутов в сервер приложений Delphi: <input checked="" type="checkbox"/>
	URL к интеграции:  http://asuweb:8625/SOAP
	<b>Лицензирование</b>
	Идентификатор лицензионного ключа:  asuweb
	Имя файла лицензионного ключа:  zvkey.lic
	Настройка взаимодействия с внешними сервисами
	Включено: <input type="checkbox"/>
Сохранить	
Перезагрузить контейнеры и сервисы	

Рисунок 12.73 – Указание параметров ключа в конфигураторе

16. Выполнить перезапуск docker контейнеров ПК «АСУРЭО» для применения изменений.

Выполнить команду: ***docker-compose down && docker-compose up -d*** (Рисунок 12.74).

```
sysadmin@ClusterPG-1:/opt/asureo$ docker-compose down && docker-compose up -d
```

Рисунок 12.74 – Выполнение команды docker-compose down &amp;&amp; docker-compose up -d

17. Проверить результат маппинга лицензионного ключа с помощью лог-файла веб-заявок ***backend-startup-%дана%.log*** (Рисунок 12.75).

```
22:03:32.221 [INF] Проверка лицензии на запуск сервера приложений .NET. Попытка 1 из 40
22:03:32.311 [INF] Запускаем сервер приложений ...
22:03:33.446 [INF] Инициализация справочника: SettingsStorage
22:03:33.467 [INF] Инициализация справочника: WorkTime
22:03:33.474 [INF] Инициализация справочника: ZVKCategory
22:03:33.481 [INF] Инициализация справочника: Enterprise
22:03:33.549 [INF] Инициализация справочника: EnterpriseAlias
22:03:33.557 [INF] Инициализация справочника: PredefinedRoute
22:03:34.402 [INF] Инициализация справочника: RepairType
22:03:34.413 [INF] Инициализация справочника: CondConstruction
22:03:34.416 [INF] Инициализация справочника: SwitchProgram
22:03:34.419 [INF] Инициализация справочника: AttributeGroup
22:03:34.421 [INF] Инициализация справочника: CommonAttribute
22:03:34.456 [INF] Инициализация справочника: Owner
22:03:34.462 [INF] Инициализация справочника: Territory
```

22:03:34.468 [INF] Инициализация справочника: ServiceGroup  
22:03:34.475 [INF] Инициализация справочника: ZVKUser  
22:03:34.483 [INF] Инициализация справочника: Holiday  
22:03:34.488 [INF] Инициализация справочника: GTPG  
22:03:34.493 [INF] Инициализация справочника: ZVKGroup  
22:03:34.501 [INF] Инициализация справочника: NoteType  
22:03:34.505 [INF] Инициализация справочника: Device  
22:03:35.011 [INF] Инициализация справочника: DeviceType  
22:03:35.022 [INF] Инициализация справочника: ContractorType  
22:03:35.025 [INF] Инициализация справочника: Contractor  
22:03:35.031 [INF] Инициализация справочника: PowerSystem  
22:03:35.035 [INF] Инициализация справочника: ZVKDeviceManagement  
22:03:35.075 [INF] Инициализация справочника: PowerObjectType  
22:03:35.080 [INF] Инициализация справочника: ZVKDeviceManagement  
22:03:35.424 [INF] Инициализация справочника: DeviceCompatibility  
22:03:35.435 [INF] Инициализация справочника: DeviceState  
22:03:35.494 [INF] Инициализация справочника: Roles  
22:03:35.565 [INF] Инициализация справочника: PowerObject  
22:03:35.579 [INF] Инициализация справочника: UserRole  
22:03:35.584 [INF] Инициализация справочника: ClassLink  
22:03:35.613 [INF] Инициализация справочника: Filter  
22:03:35.620 [INF] Инициализация справочника: UserNotificationSettings  
22:03:35.647 [INF] Инициализация справочника: Reglament  
22:03:35.687 [INF] Инициализация справочника: PrimaryZvkIds  
22:03:35.738 [INF] Инициализация справочника: ZVKRouteRule  
22:03:35.770 [INF] Инициализация справочника: DeviceVersion  
22:03:36.389 [INF] Сервер приложений успешно запущен.

Рисунок 12.75 – Пример успешной проверки лицензии веб-заявок

## **12.9 Последовательность действий на клиентах после обновления Системы**

При обновлении происходит разрыв связи с сервером приложений. Пользователю отображается модальное окно «Ошибка соединения с сервером приложений» (Рисунок 12.76).

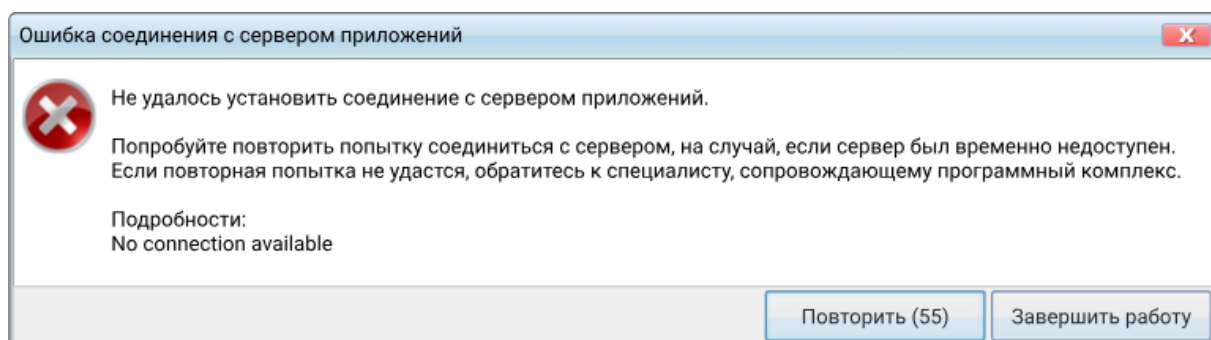


Рисунок 12.76 – Модальное окно «Ошибка соединения с сервером приложений»

По нажатию на кнопку «Повторить» форма закрывается и выполняется повторная попытка соединения с сервером приложений. При успешном соединении 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 Системы, ПО «Ремонты», Интерфейс оборудования, Интерфейс Администратора).

В случае, 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 12.77).

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.

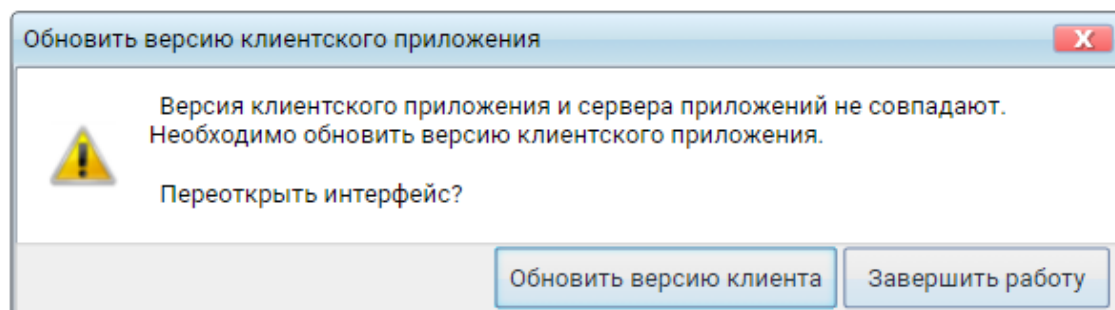


Рисунок 12.77 – Модальное окно «Обновить версию клиентского приложения»

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:*

### **Сценарий 1**

*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 обрабатывают. По нажатию на кнопки ничего не происходит.

## 12.10 Обновление 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](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](http://download.microsoft.com/download/6/7/D/67D80164-7DD0-48AF-86E3-DE7A182D6815/rewrite_2.0_rtw_x64.msi).

---

Для установки компонента прокси-перееадресации 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](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](http://download.microsoft.com/download/3/4/1/3415F3F9-5698-44FE-A072-D4AF09728390/ARRv2_setup_x64.EXE).

Для установки компонента прокси-перееадресации 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: Оперативный журнал и ПК «Метролог», если они были установлены ранее.

**Внимание!** При обновлении папка с установленным экземпляром должна быть **обязательно закрыта**. Если старая версия Системы 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 на СУБД PostgreSQL необходимо включить для пользователя опцию «Superuser». После завершения обновления опция должна быть выключена.

Обновление установленной версии Системы 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 «12.3 Установка Системы на СУБД MSSQL/PostgreSQL на ОС Windows»).

Для обновления необходимо в окне мастера «Выбор производных действий» выбрать пункт «Обновить экземпляры» и в списке «Установленные экземпляры» выбрать нужные экземпляры (Рисунок 12.78). Выбор нескольких экземпляров производится с помощью клавиш «Shift» или «Ctrl».

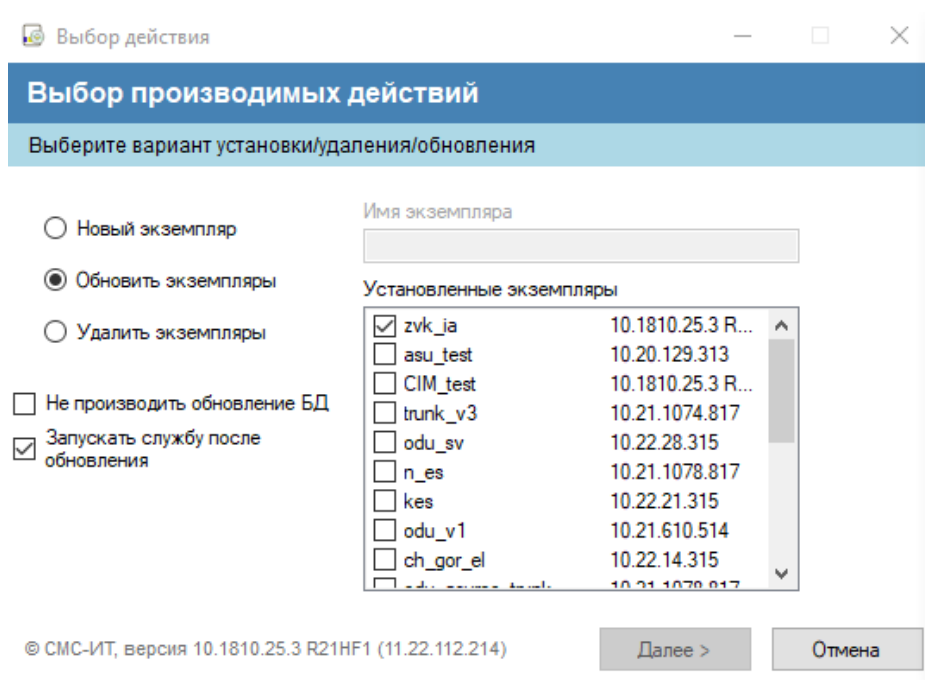


Рисунок 12.78 – Выбор экземпляров для обновления

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 12.79). По умолчанию установлены флаги «Планы ремонтов» и «ПК Заявки».

**Внимание!** При обновлении с версий В5, В6 и В7 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».

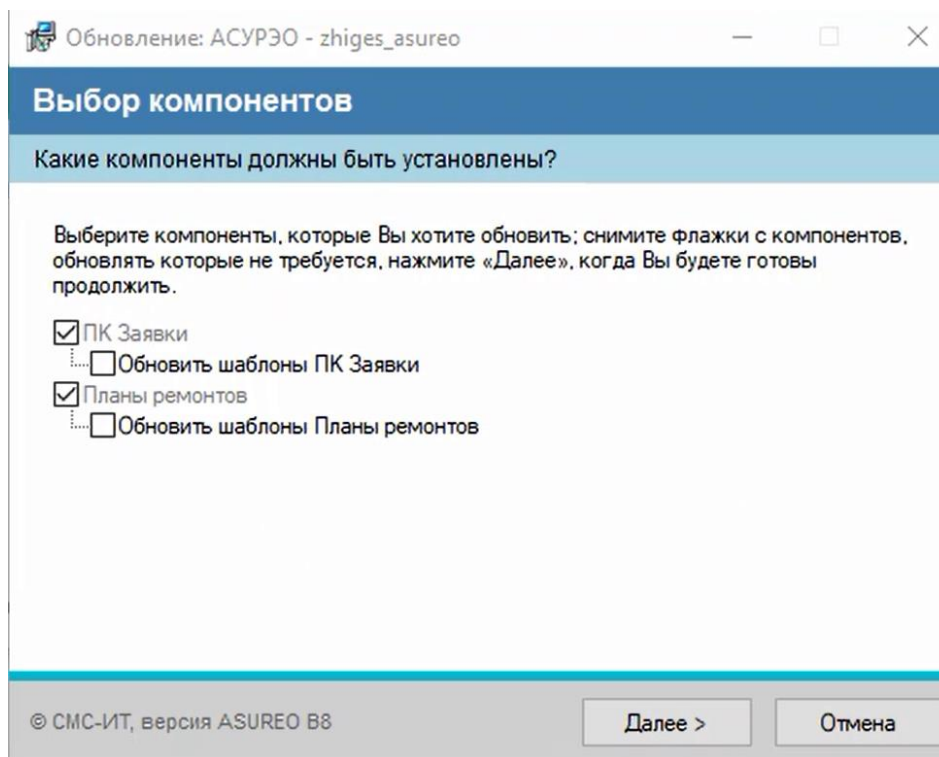


Рисунок 12.79 – Выбор компонентов обновления

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. Прогресс работы инсталлятора отображается на экране (Рисунок 12.80).

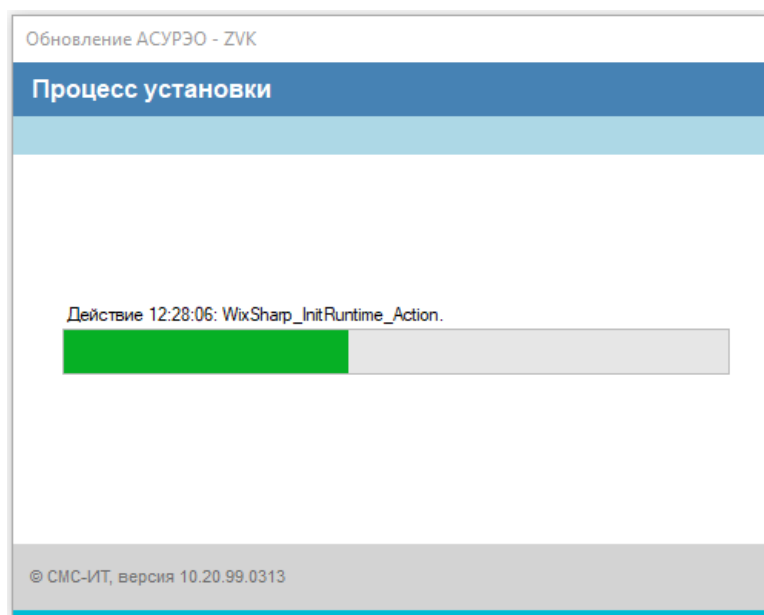


Рисунок 12.80 – Процесс обновления

По окончании процесса обновления для выбранных компонентов появляется окно завершения мастера установки (Рисунок 12.81).

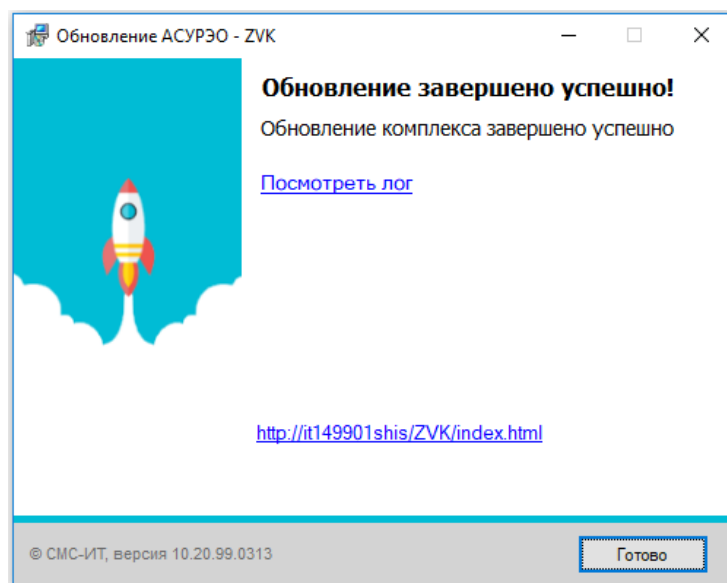


Рисунок 12.81 – Завершение обновления

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

**Внимание!** Начиная с версии 10.20.115.0313 часть параметров файла `instal.i.ini` переносится в системный реестр (Рисунок 12.82).

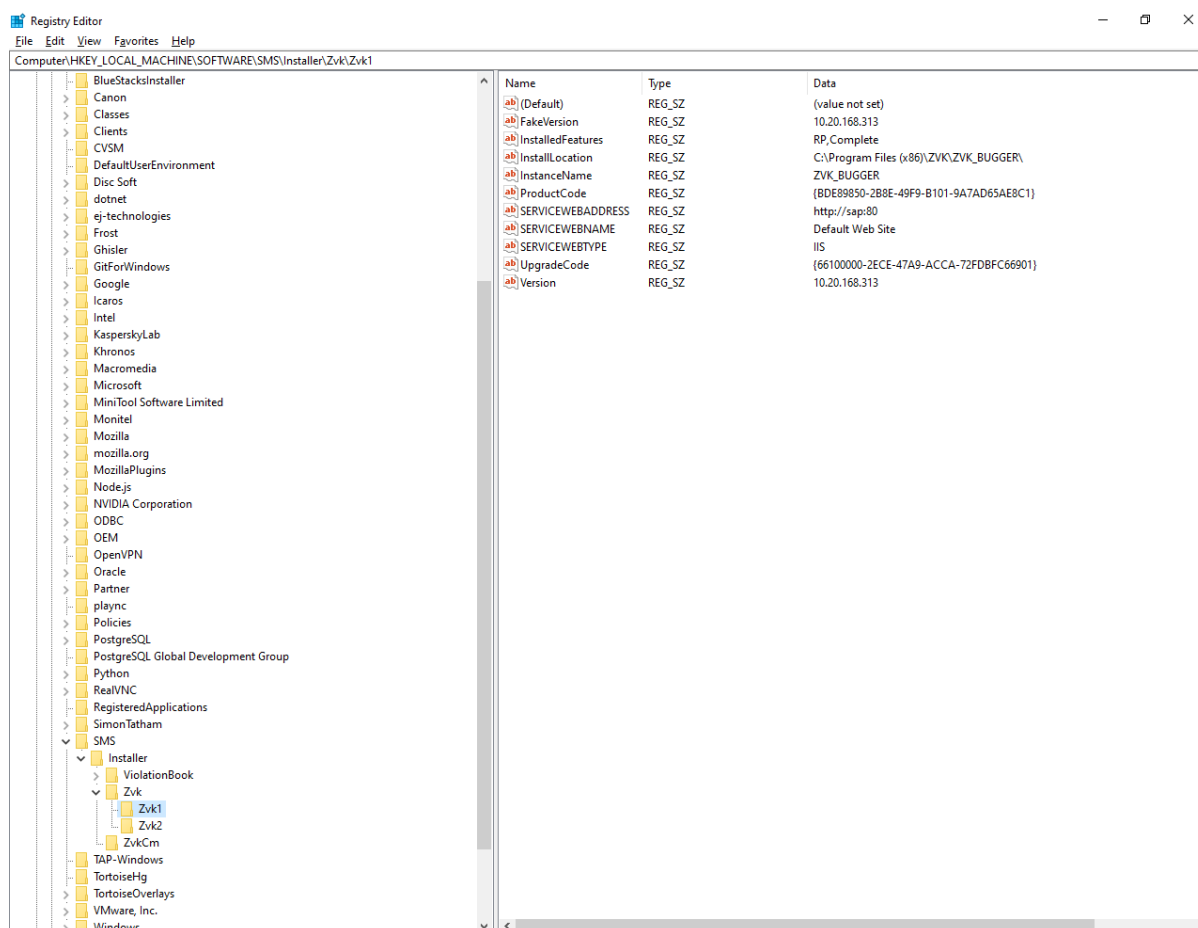


Рисунок 12.82 – Системный реестр

**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 12.83), 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 12.84). 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.

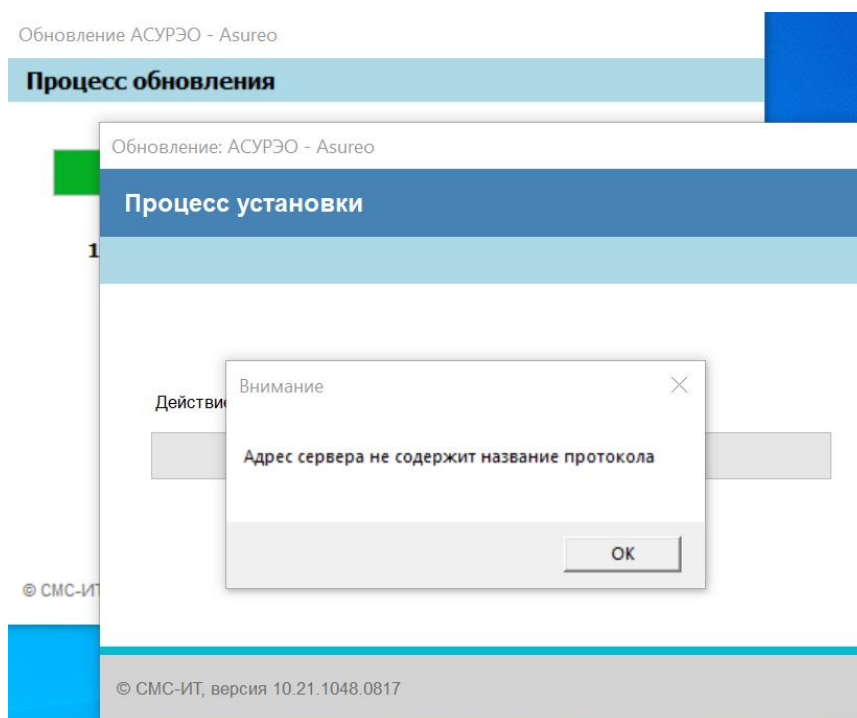


Рисунок 12.83 – Предупреждение

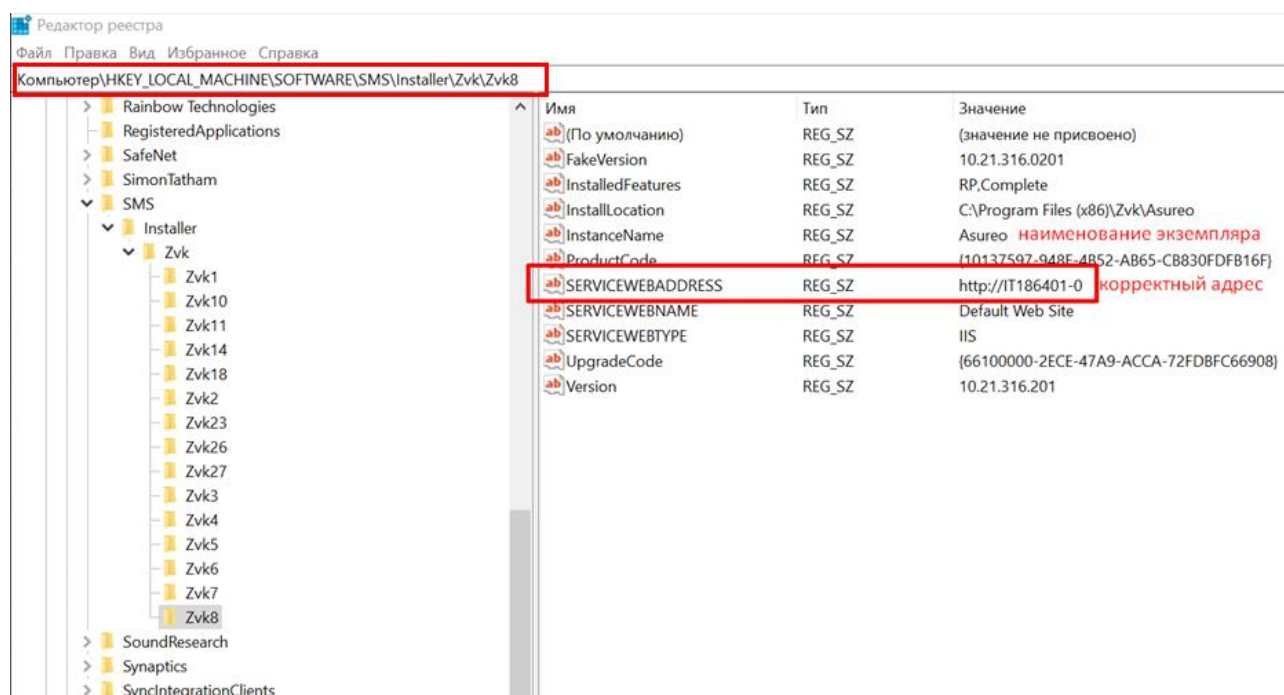


Рисунок 12.84 – Корректный полный адрес в реестре

## 12.11 Интеграция с Avanpost FAM

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

---

## 12.12 Проверка работоспособности ПК после установки

Для проверки работоспособности ПК после установки или обновления, 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, открыть любую заявку на просмотр.
4. Перейти в Интерфейс пользователя ПК «Планы ремонтов», открыть любой график на просмотр.

## 12.13 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 (см. раздел «16.3 Создание резервной копии базы данных в инструментарии PGAdmin»).
2. Деинсталлировать ПК (см. разделы «12.15 Удаление на ОС семейства Linux»).
3. Восстановить БД из резервной копии сделанной до обновления ПК (см. раздел «16.5 Восстановление БД из резервной копии в инструментарии PGAdmin»).
4. Установить ПК из комплекта поставки предыдущей версии (см. раздел «12.3 Установка Системы на СУБД MSSQL/PostgreSQL на ОС Windows», «12.4 Установка Системы на ОС семейства Linux»).
5. Проверить работоспособность установленного ПО.

## 12.14 Удаление на ОС MS Windows

Удаление ранее установленных экземпляров на ОС MS Windows может быть произведено с помощью программы установки ПК «*setup.exe*» (см. раздел «12.3 Установка Системы на СУБД MSSQL/PostgreSQL на ОС Windows»).

С помощью программы установки ПК «*setup.exe*» для удаления экземпляров необходимо в окне мастера «*Выбор производимых действий*» выбрать пункт «*Удалить экземпляры*» и в списке «*Установленные экземпляры*» выбрать нужные экземпляры (Рисунок 12.85). Выбор нескольких экземпляров производится с помощью клавиш «*Shift*» / «*Ctrl*».

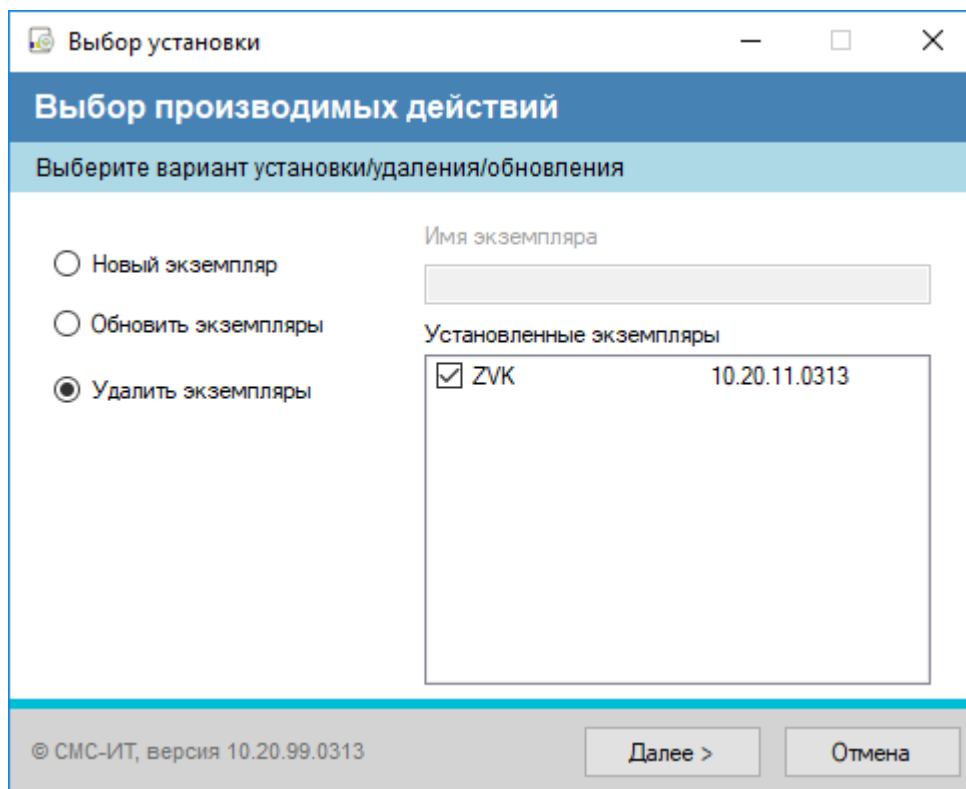


Рисунок 12.85 – Выбор экземпляра для удаления

На следующем шаге, если установить флаг «*Удалить файлы пользователя*» (по умолчанию – установлен), то производится удаление всех файлов из каталога установки экземпляра (Рисунок 12.86). Если флаг снят, то созданные пользователем файлы в директории экземпляра и журнала сервера приложений не удаляются. Удаление БД, с которой работал экземпляр, не производится.

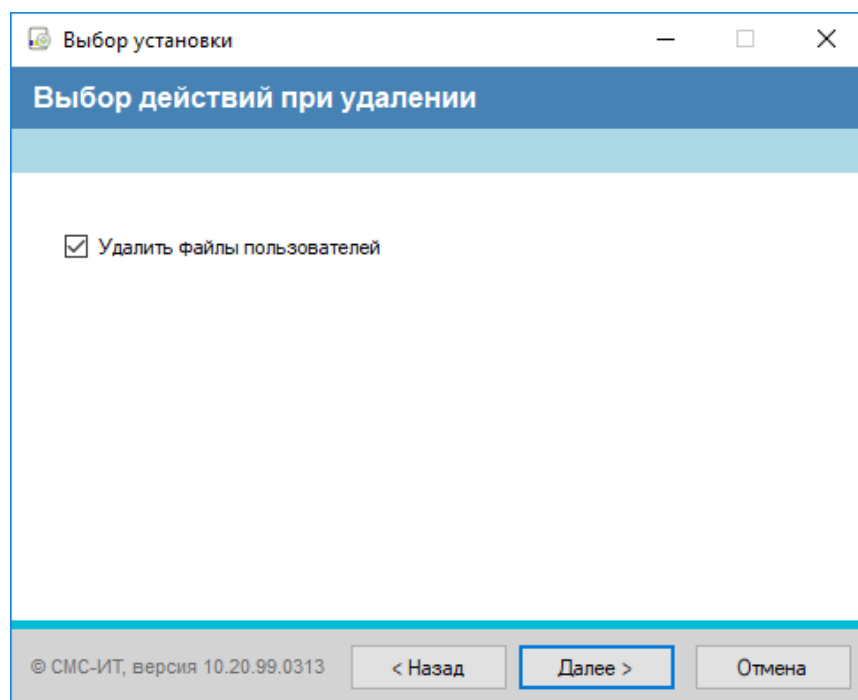


Рисунок 12.86 – Установка флага «Удалить файлы пользователей»

По окончании процесса удаления выбранных экземпляров появляется окно завершения мастера установки (Рисунок 12.87).

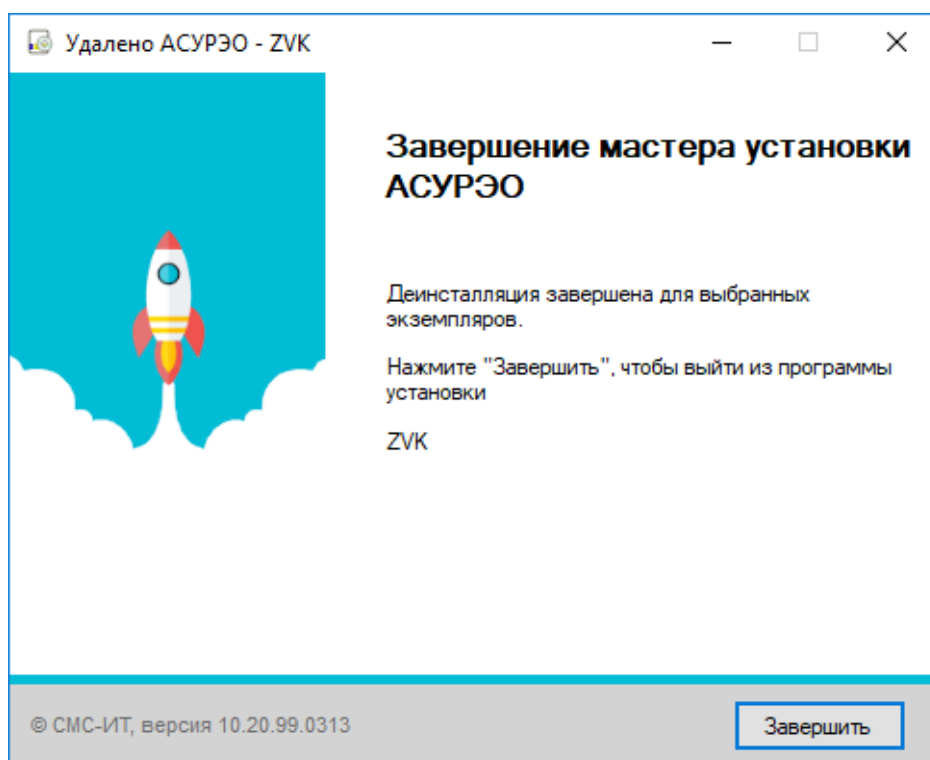


Рисунок 12.87 – Завершение удаления

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

## 12.15 Удаление на ОС семейства Linux

Удаление ранее установленного экземпляра на ОС семейства Linux может быть произведено путём удаления docker-контейнеров и docker образа. Для удаления необходимо выполнить следующие действия:

1. Вывести весь список docker контейнеров. Выполнить команду: *docker ps* (Рисунок 12.88).

```
sysadmin@ClusterPG-1:/opt/asureo$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED
STATUS	PORTS	NAMES	
SD8ad1e703e50	asu:v9sd9_release	"/home/root/docker-e..."	9 seconds ago
Up 8 seconds	0.0.0.0:8625->8625/tcp	asureo	

Рисунок 12.88 – Выполнение команды *docker ps*

2. Остановить и удалить действующий docker контейнер с удалением volume. Выполнить команду: *sudo docker-compose down -v* (Рисунок 12.89).

```
sysadmin@ClusterPG-1:/opt/asureo$ sudo docker-compose down -v
Stopping asureo ... done
Removing asureo ... done
Removing volume asureo_www
```

Рисунок 12.89 – Выполнение команды остановки контейнера

3. Очистить каталог */opt/asureo/www*: *sudo rm -r /opt/asureo/www/\** (Если этот каталог расположен в */opt/asureo*, если нет, то скорее всего каталог уже очищен предыдущей командой в системных каталогах докера).
4. Вывести список docker образов. Выполнить команду: *docker images* (Рисунок 12.90).

```
sysadmin@ClusterPG-1:/opt/asureo$ docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
asureo_linux	B9SD9_release	e397f47dfbf0	1 week ago	4.13GB

Рисунок 12.90 – Выполнение команды *docker images*

5. Удалить docker образ. Выполнить команду: *sudo docker rmi <имя:тег>* (Ваше имя образа может отличаться) (Рисунок 12.91).

```
sysadmin@ClusterPG-1:/opt/asureo$ sudo docker rmi asureo_linux:B9SD9_release
Untagged: asureo_linux:B9SD9_release
Deleted: sha256:e397f47dfbf0ec6e6174ea6a3d5e3c79664e889240ff6653b1277c7c7a053cb1
```

Рисунок 12.91 – Выполнение команды удаления docker образа

- 
6. Удалить папку `/opt/asureo`. Выполнить команду: `rm -r /opt/asureo` (Рисунок 12.92).

```
sysadmin@ClusterPG-1:/opt/asureo$ rm -r /opt/asureo
```

Рисунок 12.92 – Выполнение команды `rm -r /opt/asureo`

---

## 13 Настройка клиентского рабочего места

### 13.1 Настройка ClickOnce при изменении параметров веб-сервера

#### 13.1.1 Общие сведения

Установка клиента 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 Системе по протоколу https или изменился путь, по которому происходит подключение к Системе, необходимо пересобрать ClickOnce.

#### 13.1.2 Пересборки ClickOnce на MS Windows

1. Сделать резервную копию папки Системы.
2. Остановить службу Системы.
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 Системы и проверить запуск интерфейсов.

В случае необходимости возврата к изначальным настройкам необходимо:

1. Остановить службу Системы.
2. Скопировать из резервной копии содержимое папки Системы.
3. Запустить службу Системы и проверить запуск интерфейсов.

Для корректной работы 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 13.1).

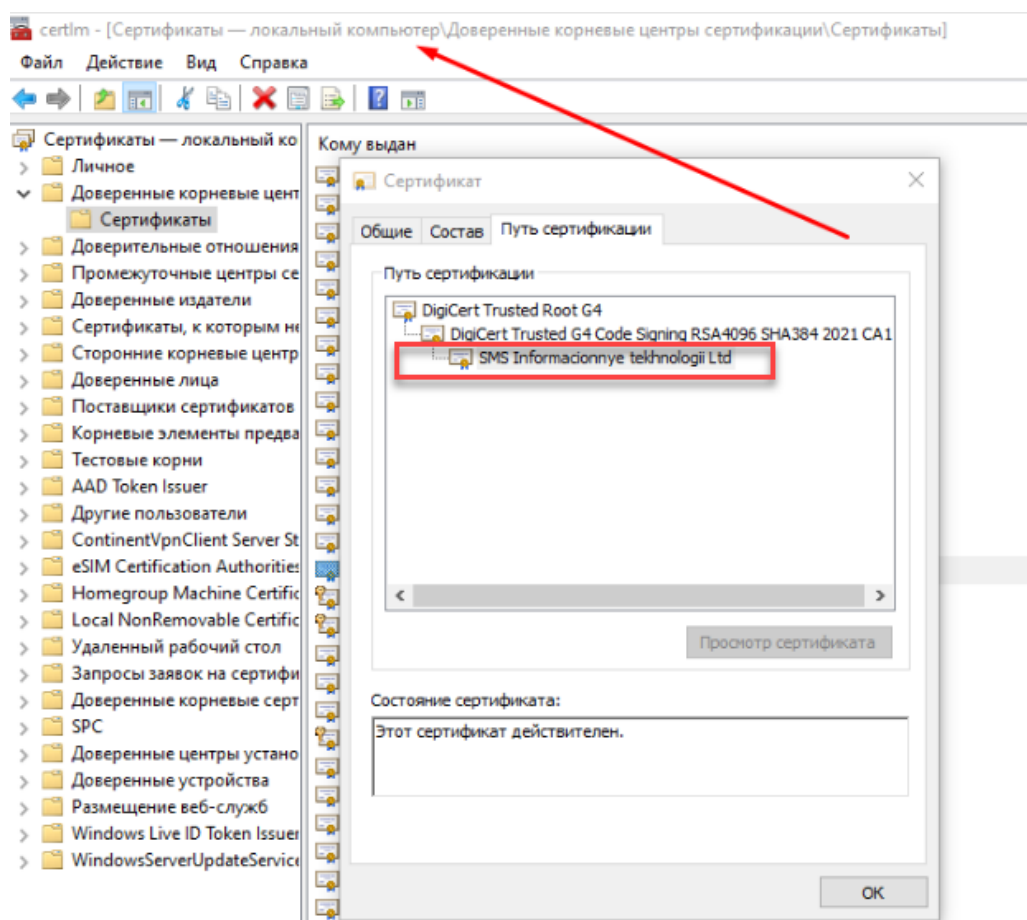


Рисунок 13.1 – Управление сертификатами

### 13.1.3 Пересборка ClickOnce на Linux

1. В серверной директории остановить контейнеры командой `sudo docker-compose down -v`.
2. При наличии директории `www` очистить её содержимое `sudo rm -rf www/*`.
3. Сделать бэкап файла `zvk.ini`.
4. В конфигурационный файл `zvk.ini` в строку `#ApplicationUrl` внести изменённую строку подключения.
5. Запустить контейнеры командой `sudo docker-compose up -d`. Дождаться сборки приложений ClickOnce и старта сервера приложений.

В случае необходимости возврата к изначальным настройкам необходимо:

1. В серверной директории остановить контейнеры командой `sudo docker-compose down -v`.
2. При наличии директории `www` очистить её содержимое `sudo rm -rf www/*`.

- 
3. Восстановить из бэкапа старый файл zvz.ini.
  4. Запустить контейнеры и дождаться сборки приложений ClickOnce и старта сервера приложений.

## **13.2 Настройка клиентского рабочего места и установка клиентской части Системы на MS Windows**

### **13.2.1 Настройка 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 13.2).



При использовании браузеров Yandex, Edge, Chrome клиентские интерфейсы скачиваются каждый раз в загрузки и их необходимо запускать вручную (Рисунок 13.3).

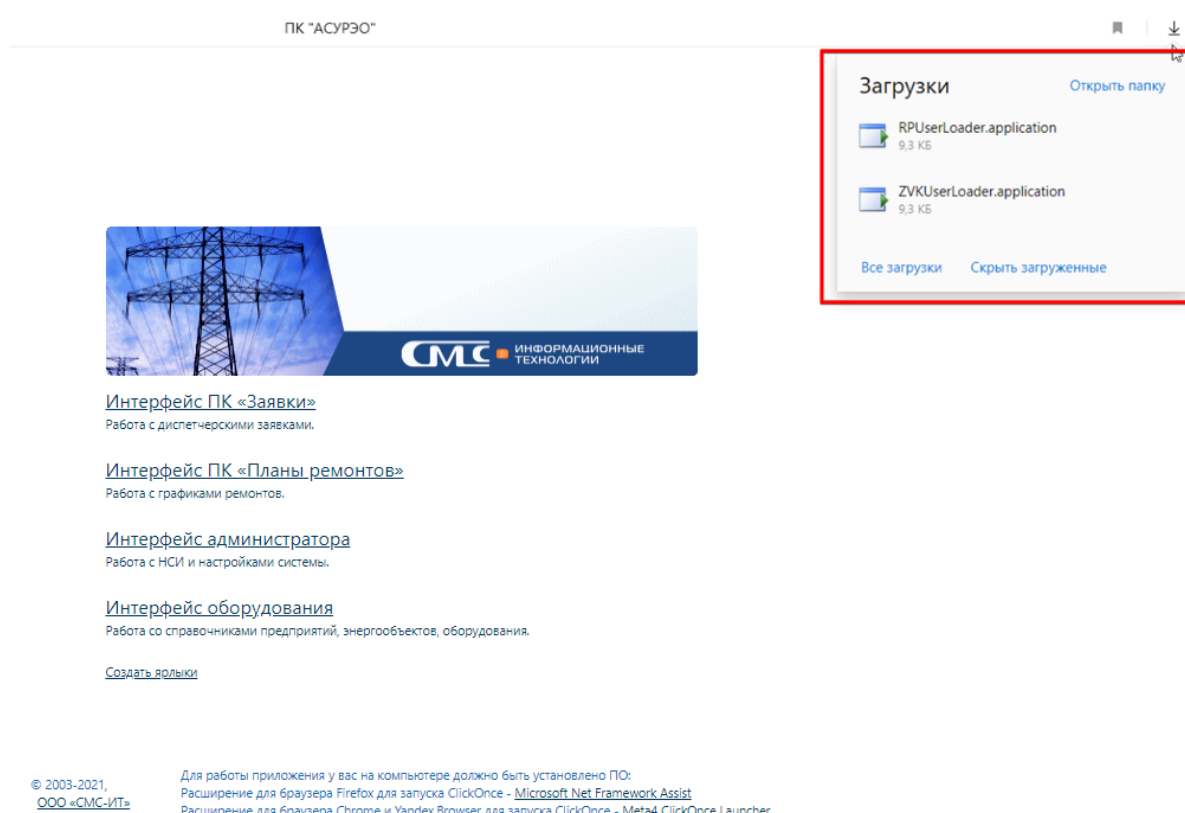


Рисунок 13.3 – Загрузки

При открытии файла загрузки открывается окно установки выбранного приложения (Рисунок 13.4).

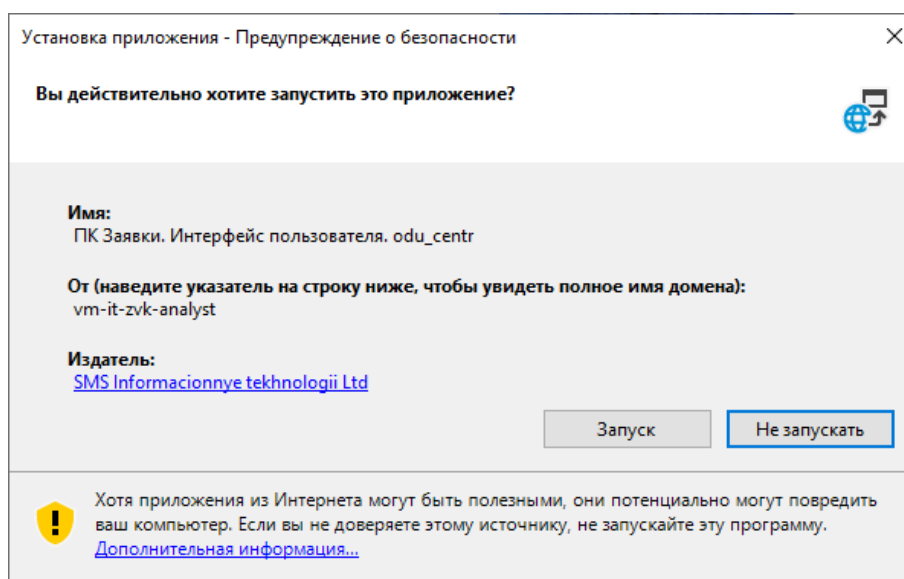


Рисунок 13.4 – Окно установки приложения

Для подтверждения запуска выбранного приложения необходимо нажать кнопку «Запуск». После подтверждения запуска начинается скачивание выбранного приложения (Рисунок 13.5).

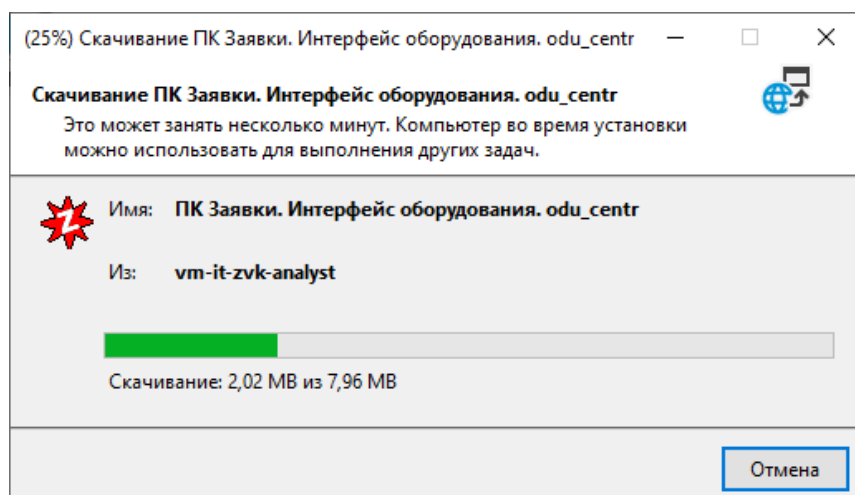


Рисунок 13.5 – Скачивание приложения

При скачивании клиентских интерфейсов Системы в ОС семейства Linux появляется предупреждение Windows о неопознанном приложении (Рисунок 13.6). Для успешного запуска приложения необходимо нажать кнопку «*Выполнить в любом случае*». Отображение такого предупреждения является корректным для ОС семейства Linux.

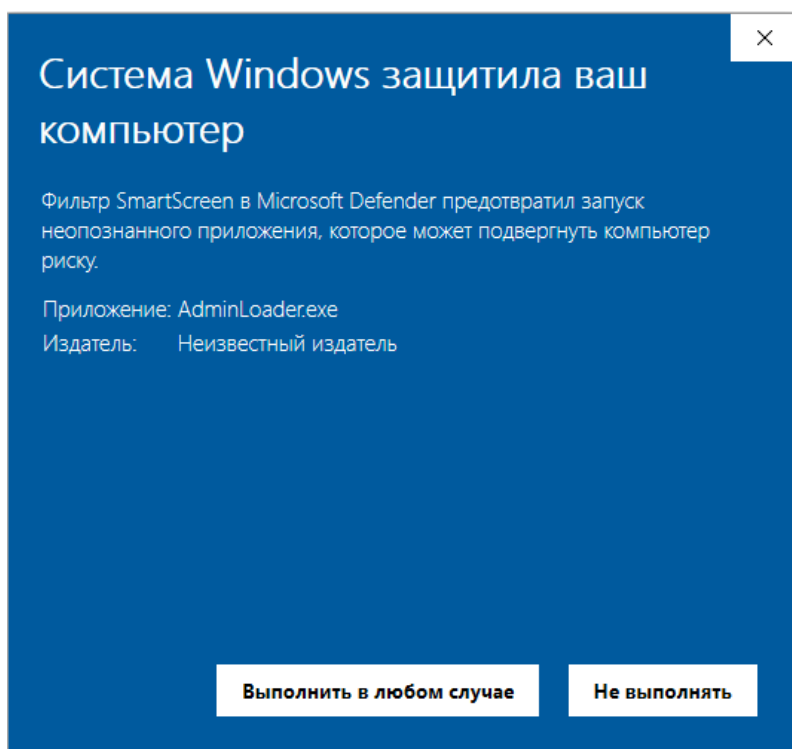


Рисунок 13.6 – Предупреждение Windows о неопознанном приложении

### 13.2.3 Первый запуск ПК на рабочей станции

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 подсистемы, пользователю предлагается установка компонентов программного комплекса на клиенте (Рисунок 13.7).

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



Рисунок 13.7 – Установка подсистемы на клиенте

После перехода по ссылке открывается окно установки приложения (Рисунок 13.8).

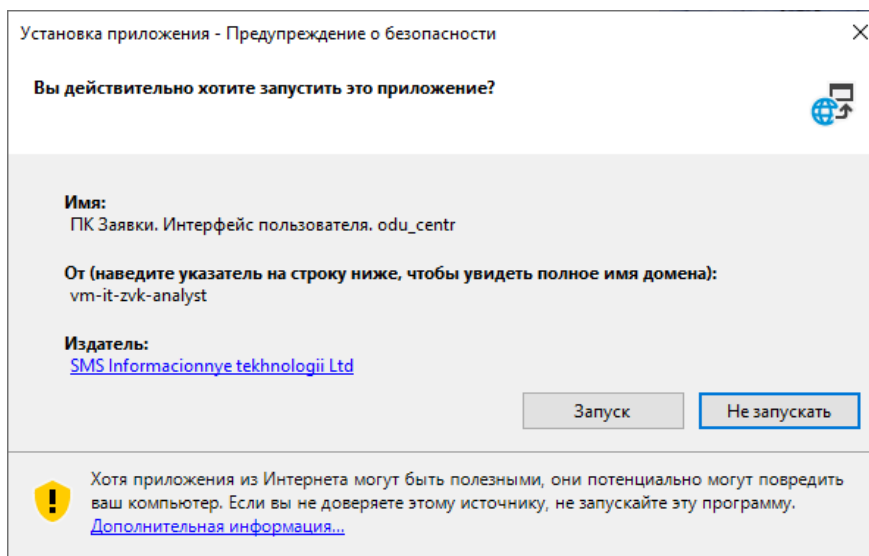


Рисунок 13.8 – Окно установки приложения

Для подтверждения запуска установки приложения необходимо нажать кнопку «Запуск». После подтверждения запуска начинается скачивание выбранного приложения (Рисунок 13.9). Для отмены запуска установки выбранного приложения необходимо нажать на кнопку «Не запускать».

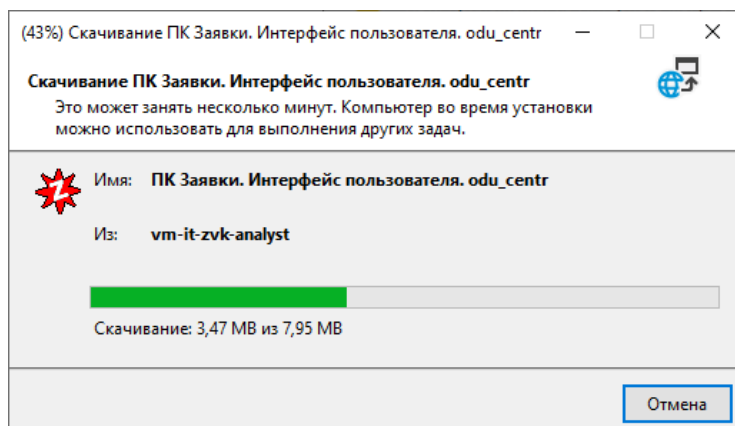


Рисунок 13.9 – Скачивание приложения

После чего запускается процесс установки приложения на рабочую станцию пользователя (Рисунок 13.10).

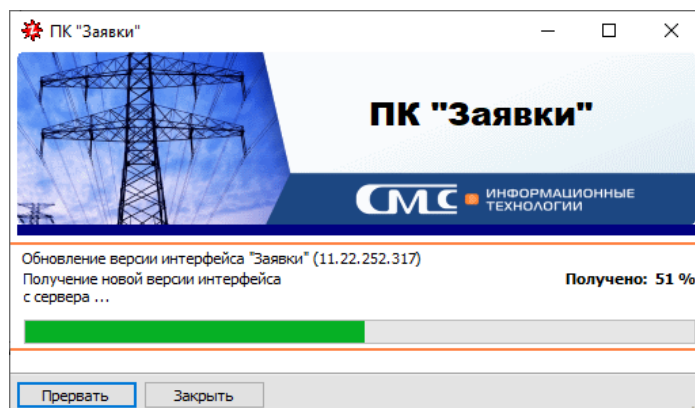


Рисунок 13.10 – Установка приложения

В процессе получения информации с сервера, если нажать на кнопку «Прервать», то скачивание приостановится, кнопка изменится на «Повторить» (Рисунок 13.11).

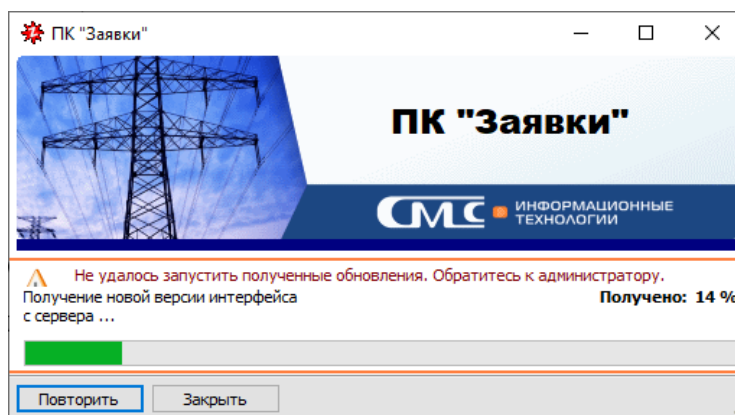


Рисунок 13.11 – Прерывание процесса загрузки обновлений

---

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 компьютере 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.

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 «V9.XXXX.XX.XX», «V10.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, «V11.XXXX.XX.XX»).
- В случае, если в директории ZVK хранятся файлы для трех версий подсистемы (например, в папках «V8.XXXX.XX.XX», «V9.XXXX.XX.XX» и «V10.XXXX.XX.XX»), то при обновлении подсистемы из директория ZVK автоматически удаляется папка с файлами для наиболее ранней версии (в данном примере папка «V8.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, «V11.XXXX.XX.XX»).

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 подсистемы.

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 13.12).

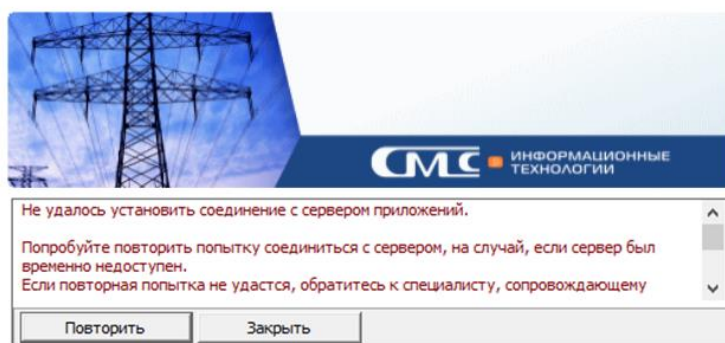


Рисунок 13.12 – Ошибка при получении пакета установки с сервера

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 подсистемы, соответствующая версии подсистемы на сервере. В папке содержатся файлы приложений, относящиеся к данной версии.

**Пример:**

C:\ProgramData\ZVK\V10.1810.25.3\ – каталог, содержащий файлы интерфейсов ПК версии 10.1810.25.3.

DeviceDescr.exe	– файлы интерфейсов оборудования,
ZVKAdmin.exe	администратора и пользователя для версии
ZVKUser.exe	10.1810.25.3.
alert.wav	– файл звукового оповещения о приходе новых заявок для рассмотрения (подгружается вместе с ZVKUser.exe).

После загрузки с сервера компонентов интерфейса на рабочей станции пользователя открывается окно подсистемы с приглашением входа в приложение (Рисунок 13.13). В окне необходимо ввести имя и пароль пользователя.

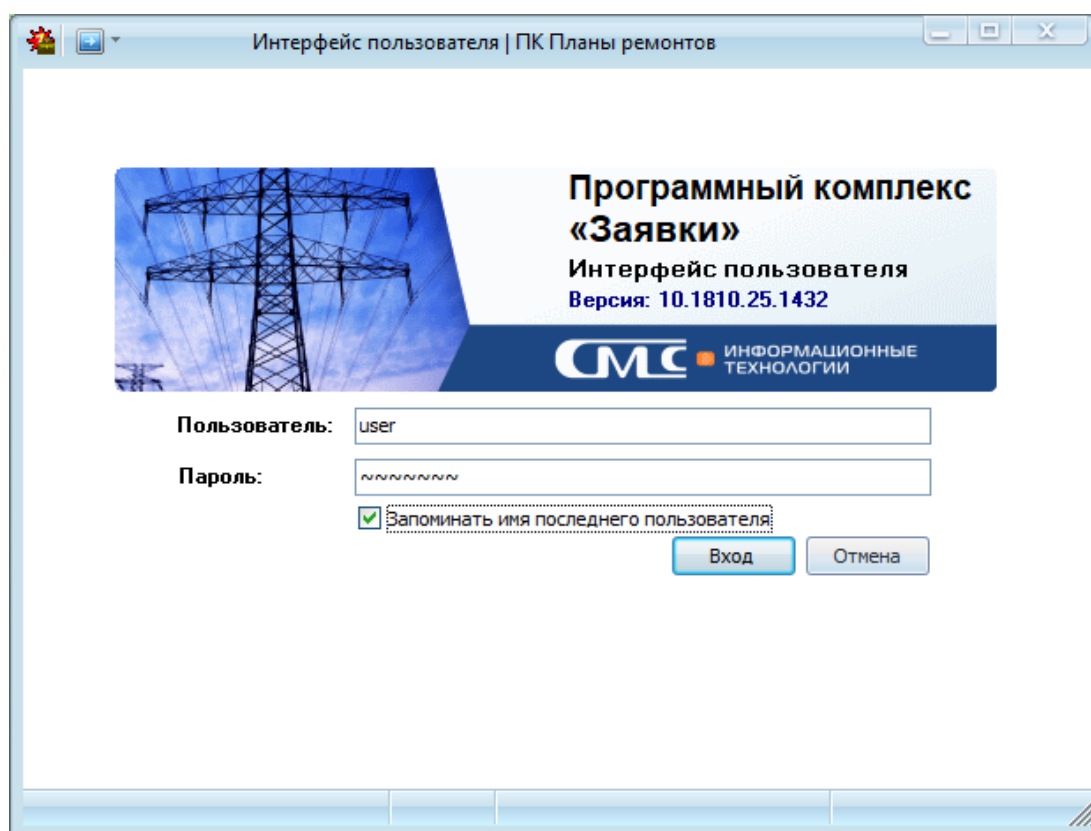


Рисунок 13.13 – Диалоговое окно входа в систему

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 «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 Системы 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.

### 13.2.4 Создание 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 13.14).

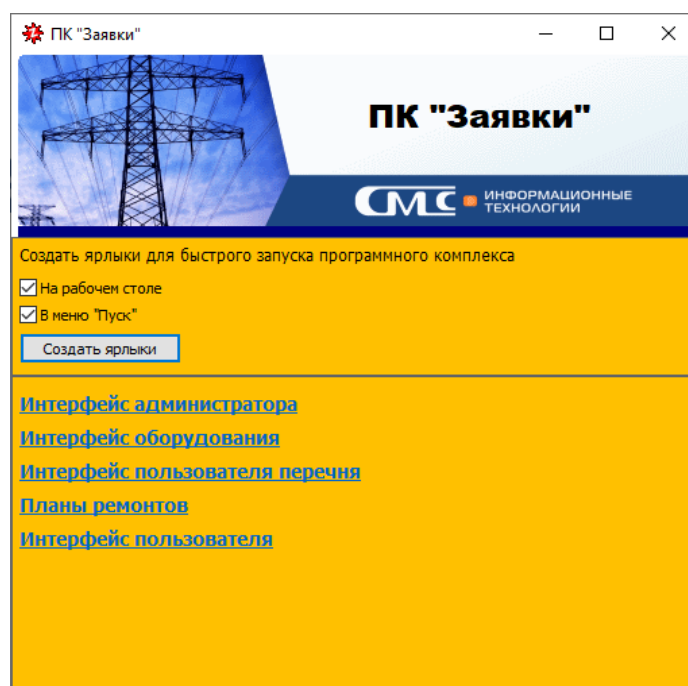


Рисунок 13.14 – Создание ярлыка

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 подсистемы в ней создаются ярлыки для запуска интерфейса пользователя, администратора, оборудования и пользователя подсистемы «Ремонты».

---

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 подсистемы «Ремонты» необходимо провести вручную. Для этого необходимо скопировать их из меню Пуск / Программы / Подсистема «Заявки» (Рисунок 13.15).

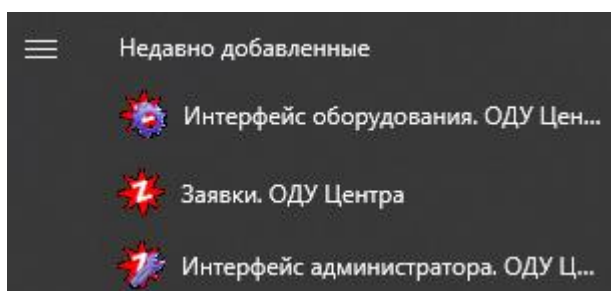


Рисунок 13.15 – Ярлыки интерфейсов в меню «Пуск»

Пользователь также может создать себе на компьютере ярлык интерфейса пользователя ЗРП.Net для быстрого запуска интерфейса пользователя в Яндекс браузере.

Для этого необходимо выполнить следующие шаги:

**Способ 1** (Рисунок 13.16)

1. Открыть нужную страницу в Яндекс браузере.
2. Нажать на меню в правом верхнем углу (три горизонтальные линии).
3. Выбрать пункт «Дополнительно».
4. В раскрывающемся меню выбрать опцию «Добавить страницу на рабочий стол».
5. Подтвердить создание – ярлык появится на рабочем столе.

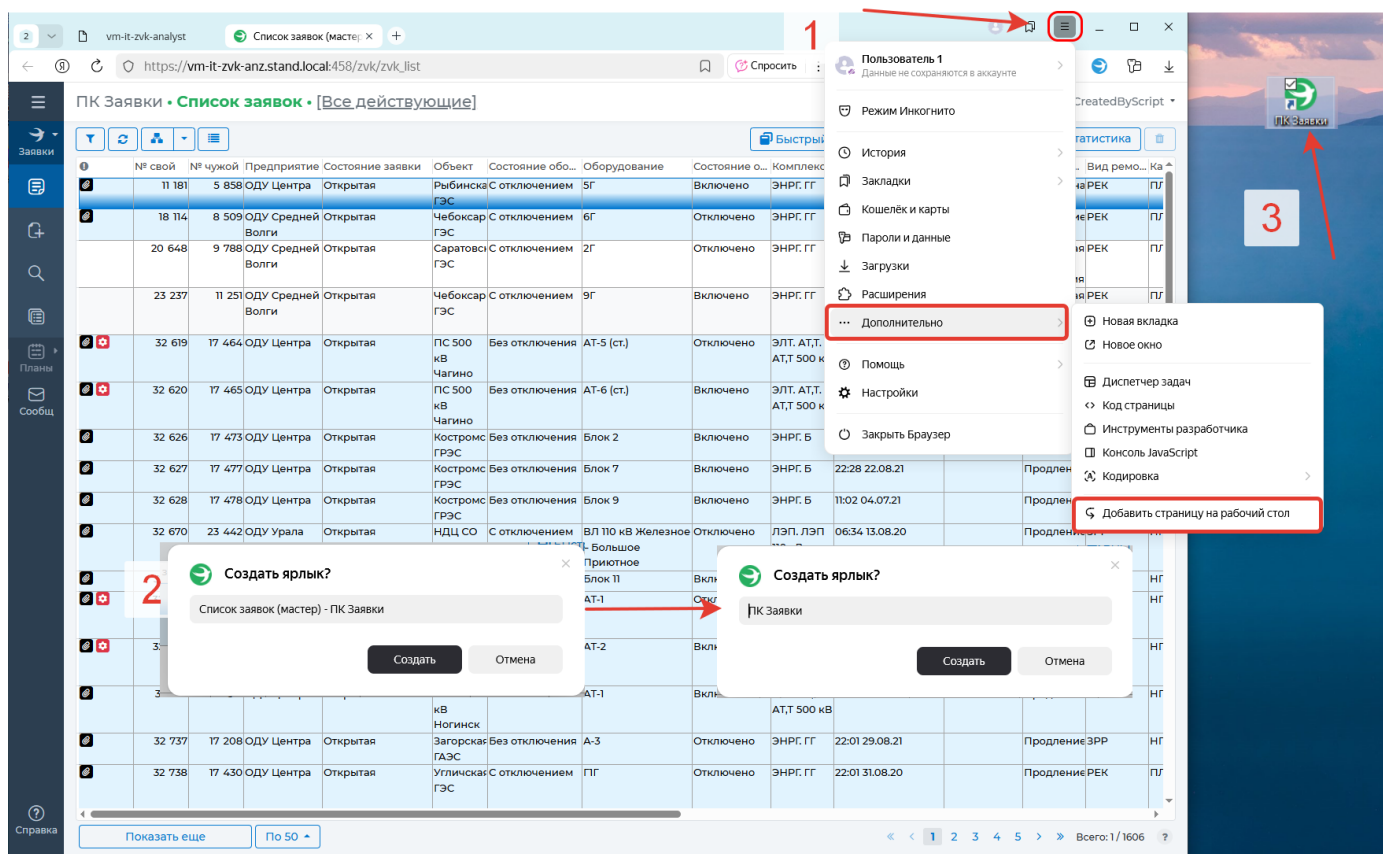


Рисунок 13.16 – Создание ярлыка в Яндекс браузере (1 способ)

### Способ 2 (Рисунок 13.17)

1. Открыть нужную страницу в Яндекс браузере.
2. Нажать на меню в правом верхнем углу (три горизонтальные линии).
3. Выбрать пункт «Дополнительно».
4. В раскрывающемся меню выбрать пункт «Дополнительные инструменты».
5. В раскрывающемся меню нажать на «Добавить страницу на Рабочий стол».
6. Подтвердить создание – ярлык появится на рабочем столе.

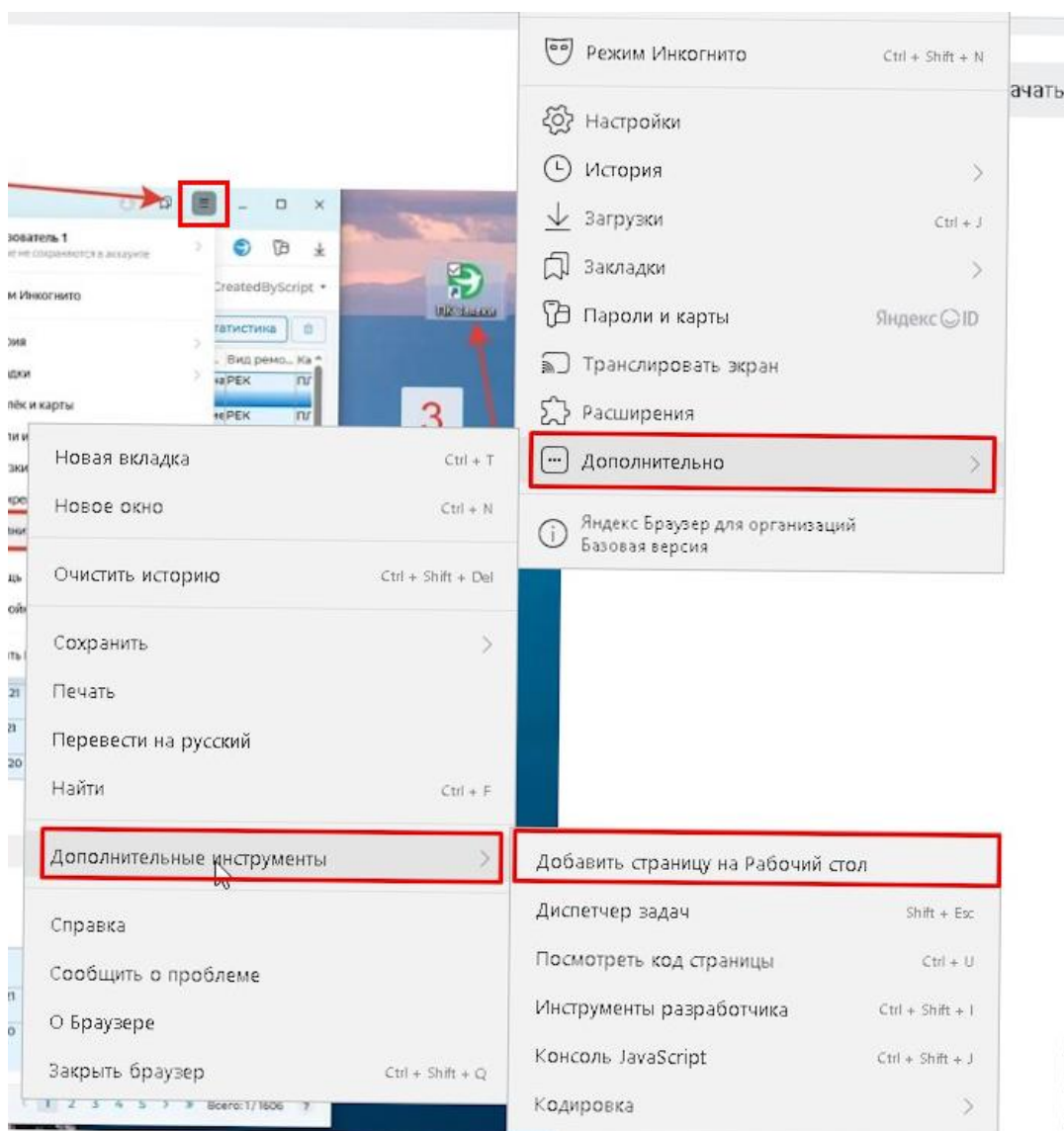


Рисунок 13.17 – Создание ярлыка в Яндекс браузере (2 способ)

### 13.2.5 Проверка настроек прокси-сервера перед обновлением клиентской части ПК

Для обеспечения успешного проведения обновления Системы необходимо выполнить проверку настроек прокси-сервера:

1. Проверить работоспособность прокси-сервера.

Перед началом обновления необходимо убедиться, что прокси-сервер, указанный в настройках, доступен и функционирует корректно.

- Если прокси-сервер работает, то дополнительных действий не требуется.
- Если прокси-сервер не работает, то необходимо отключить использование прокси-сервера в настройках на всех клиентских машинах. Обновление при неработающем прокси и активной соответствующей настройке пройдет успешно. Однако после

завершения обновления все клиентские машины столкнутся с ошибкой при запуске, так как будут пытаться подключиться к недоступному прокси-серверу.

## 2. Проверить аутентификацию на прокси-сервере.

Если для подключения к прокси-серверу требуется аутентификация (логин и пароль), то необходимо заранее предпринять одно из следующих действий:

Вариант 1: Отключить аутентификацию навсегда.

Обновление пройдет успешно. Однако после завершения обновления все клиентские машины столкнутся с ошибкой при запуске, так как не смогут авторизоваться.

Вариант 2: Настроить учетные данные на каждом клиенте.

Если отключение аутентификации невозможно, необходимо вручную прописать логин и пароль для прокси на каждой клиентской машине. Данные указываются в файле `zvkuser.dat`.

Убедитесь, что в данном файле присутствуют актуальные и корректные учетные данные для доступа к прокси-серверу.

### 13.2.6 Обновление 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 13.18).

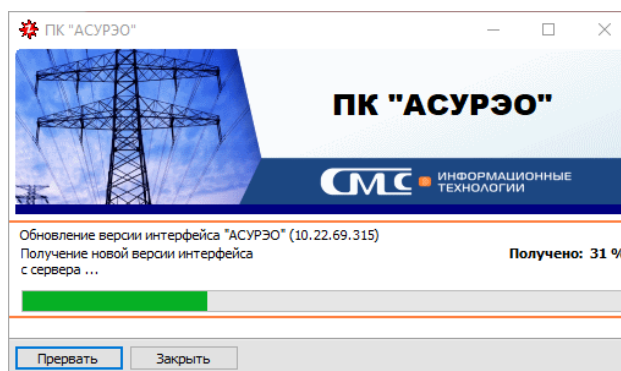


Рисунок 13.18 – Загрузка компонентов интерфейса пользователя с сервера

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:

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

### 13.2.7 Хранимые 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 «14.2 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.

### 13.3 Установка клиентской части Системы на ОС Astra Linux

Для установки клиентов Системы 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 13.19).

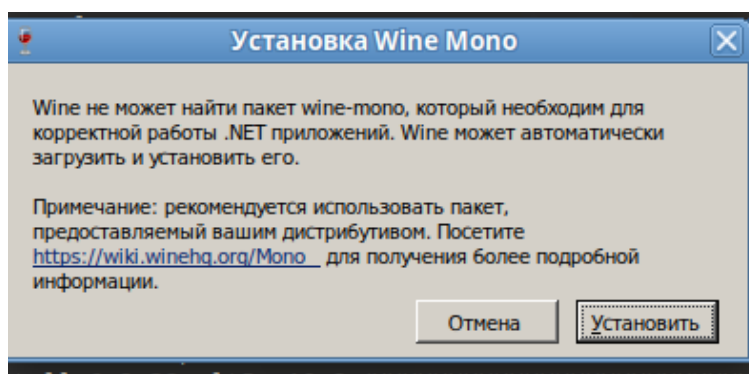


Рисунок 13.19 – Всплывающее окно «Wine Mono»

- Принять лицензионное соглашение и нажать кнопку «Установить» (Рисунок 13.20), после установки нажать кнопку «Готово» (Рисунок 13.21).

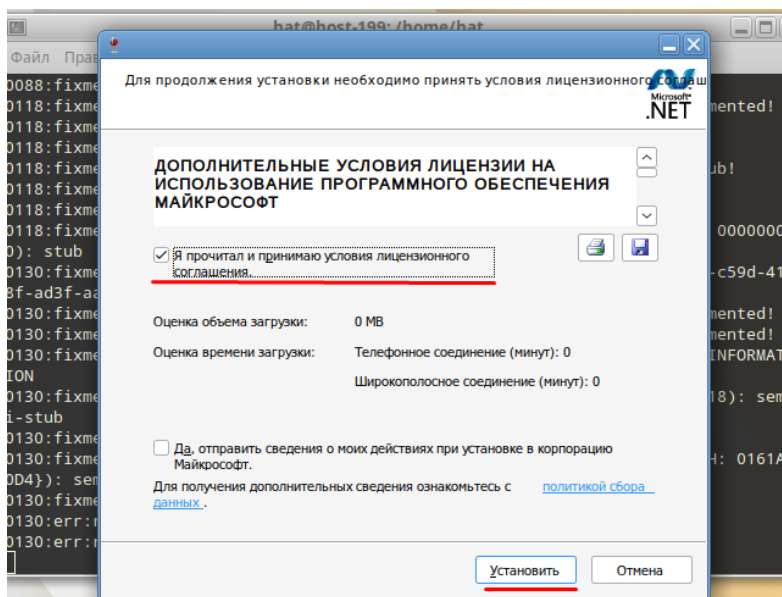


Рисунок 13.20 – Принятие лицензионного соглашения

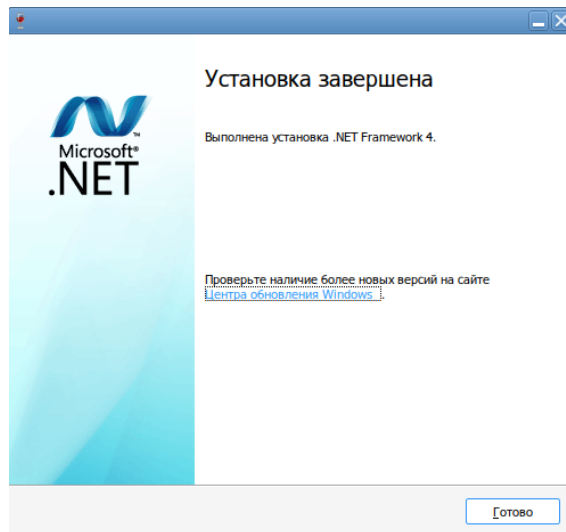


Рисунок 13.21 – Завершение установки

- Далее в окне «Майкрософт .NET Framework 4.5» нажать кнопку «Продолжить» (Рисунок 13.22).

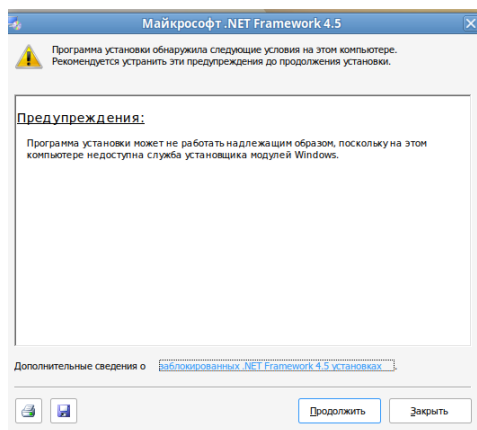


Рисунок 13.22 – Окно «Майкрософт .NET Framework 4.5»

- Принять лицензионное соглашение и нажать на кнопку «Установить» (Рисунок 13.23).

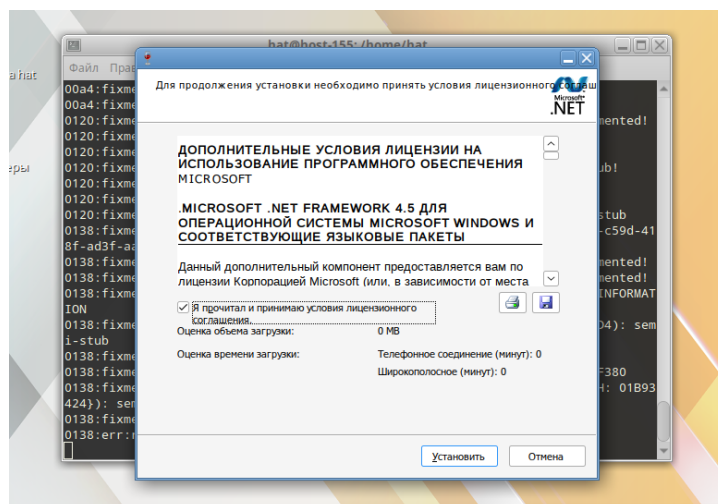


Рисунок 13.23 – Принятие лицензионного соглашения

- Скачать интерфейс ПК «Заявки» с индексной страницы (Рисунок 13.24).

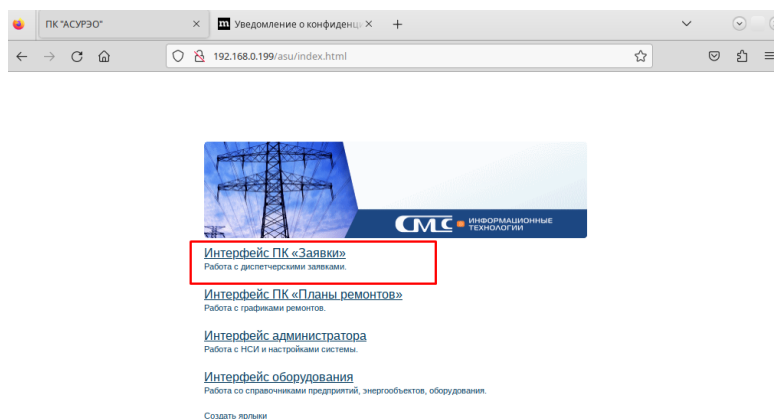


Рисунок 13.24 – Скачивание интерфейса

- Запустить приложение:  
**wine /home/\$USER/Загрузки/ZvkUserLoader.application**

Либо открыть проводник – **wine explorer**, и запустить интерфейс двойным нажатием (Рисунок 13.25).

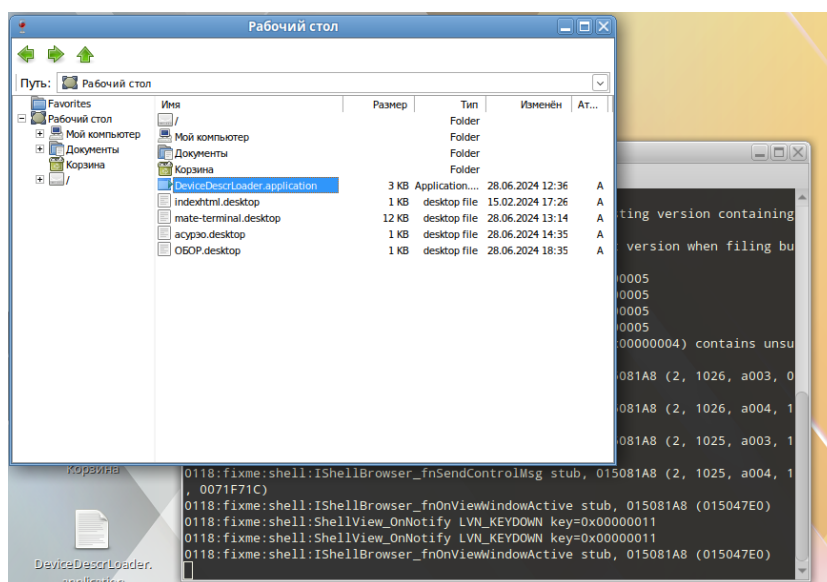


Рисунок 13.25 – Запуск интерфейса

- 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 13.26):

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

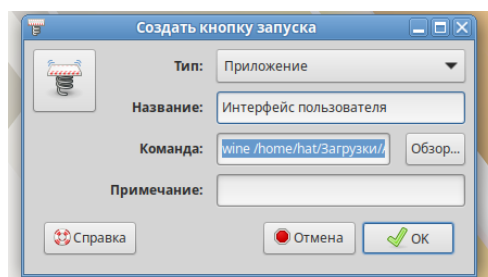


Рисунок 13.26 – Создание кнопки запуска

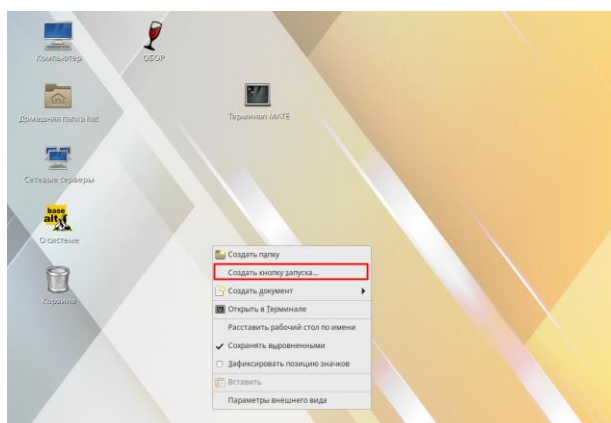


Рисунок 13.27 – Создание кнопки запуска

- Пользователь заходит в Интерфейс пользователя через ярлык (Рисунок 13.28).

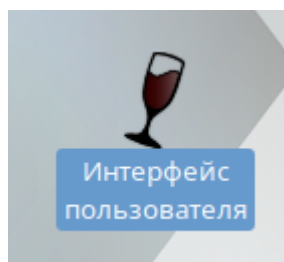


Рисунок 13.28 – Ярлык Интерфейса пользователя

Для устранения проблемы мерцания пользовательского интерфейса при работе приложения в среде Wine необходимо выполнить следующую настройку:

1. Открыть Wine Configuration (Настройки Wine).
2. Перейти во вкладку «Графика».
3. В разделе «Настройки окон» установить параметры, представленные на рисунке 13.29.

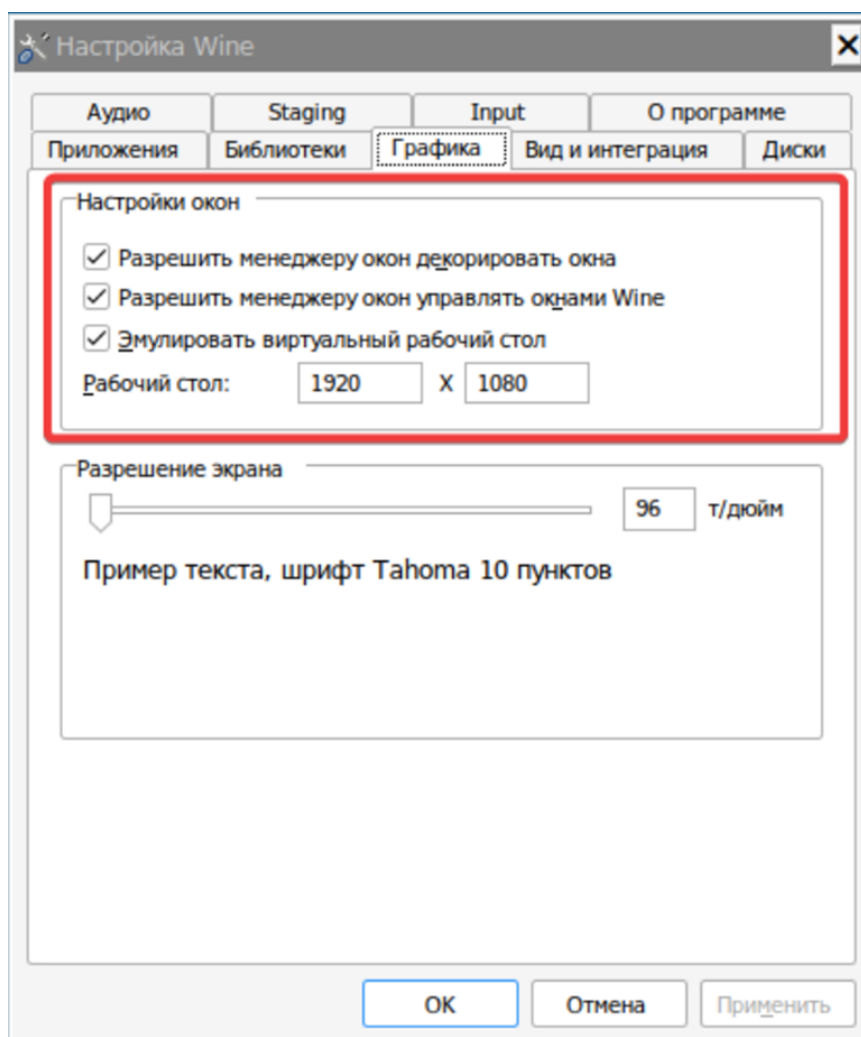


Рисунок 13.29 – Настройка графики

---

### 13.3.1 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 «13.3 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/zvk.
3. В этом же каталоге создать файл-ярлык, который будет размещаться на рабочих столах пользователей:

`nano ZVK.desktop`

внести содержимое:

[Desktop Entry]

Name=ZVK

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, 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. Указание не обязательно. URL требуется если на клиенте планируется запуск комплекса 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/zvk* создать скрипт распаковки клиентских файлов:

```
nano extract_ZVK.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 ZVK.desktop на рабочий стол, если файлов-ярлыков было создано
несколько – то скопировать все
```

```
cp ./ZVK.desktop "$DESKTOP/"
```

```
сделать скрипт исполняемым: chmod +x extract_ZVK.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 Системы, для этого из каталога `/opt/makeself-2.5.0/` выполнить команду:

```
./makeself.sh --gzip /home/$USER/zvk/ ZVK_installer.run "ZVK Installer"
./extract_ZVK.sh, где
```

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

Переместить полученный архив `ZVK_installer.run` на рабочие места пользователей вручную или следовать рекомендациям из раздела «13.3.2 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 ZVK_installer.zip`

Запустить архив: `./ZVK_installer.zip`

На рабочем столе пользователя появится ярлык Системы, 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 потребуются установка Wine Mono, на всплывающем окне «Установка Wine Mono» необходимо нажать кнопку «Установить» (Рисунок 13.30).

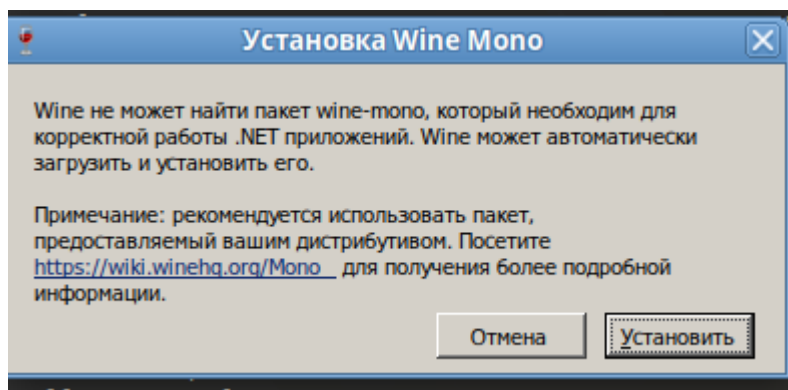


Рисунок 13.30 – Всплывающее окно «Wine Mono»

В дальнейшем, при обновлении версии Системы 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.

**Внимание!** На рабочих местах пользователей с ОС **Alt Linux** после обновления на Wine 10 запуск клиентской части необходимо производить с явным указанием 32-битного Wine, для этого рекомендуем следующее:

1. Создать префикс: `WINEARCH=win32 WINEPREFIX=~/.wine-win32 wineboot`
2. Скопировать файл `zvk.exe` в директорию с новым префиксом `/home/~/.wine-win32/drive_c/ProgramData/ZVK`.
3. В свойствах ярлыка прописать запуск с новым префиксом: `WINEPREFIX=~/.wine-win32 wine C:\\ProgramData\\ZVK\\ZVK.EXE URL=https://zvctest/zvk/appsrv/proxy.dll INTF=RPUser.exe`

При этом может возникнуть проблема с параметром ProxyEnable, потребуется редактирование или создание параметра ProxyEnable (DWORD, значение «0» в шестнадцатеричном счислении) в системном реестре Wine в разделе:

«Компьютер\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings».

Для этого необходимо выполнить команду вызова реестра для 32-битного Wine:

`WINEPREFIX="/home/user/.wine-win32" wine regedit.`

### 13.3.2 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 Системы (по умолчанию C:\Program Files\Zvk\{имя\_экземпляра}) необходимо создать новую папку, например, clientLin, и разместить в неё ранее сформированный самораспаковывающийся архив ZVK\_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 13.31).

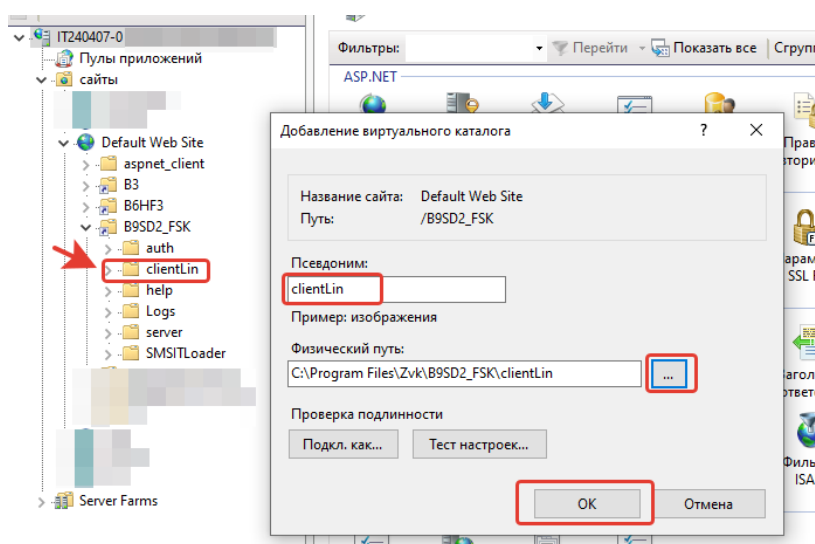


Рисунок 13.31 – Создание виртуального каталога в IIS

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 13.32).

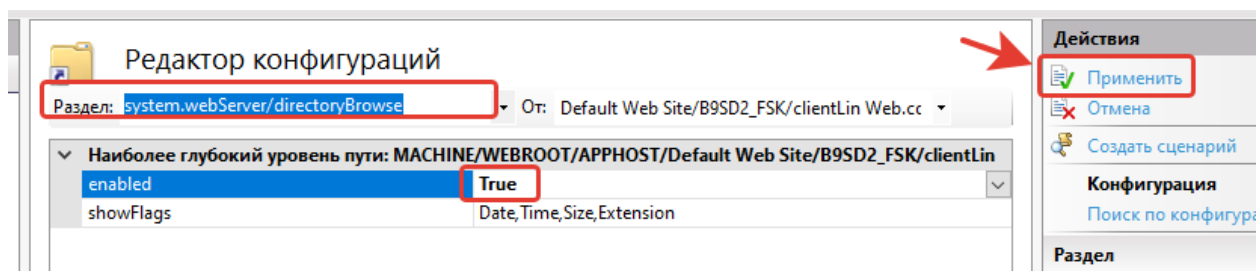


Рисунок 13.32 – Настройка редактора конфигураций IIS

После выполненных вышеуказанных действий самораспаковывающийся архив ZVK\_installer.zip доступен к скачиванию по URL: [http\(s\)://xx.xxx.xx.xxx/<имя экземпляра>/clientLin](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;
- clientLin – имя виртуального каталога, созданный ранее в IIS для размещения самораспаковывающегося архива.

### 13.3.3 Размещение самораспаковывающегося архива на веб-сервере nginx

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 в серверной директории необходимо создать новую директорию, например, с именем ClientLin:

```
mkdir /opt/zvk/ClientLin
```

Разместить в неё ранее сформированный самораспаковывающийся архив ZVK\_installer.zip. Далее необходимо добавить mapping данной директории в контейнер nginx. Для этого добавить в файл docker-compose.yml в секцию volumes для контейнера webserver строчку.

```
./ClientLin:/etc/nginx/www/ClientLin
```

Также необходимо добавить новый location в конфигурационный файл default.conf. Для этого в default.conf для сайта ЗРП.Delphi добавить следующую секцию:

```
location /ClientLin {
 autoindex on;
}
```

После этого необходимо осуществить пересборку контейнеров командами:

```
sudo docker-compose down
```

---

```
sudo docker-compose up -d
```

## 13.4 Настройка использования Proxy с поддержкой сетевого протокола аутентификации Kerberos

Для работы ЗРП.Delphi с Proxy сервером с использованием сетевой аутентификации kerberos необходимо указать настройки Proxy.

Настройки могут быть указаны в нескольких местах, и их приоритет следующий:

1. Клиентский файл zvkc.ini подробнее в разделе «14.3 Описание параметров файла клиентского zvkc.ini».
2. Файл ZvkUser.DAT подробнее в разделе «14.4 Описание параметров клиентского файла ZVKUser.DAT».
3. Системные настройки (реестр Windows).

Порядок подключения с использованием Proxy должен производиться в следующем порядке приоритета:

- если в клиентском файле zvkc.ini не заданы параметры Proxy, то осуществляется проверка параметров клиентского файла ZvkUser.DAT;
- если в ZvkUser.DAT не указаны параметры Proxy, то производится обращение к реестру;
- если в реестре не указаны параметры Proxy, то осуществляется подключение без использования Proxy.

## 13.5 Хранение паролей на клиенте

Хранение паролей осуществляется только если в Интерфейсе администратора в разделе «Системные настройки» установлен флаг «Разрешить хранение пароля для десктопной версии клиента».

На ПК пользователя в папке C:\Users\<Имя пользователя/компьютера>\AppData\Roaming\SMS-IT создается папка ZVK с файлом zvkcuser.DAT при попытке логина пользователем с включенным функционалом.

В данный файл в секцию [Autologin] сохраняются параметры: LGN и PWD (подробнее в разделе «14.4 Описание параметров клиентского файла ZVKUser.DAT»).

Алгоритм авторизации пользователя с использованием сохраненного на клиенте пароля:

- 
1. Если включена доменная авторизация, то осуществляется попытка выполнить доменную авторизацию. Если доменная авторизация не удалась, то осуществляется переход к форме ввода логина и пароля.
  2. При успешном входе через форму авторизации в Систему осуществляется сохранение LGN и PWD в файл zvkuser.DAT в описанном формате.
  3. При последующей авторизации Система автоматически берет LGN и расшифровывает PWD из файла и выполняет вход.
  4. Если LGN и PWD не верные, производится отказ в авторизации. Ошибка не отображается. Пользователь перенаправляется на страницу ввода логина и пароля.

Примечание. При смене пароля/логина пользователь пытается авторизоваться. Авторизация не производится, пользователь автоматически перенаправляется на форму ввода логина и пароля и при успешной авторизации в файл сохраняются актуальные зашифрованные данные.

---

## 14 Набор файлов установленного экземпляра

### 14.1 Описание параметров файла web.config для IIS

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).

В конфигурационном файле IIS необходимо добавить правило для модуля Rewrite:

```
<add input="{HTTP_USER_AGENT}" pattern="RemObjects ZVKHTTP" ignoreCase="true" />
```

#### 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 zvkc.ini также следует изменить и конфигурационный файл web.config. В примере полужирным шрифтом выделены строки, которые необходимо изменить.

### 14.2 Описание параметров файла zvkc.ini

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

Файл конфигурации zvkc.ini Системы на ОС семейства Linux монтируется с хоста сервера в docker контейнер. Файл располагается по адресу /opt/zvk/zvkc.ini. При первой установке необходимо использовать файл zvkc.ini из комплекта поставки, заполнив обязательные параметры, для работы на рабочем сервере. Далее следуют примеры и расшифровка значений.

## **Пример:**

### **[Service]**

SessionTimeout=5  
Name=TEST  
DisplayName=TEST  
HTTPPort=8621  
TCPPort=8822  
ContractorLogic=1  
NativeHTTPPort=9877  
ServerThreadCount=150  
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=900  
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 (мс)  
Duration=500  
; пауза перед первым запуском (мс)  
StartPause=10000  
; необязательное значение таймаута (мс) 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 3:00
RPLimitDay=30
ArchiveZVKTask=86400,01:30

[Key]
Number=27157AA6
Instance=asu

[Transport]
SendTimeout=180
ReceiveTimeout=180

[EmergencySystemIntegration]
Url=http://localhost:5005/

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

[AdditionalFunctions]
UseInsideReglament=1
CalculateChangeInitiator=1
ConsiderChilds=1
IsRepairDiffActive=1
ShowAllManagementDevices=1
FixedPowerObjectList=1
IsAdjustmentDateEditable=1
DeviceDescrDefaultPO=1
EnableEmergencySystemIntegration=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
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 количество кодовых потоков, обслуживающих клиентские запросы), по умолчанию 20, в высоконагруженной среде с большим количеством одновременно активных пользователей увеличение этого значения способствует ускорению реакции сервера на одновременные клиентские запросы, максимально-возможный размер ограничен ресурсами, для комфортного параллельного обслуживания до 50 активных пользователей рекомендуемое значение – 150;
- 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).
- UseTCPKeepAlive – использование режима TCP KeepAlive. Для ускорения обнаружения потери соединений со службами резервирования других экземпляров сервера приложений. Необязательное значение, по умолчанию – использовать;

- TCPKeepAliveProbeTime – выдержка времени (мс) перед первой пробой канала в режиме TCP KeepAlive. Необязательное значение, по умолчанию – 5000 мс;
- TCPKeepAliveProbeInterval – интервал (мс) перед между пробами канала в режиме TCP KeepAlive. NOTE: Начиная с Vista максимальное количество проб постоянно (10). Необязательное значение, по умолчанию – 1000 мс.

**Пример:**

**[Service]**

```
SessionTimeout=5
Name=TEST
DisplayName=TEST
HTTPPort=8621
TCPPort=8822
ContractorLogic=1
NativeHTTPPort=9877
ServerThreadCount=150
SessionManager=DB
IsTestInstance=1
AdditionalTitle=(ПОЛИГОН)
UseTCPKeepAlive=1
TCPKeepAliveProbeTime=5000
TCPKeepAliveProbeInterval=1000
```

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

- Driver – используемый драйвер БД;
- HostName – сервер БД;
- Database – название БД;
- User\_Name – имя пользователя БД;
- Password – пароль пользователя БД. После установки/изменении пароля и при последующем запуске сервера приложений производится шифрование пароля заменяя каждый символ пароля знаком «\*». Пароль в зашифрованном виде сохраняется в поле «Password=» взамен ранее заданного пользователем;
- RowsetSize – количество 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=vm-it-zvk-vnedr.mail.sms-samara.ru
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 количество подготовленных к использованию соединений, добавляемых в пул сразу при его создании, по умолчанию 3;
- DBPoolMaxReserved – максимальное количество 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=450
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 Системе;
- LogRequests.FileName – имя файла лога, в который будут записываться тела запросов/ответов к Системе;
- 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).

**Пример:**

```
; Допустимы следующие уровни
; debug, info, warn, error, fatal
Level=debug
LogsFolder=D:\zv\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 секцию **[Logger]** реализована возможность задавать дополнительные параметры, которые необходимо расширенно логировать. Параметры в логе задаются по следующим правилам:

- если дополнительный параметр в логе не указан, то данные по нему не логируются;
- если задана строка «Feature» / «Feature.FileName» / «Feature.Level», то считается, что дополнительный параметр включен;
- если для дополнительного параметра указан уровень, то используется настройка уровня для дополнительного параметра;
- если для дополнительного параметра не указан уровень, но дополнительный параметр включен, то берется базовый уровень;
- если для дополнительного параметра указан путь лога, то данные по нему записываются в лог в соответствии с настройкой для дополнительного параметра;
- если для дополнительного параметра не указан путь лога, но дополнительный параметр включен, то данные по нему записываются в соответствии с настройкой для параметра «Level».

**Внимание!** Все изменения, произведенные в секции [Logger], применяются без перезапуска сервера приложений.

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 (мс)
Duration=500
; пауза перед первым запуском (мс)
StartPause=10000
; необязательное значение таймаута (мс) 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 – 1 интервал времени между выполнением задачи отправки сообщений в секундах; 2 время первого запуска задачи в формате hh:mm;
- InTransportTask – 1 интервал времени между выполнением задачи приема сообщений; 2 время первого запуска задачи в формате hh:mm;
- CheckAckTimeoutTask – 1 интервал времени между выполнением задача проверки квитанций; 2 время первого запуска задачи в формате hh:mm;
- ClearDataTask – 1 интервал времени между выполнением задачи очистки и архивации данных; 2 время первого запуска задачи в формате hh:mm;
- RPTask – параметр, предназначенный для очистки уведомлений пользователя по сроку давности с указанным интервалом (86400 сек = 1 сутки) и временем запуска (3:00);
- 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=86400,3:00
RPLimitDay=180
ArchiveZVKTask=86400,01:30
```

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

- 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
Instance=asu
```

Секция [EmergencySystemIntegration] предназначена для включения интеграции с системой ПК «Аварийность». Секция и параметр добавляются в файл zvk.ini вручную. По умолчанию секция не добавлена. При добавлении параметра в интерфейсе пользователя на ФОЗ отображается кнопка «ПК «Аварийность»».

#### Пример:

```
[EmergencySystemIntegration]
Url=http://localhost:5005/
```

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://&lt;client_name>:&lt;clientPort>/?command=goto&point_id=&lt;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] добавляется вручную в файл zvk.ini. В секции [AdditionalFunctions] указываются следующие параметры:

- SubscriberEnterprise – включение функционала предприятий-абонентов (в справочник «Предприятия» добавится столбец «Абонент», в справочник «Службы и пользователи» добавится настройка для службы «Ограничение по предприятию», в справочник «Маршруты графиков ремонтов» на панель инструментов добавится поле с раскрывающимся списком «Предприятие»). Параметр добавляется вручную. Если параметр отсутствует в секции [AdditionalFunctions], то настройки функционала

- 
- предприятий-абонентов будут скрыты. При отключении параметра все настройки предприятий-абонентов удаляются. По умолчанию параметр отсутствует.
- 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 задается. По умолчанию параметр отсутствует;
  - EnableEmergencySystemIntegration – включение функционала интеграции с ПК «Аварийность». Параметр добавляется вручную. По умолчанию параметр отсутствует. Если значение параметра равно 1, то осуществляется отправка информации по закрытым заявкам в ПК «Аварийность»;
  - 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, rptМО. 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 или поле состояние оборудования, в результате которого формируется сообщение типа «Информация об открытии/закрытии заявки» с любого предприятия независимо от его расположения и цели на маршруте (с уровня уведомления тоже формируется оповещение) и отправляется по маршруту при открытии/закрытии заявки и при изменении значения в поле состояние оборудования. 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 Системы 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 Системы»;
  - **AutoTransferNCIDevCurrentEnt** – функционал автоматической передачи НСИ (**AutoTransferNCI**) в части передачи изменений по оборудованию.

- 
- Если значение параметра равно 1, то при наличии изменений в справочнике «Оборудование» в файле передаются изменения по тому оборудованию, которое находится под предприятиями из настройки «Передавать изменения по оборудованию выбранных предприятий:» на форме «Обмен изменениями в справочниках».
  - Если параметр отсутствует или значение равно 0, то изменения по оборудованию передаются согласно требованиям, описанным для функционала AutoTransferNCI (т.е. в файле передаются изменения по оборудованию, которое находится в заявочном управлении/ведении предприятия, указанного в поле «Передавать изменения на предприятия»).
  - Параметр добавляется вручную.
  - По умолчанию параметр отсутствует.
  - Функционал недоступен, если параметр AutoTransferNCI отключен. При включении данного функционала к системе необходимо подключить модуль SMSNotifier.
- 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 (ремонт на несовместимое оборудование) добавляется параметр ResponsibleUser;
  - ScheduleAgreeComparison – включение функционала по сопоставлению диспетчерских заявок с целью «Для согласования», «Поданная на своем предприятии», и «Для утверждения» с плановыми заявками из месячных графиков с целью «Утверждение», «Согласование» и «Предварительное 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»;
  - 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;

- SendScheduleForApproveInfo – включение функционала уведомления предприятий о ходе утверждения графика. Если значение параметра равно 1, то:
  - в сторону уведомляемого предприятия автоматически формируются и отправляются ГДИ с информацией о ходе утверждения графика.
  - во входящих ГДИ отображаются данные о состоянии графика у отправителя.

Если параметр отсутствует или значение равно 0, то уведомление предприятий о ходе утверждения графика не выполняется. По умолчанию параметр отсутствует.

**Пример:**

**[AdditionalFunctions]**

UseInsideReglament=1  
CalculateChangeInitiator=1  
ConsiderChilds=1  
IsRepairDiffActive=1  
ShowAllManagementDevices=1  
FixedPowerObjectList=1  
IsAdjustmentDateEditable=1  
DeviceDescrDefaultPO=1  
AutoNotification=Пуск и др.  
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  
FinesForecast=1  
CheckForDuplicateInstance=1

NumberApplicationNotice=ОДУ Центр

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:**

**[Transport]**

SendTimeout=180

ReceiveTimeout=180

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

- ChannelType – определяет, через какой канал будет выполняться внешняя коммуникация (etcd или База данных). Не обязательный параметр.

Возможные значения:

- database
- etcd

- PingIntervalSec – интервал в секундах пинга каналов выше приоритетом, чем текущий. Значение по умолчанию: 60.
- UseResendExpired – флаг повторной отправки сообщений, для которых не было получено квитанции.
- ResendExpiredIntervalSec – интервал в секундах для переотправки неотправленных ранее сообщений. Значение по умолчанию: 60.
- Host – адрес сервера ETCD. Не обязательный, если канал etcd отключен.
- Port – порт сервера ETCD. Не обязательный, если канал etcd отключен.
- GroupID – название группы серверов, которое будет добавляться в качестве префикса к ключам ETCD, если на один сервер ETCD настроено несколько экземпляров ПК Заявки. Для каждого экземпляра должно быть уникальным.
- Username – не обязательный параметр. Учетные данные для аутентификации на etcd-сервере, если он настроен с включенной аутентификацией.
- Password – не обязательный параметр. Учетные данные для аутентификации на etcd-сервере, если он настроен с включенной аутентификацией.
- ConnectTimeout – максимальное время (в секундах), в течение которого сервер приложений будет ожидать установления соединения с etcd. По умолчанию 10 секунд.
- ReadTimeout – Максимальное время (в секундах), в течение которого сервер приложений будет ожидать ответа от etcd после отправки запроса, при установленном соединении. По умолчанию 10 секунд.
- MessageEncryption – по умолчанию 0. Если 1, то отправляемые сообщения шифруются тем же алгоритмом, что и пароль к БД.

- PublisherGuid – опциональный параметр (любая строка). Можно задать постоянный гуид клиента-публикатора сообщений. Если параметр не задан, при старте СП будет генерироваться новый гуид.

#### **Пример:**

##### **[MessageServerConnection]**

```
ChannelType=etcd
Host=localhost
Port=2379
GroupID=[идентификатор группы]
ConnectTimeout=10
ReadTimeout=10
MessageEncryption=0
PingIntervalSec=60
UseResendExpired=0
ResendExpiredIntervalSec=60
```

### **14.3 Описание параметров файла клиентского zvk.ini**

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

- URL – URL Сервера;
- UseProxy – параметр указания использования Proxy сервера. В параметре доступно указание следующих значений:
  - UseProxy=1, то необходимо использовать параметр Proxy. Если значения в данном поле не заполнено ни в клиентском zvk.ini, ни в Zvkuser.DAT (например так: "Proxy="), то по приоритетам источников настроек будут взяты из реестра Windows;
  - UseProxy=0 – если в параметр = 0, то Proxy сервер не используется, осуществляется попытка подключения напрямую по координатам, указанным в параметре URL;
  - UseProxy отсутствует в клиентском zvk.ini - если параметр отсутствует в конфигурационном файле zvk.ini, то считаем, что он задан UseProxy=1.

### **14.4 Описание параметров клиентского файла ZVKUser.DAT**

После успешного завершения процесса установки в папке C:\Users\<Имя пользователя\компьютера>\AppData\Roaming\SMS-IT\ZVK будет создан файл ZVKUser.DAT.

По умолчанию в файл добавлена секция [Proxy].

В данном файле сразу при создании в секции [Proxy] по умолчанию прописаны незаполненными параметры:

Proxy=

---

UserName=

Password=

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

- Proxy – в параметре указываются координаты Proxy сервера в следующем формате `proto://UserName:Password@localhost:Port?AuthType=Basic`. В параметре можно указать отдельный прокси сервер на каждый протокол, в таком случае значения прописываются через «;». Указание параметра не обязательно;
  - `proto:` – протокол, который используется для соединения с прокси-сервером, возможные значения: `http,https`. Не обязательный, можно указать без данного параметра, тогда строка начинается с `//`;
  - `UserName` – имя пользователя для авторизации на Proxy сервере. Необязательный;
  - `localhost` – адрес прокси-сервера;
  - `Password` – пароль пользователя для авторизации на Proxy сервере. Необязательный;
  - `Port` – порт, на котором работает прокси-сервер (например, 8080 или 3128). Этот порт должен соответствовать настройкам прокси-сервера. Не обязательный параметр, в контексте HTTP по умолчанию будет использован порт 80, в контексте HTTPS - 443;
  - `AuthType=Basic` – тип аутентификации, используемый для подключения к прокси-серверу. В данном случае это базовая аутентификация (Basic), которая передает имя пользователя и пароль в закодированном виде (Base64). Необязательный параметр, при указании учетной записи по умолчанию будет использована Basic-авторизация. Необязательный. Если тип авторизации не указан будет определяться автоматически.
- `UserName` – имя пользователя для авторизации на proxy;
- `Password` – пароль для авторизации на proxy. Пароль шифруется. Изначально пароль в файле указывается в незашифрованном виде, после попытки авторизации пароль зачитывается и зашифровывается с помощью специального внутреннего ключа, который хранится в Системе. В дальнейшем пароль хранится в файле в зашифрованном виде.

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

- `LGN` – логин пользователя;

- PWD – пароль пользователя в зашифрованном виде. PWD шифруется с помощью специального внутреннего ключа, который жестко встроен в Систему.

**Пример:**

**[Proxy]**

Proxy=//user:pass@proxy.example.com:8080?AuthType=Basic

UserName=IvanovAA

Password=626590112DCB67

**[AUTOLOGIN]**

LGN=sms

PWD=626590112DCB67

## 14.5 Описание параметров файла sms.ZRP.WebApi.settings.json

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 «14.5 Описание параметров файла sms.ZRP.WebApi.settings.json»);
- файл с параметрами Identity сервера IdentityServer\AuthServer.settings.json (раздел «14.6 Описание параметров файла authServer.settings.json сервера авторизации»);
- файл с параметрами сервера авторизации ZRP.NET\wwwroot\Content\assets\config\config.json (раздел «14.7 Описание параметров файла config.json сервера авторизации»).

### 14.5.1 Настройки 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 PostgreSQL; 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.
- **Server** – строка подключения:
  - **Port** – порт для соединения СУБД;
  - **Database** – название БД;
  - **User Id** – имя пользователя БД;
  - **Password** – пароль пользователя БД.

```
"Server=server_name;Port=5432;Database=db_name;User
Id=user_name;Password=!encrypted!RxY6nlrdXf0SBr5szKHhWA==!encrypted!;"
```

### 14.5.2 Настройки логирования запросов к базе данных

```
"DbLoggerSettings": {
 "Enable": true,
 "IsLogQueriesActive": false,
 "IsLogDbContextActive": false
},
```

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

### 14.5.3 Настройки для подключения

- **InstanceName** – наименование 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 BadRequest;
  - **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.

#### 14.5.4 Настройка 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** – NativeHttpPort (смотреть zvk.ini) сервера Delphi.

```
"IntegrationServiceSettings": {
 "UseIntegrationService": true,

 "IntegrationServiceUri": "localhost:8620/SOAP">
}
```

---

### 14.5.5 Настройки подключения к etcd серверу

**Примечание.** Канал etcd не используется и не требует подключения, коммуникации между серверами приложений происходят только по каналу БД.

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>"
}
```

### 14.5.6 Настройки 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 «14.5.5 Настройки подключения к etcd серверу»).

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

### 14.5.7 Настройки коммуникации с внешними сервисами

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

- **Enable** – включить или выключить коммуникацию с внешними сервисами;
- **Channel** – канал коммуникации. Возможные значения: **etcd** и **database**. Возможно указание только одного канала коммуникации.
  - Если выбран тип etcd, то необходимо настроить секцию EtcdSettings (см. раздел «14.5.5 Настройки подключения к etcd серверу»).
- **AllowResend** – включить или выключить повторную отправку сообщений по каналу внешней коммуникации.
- **MessageAgeForResendInSeconds** – Возраст сообщения для переотправки в секундах. Значение по умолчанию: 60.

```
"ExternalCommunicationSettings": {
 "Enable": false,
 "Channels": "etcd",
 "AllowResend": false,
 "MessageAgeForResendInSeconds": 60
}
```

### 14.5.8 Настройка 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": "*"
```

```
}
```

### 14.5.9 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"
}
```

### 14.5.10 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 * * * *"
}
```

### 14.5.11 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, так как может быть уже произведена выгрузка информации по вкладке браузером. Если в параметре указано значение 0, то функционал отключен.
- **ChangePassword** – функционал по изменению пароля для входа в систему через Интерфейс пользователя. Если значение параметра true, то кнопка [Сменить пароль] отображается в информации о пользователе, позволяющая сменить пароль у текущего пользователя и отображается форма «Смена пароля» после страницы авторизации, если истек срок действия пароля, заданный на вкладке «Общие» в разделе «Системные настройки» (подробнее см. документ «Руководство по работе с приложением «Интерфейс администратора»» раздел «Системные настройки»). Если параметр отсутствует, то функционал скрывается и игнорируется. Дополнительно параметр должен быть добавлен в FeatureManagerSettings в конфигурационный файл AuthServer.settings.json. Если параметр еще не добавлен, то параметр добавляется автоматически со значением по умолчанию для asu по нажатию кнопки «Сохранить» в конфигураторе на вкладке «Сервер приложений». Если параметр уже добавлен, то перезапись данного значения не осуществляется.

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

---

#### 14.5.12 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.

#### 14.5.13 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. Дополнительно параметр должен быть добавлен в FeatureManagerSettings в конфигурационный файл AuthServer.settings.json. Если параметр еще не добавлен, то параметр добавляется автоматически со значением по умолчанию для asu по нажатию кнопки «Сохранить» в конфигураторе на вкладке «Сервер приложений». Если параметр уже добавлен, то перезапись данного значения не осуществляется;
  - **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;
  - **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 и 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;
- **DeviceDisconnectionCounter** – включение функционала подсчета отключений оборудования с начала года. По умолчанию: false.

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

#### 14.5.14 Настройки Swagger

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

```
"UseSwagger": true
```

#### 14.5.15 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",
 "KeyFileName": "zvkkey.lic"
}
```

#### 14.5.16 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"
```

#### 14.5.17 Настройка префикса для маршрутизации запросов внутри одного порта

- **BasePath** – общий префикс для всех эндпоинтов API. Для перевода работы Системы на работу через один внешний порт используется дополнительный префикс и location в nginx, через которые будет происходить маршрутизация запросов в веб-сервере. Базовый путь является частью основного пути запроса. На основе базового пути запрос направляется к определенному серверу приложения. Чтобы был корректный редирект запроса к нужному серверу, для веб-заявок указывается свой базовый путь, для идентити свой базовый путь, для конфигуратора - свой, для делфи-заявок - свой. Веб-сервер Nginx по базовому пути понимает, к какому серверу идет обращение, и перенаправляет запрос.

##### Пример:

- Основной путь: `https://localhost/zvkdev/web/zvk/zvk-list`
- Базовый путь: `/zvkddev/web/`

- Можно указать только одно значение.
- Указывается значение в формате: '<базовый путь веб-приложения ПК Заявки>/'.
- Не обязательный параметр. Заполняется только при необходимости.
- Является уникальным. Не должен совпадать с базовым путем Identity, конфигулятора и делфи-заявок!!!

```
{
...
 "BasePath": "/zvkddev/web/",
...
}
```

Если на одном сервере запущено несколько экземпляров приложения с одинаковым origin (протокол, домен, порт), для каждого из них необходимо задать уникальный BasePath.

Совпадение BasePath нарушает корректную работу приложения, в частности работу плагина «Помощник ЗРП.Net».

При указании параметра необходимо убедиться, что значения BasePath всех экземпляров различаются. Простой способ добиться уникальности — добавить символ в начало пути, например:

/zvkddev/identity/

/1zvkddev/identity/

#### 14.5.18 Настройка архивирования файлов логирования

- **ArchiveOldLogsSettings** – секция для настройки архивирования файлов логирования:
- **ArchiveOldLogs** – включение функционала по архивированию файлов логирования.
  - Возможные значения: true/false;
  - По умолчанию значение - true.
- **LogLifeDayCount** – Количество дней по истечению которых будет производиться архивирование файлов логирования. Время архивации логов зависит от ScheduledJobs (ArchiveOldLogs).
  - По умолчанию значение - 3. Все логи старше 3х дней будут архивироваться.

```
"ArchiveOldLogsSettings": {
 "ArchiveOldLogs": true,
```

```
"LogLifeDayCount": 3
},
```

#### 14.5.19 Настройка логирования полных запросов и ответов от клиента к серверу приложений

- **HttpLoggerSettings** – секция для настройки расширенного логирования полных запросов от клиента к серверу приложений и ответов от сервера клиенту. Включение логирования производится на лету (без перезапуска СП). Данное логирование занимает большое количество места на диске. Рекомендуется включать временно по запросу. Dotnet перезаписывает логи, конфиги каждые 4 секунды - значение по умолчанию, изменить нельзя (Внесённые в конфигурационный файл изменения будут автоматически применены в течение ~4 секунд).
- **LogRequestHeaders** – включение логирования заголовков запросов (Сохраняет все HTTP-заголовки, переданные клиентом).
  - Возможные значения: true/false;
  - По умолчанию значение - false.
  - Не обязательный параметр. Заполняется только при необходимости.
- **LogRequestBody** – включение логирования тела запроса (Сохраняет содержимое тела запроса).
  - Возможные значения: true/false;
  - По умолчанию значение - false.
  - Не обязательный параметр. Заполняется только при необходимости.
- **LogResponseHeaders** – включение логирования заголовков ответов сервера (Сохраняет все HTTP-заголовки, возвращаемые сервером).
  - Возможные значения: true/false;
  - По умолчанию значение - false.
  - Не обязательный параметр. Заполняется только при необходимости.
- **LogResponseBody** – включение логирования тела ответа с сервера (Сохраняет содержимое тела ответа).
  - Возможные значения: true/false;

- По умолчанию значение - false.
- Не обязательный параметр. Заполняется только при необходимости.

```
"HttpLoggerSettings": {
 "LogRequestHeaders": false,
 "LogRequestBody": false,
 "LogResponseHeaders": false,
 "LogResponseBody": false
},
```

## 14.6 Описание параметров файла authServer.settings.json сервера авторизации

### 14.6.1 Настройки базы данных и подключения

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

### 14.6.2 Настройки 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 – ОС MS Windows. Для ОС MS 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 ОС MS Windows. Если стоит false, для ОС Windows будет использоваться протокол NTLM, а для ОС семейства 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 (например, cdu);
  - **realm** – полное имя домена (например, cdu.so-ups.ru), включающее в себя доменную зону. Параметр добавляется автоматически по нажатию на кнопку «Сохранить» в конфигураторе. Параметр обязательный для заполнения, важен для работы авторизации. По умолчанию конфигуратором добавляется значение "realm": null. Если оставить `realm = null`, возможны ошибки при логине. Полное имя домена можно заполнить вручную в конфигурационном файле или в конфигураторе;

- **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.
- Для авторизации пользователей из разных доменных зон необходимо в параметре DomainAliasMap для каждой зоны указать свой блок со значениями domain, realm, values.

```
"DomainAliasMap": [
 {
 "domain": "смс",
 "realm": domain.local,
 "values": [
 "mail.sms-samara.ru",
 "sms-a.ru",
 "смс"
]
 },
 {
 "domain": "stand",
 "realm": domain.local,
 "values": [
 "stand.local",
 "stand"
]
 }
]
```

### 14.6.3 Настройки 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»).

#### 14.6.4 Настройки 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.

- 
- **RedirectUri** – 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
    - указываются относительные адреса до точки авторизации. Пример: /zvк/auth-callback
    - если у веб-сервера есть базовый путь (подробнее см. раздел «14.5.17 Настройка префикса для маршрутизации запросов внутри одного порта»), то добавляется дополнительный относительный адрес. В итоге в параметре RedirectUri указываются два адреса. Пример:  
  
/zvкdev/zvк/auth-callback  
  
/zvкdev/web/zvк/auth-callback
  - **PostLogoutRedirectUri** – набор допустимых адресов, которые может прислать клиент как точки возврата пользователя после завершения выхода из приложения;
    - если у веб-сервера есть базовый путь (подробнее см. раздел «14.5.17 Настройка префикса для маршрутизации запросов внутри одного порта»), то он должен указываться в данной настройке. Пример:  
  
/zvкdev/web/  
  
/zvкdev/
  - **AllowedCorsOrigins** – набор origins (схема, имя хоста, порт), откуда может попасть пользователь на сервер авторизации;
    - указывается адрес веб-сервера, с которого обращается клиент при обращении к identity. Если обращение настроено через один внешний порт в nginx, то указывается данный порт.
  - **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": ["/zvk/auth-callback"],
 "PostLogoutRedirectUris": [""],
 "AllowedCorsOrigins": ["http://<адрес сервера>:порт"],
 "AccessTokenLifetime": 3600,
 "AllowedGrantTypes": ["authorization_code"]
 }
]
```

#### 14.6.5 Настройка префикса для маршрутизации запросов внутри одного порта

- **IntegrationServiceSettings** – настройки интеграции с Delphi сервером приложений заявок.
- **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.
- **BasePath** – общий префикс для всех эндпоинтов API (подробнее в разделе «14.5.17 Настройка префикса для маршрутизации запросов внутри одного порта»).

```
"IntegrationServiceSettings": {
 "IntegrationServiceUri": "http://<server>/zvk/appservice/SOAP",
},
"BasePath": "/zvk/identity/"
}
```

### 14.6.6 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. Если параметр еще не добавлен, то параметр добавляется автоматически со значением по умолчанию для asu по нажатию кнопки «Сохранить» в конфигураторе на вкладке «Сервер авторизации». Если параметр уже добавлен, то перезапись данного значения не осуществляется;
  - **ChangePassword** – функционал по изменению пароля для входа в систему через Интерфейс пользователя. Параметр является обязательным, если он указан в конфигурационном файле Sms.ZRP.WebApi.settings.json (см. раздел «14.5.11 Системные настройки»). Если значение параметра true, то кнопка [Сменить пароль] отображается в информации о пользователе, позволяющая сменить пароль у текущего пользователя и отображается форма «Смена пароля» после страницы авторизации, если истек срок действия пароля, заданный на вкладке «Общие» в разделе «Системные настройки» (подробнее см. документ «Руководство по работе с приложением «Интерфейс администратора»» раздел «Системные настройки»). Если параметр отсутствует, то функционал скрывается и игнорируется. Если параметр еще не добавлен, то параметр добавляется автоматически со значением по умолчанию для asu по нажатию кнопки «Сохранить» в конфигураторе на вкладке «Сервер авторизации». Если параметр уже добавлен, то перезапись данного значения не осуществляется.

```
"FeatureManagerSettings": {
 "SubscriberEnterprise": false,
 "ChangePassword": true
}
```

## 14.7 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/zvk/auth-callback",
 "post_logout_redirect_uri": "http://localhost"
 }
}
```

## 14.8 Описание параметров файла Serilogsettings.json

В конфигурационном файле Serilogsettings.json осуществляется настройка логирования для всех файлов логирования кроме Backend-startup-ГТГММЧЧ.log.

Для Backend-startup-ГТГММДД.log настройка осуществляется в файле Serilogsettings.startup.json (файл аналогичен обычному Serilogsettings.json).

В ОС Linux конфигурационный файл Serilogsettings.json лежит внутри контейнера. То есть найти файл в папках не получится, его можно открыть через консоль на просмотр с помощью команды: *docker exec -it zrpnet cat /zrp/app/web/serilogsettings.json*.

- **path** – путь к конкретному файлу логирования, для которого ниже указываются настройки.
- **rollingInterval** – интервал перехода на новый файл. По умолчанию установлено значение Day (каждый день). Возможные значения: Hour / Month / Minute / Infinite (никогда не переходить на новый файл по дате). **Примечание!** Рекомендуемое

---

значение Day, если ставить не Day, то архивация логов может работать некорректно, так как она настраивается по Day.

- **retainedFileCountLimit** – лимит хранимых файлов. По умолчанию установлено значение null, т.е. без ограничения по количеству файлов. Настройка не имеет смысла, если не подключен rollingInterval. Если настройка rollingInterval подключена и rollingInterval указан Day, то при указании, например, значения 20 будет храниться 20 файлов логирования. При создании 21-ого файла, 1-й будет удаляться.
- **fileSizeLimitBytes** – максимальный размер одного файла в байтах. По умолчанию – 104857600 (1024 \* 1024 \* 100) - 100 Мбайт. При разбиении файлов название файла формируется по следующему шаблону: <Наименование файла логирования><Дата в формате ГГГГММДД>\_<номер файла>.log Например: backend-all-ГГГГММДД\_001.log backend-all-ГГГГММДД\_002.log.
- **rollOnFileSizeLimit** – переходить на новый файл при достижении лимита размера. Возможные значения true/false. По умолчанию установлено значение true.
- **formatter** – формат записи события в файле лога;
- **hooks** – вызывается на разные события, например, событие создания нового файла.
- **alwaysWriteHeader** – при создании нового файла всегда писать заголовок (header) во все файлы логирования. Возможные значения true/false. По умолчанию true. Если установлено значение false, то header запишется только в самый первый файл и не будет писаться в остальные файлы за день созданные при разбиении файлов на части.

Данные параметры создают слаженную систему ротации логов:

- по дате: каждый день заводится новый файл логирования;
- по размеру: если за день набирается много записей (больше 100 МБ), главный файл разбивается на несколько томов (\_001, \_002...);
- по хранению количества файлов: по умолчанию установлено значение null, т.е. без ограничения по количеству файлов.

```
{
 "Serilog": {
 "Using": [
 "Serilog.Sinks.Console",
 "Serilog.Sinks.File",
 "Serilog.Expressions",
```

```

 "Serilog.Enrichers.CorrelationId"
],

 "Enrich": [
 "FromLogContext",
 "WithMachineName",
 "WithCorrelationId"
],

 "MinimumLevel": {
 "Default": "Debug",
 "Override": {
 "System": "Error",
 "Microsoft": "Warning",
 "Microsoft.AspNetCore": "Warning"
 }
 },

 "WriteTo": [
 {
 "Name": "Console",
 "Args": {
 "formatter": {
 "type": "Serilog.Templates.ExpressionTemplate, Serilog.Expressions",
 "template": "{@t:HH:mm:ss.fff} [{@l:u3}] {@m}{#if SourceContext is not null} <{SourceContext}>{#end}\n{#if @x is not null}{@x}\n{#end}"
 }
 }
 },

 {
 "Name": "File",
 "Args": {
 "path": "./logs/auth-all-.log",
 "rollingInterval": "Day",
 "retainedFileCountLimit": null,
 "rollOnFileSizeLimit": true,
 "fileSizeLimitBytes": 104857600,
 "buffered": false,
 "shared": false,
 "formatter": {
 "type": "Serilog.Templates.ExpressionTemplate, Serilog.Expressions",

```

```

 "template": "{@t:HH:mm:ss.fff} [{@l:u3}] {@m}{#if CorrelationId is not
null}({CorrelationId}) {#end}{#if SourceContext is not null}<{SourceContext}>
{#end}\n{#if @x is not null}{@x}\n{#end}"
 },
 "hooks": {
 "type": "Sms.ZRP.Modules.Logging.Hooks.LogFileHeaderWriter,
Sms.ZRP.Modules.Logging",
 "alwaysWriteHeader": true
 }
}
},
{
 "Name": "Logger",
 "Args": {
 "configureLogger": {
 "Filter": [
 {
 "Name": "ByIncludingOnly",
 "Args": {
 "expression": "@l = 'Error'"
 }
 }
],
 "WriteTo": [
 {
 "Name": "File",
 "Args": {
 "path": "./logs/auth-error-.log",
 "rollingInterval": "Day",
 "retainedFileCountLimit": null,
 "rollOnFileSizeLimit": true,
 "fileSizeLimitBytes": 104857600,
 "buffered": false,
 "shared": false,
 "formatter": {
 "type": "Serilog.Templates.ExpressionTemplate,
Serilog.Expressions",
 "template": "{@t:HH:mm:ss.fff} [{@l:u3}] {@m}{#if CorrelationId
is not null} ({CorrelationId}){#end}\n{#if @x is not null}{@x}\n{#end}"
 }
 }
 }
],
 "hooks": {
 "type": "Sms.ZRP.Modules.Logging.Hooks.LogFileHeaderWriter,
Sms.ZRP.Modules.Logging",
 "alwaysWriteHeader": true
 }
 }
 }
}
}

```

```

 }
 }
}

]

}

},

{
 "Name": "Logger",
 "Args": {
 "configureLogger": {
 "Filter": [
 {
 "Name": "ByIncludingOnly",
 "Args": {
 "expression": "StartsWith(SourceContext,
'Serilog.AspNetCore.RequestLoggingMiddleware') "
 }
 }
],
 "WriteTo": [
 {
 "Name": "File",
 "Args": {
 "path": "./logs/auth-api-call-.log",
 "rollingInterval": "Day",
 "retainedFileCountLimit": null,
 "rollOnFileSizeLimit": true,
 "fileSizeLimitBytes": 104857600,
 "buffered": false,
 "shared": false,
 "formatter": {
 "type": "Serilog.Templates.ExpressionTemplate,
Serilog.Expressions",
 "template": "{@t:HH:mm:ss.fff} [{@l:u3}] {@m}{#if CorrelationId
is not null} ({CorrelationId}){#end}\n{#if @x is not null}{@x}\n{#end}"
 },
 "hooks": {
 "type": "Sms.ZRP.Modules.Logging.Hooks.LogFileHeaderWriter,
Sms.ZRP.Modules.Logging",
 "alwaysWriteHeader": true
 }
 }
 }
]
 }
 }
}

```

```
]
 }
}
}
```

## 14.9 Описание параметров файла appsettings.json

Для настройки интеграции с ПК «Аварийность» необходимо заполнить конфигурационный файл appsettings.json:

- **секция Logging** – настройка уровней логирования;
  - **LogLevel.Default** – уровень логирования по умолчанию. Логируются события уровня Information, Warning, Error, Critical.
  - **LogLevel.Microsoft.AspNetCore** – уровень логирования для компонентов Microsoft ASP.NET Core. Логируются только предупреждения и ошибки.
- **секция Database** – настройки базы данных;
  - **Provider** – тип системы управления базой данных (СУБД).
    - Возможные значения: SqlServer/PostgreSQL;
    - Значение по умолчанию – SqlServer;
  - **ConnectionStrings**;
    - **PostgreSql** – строка подключения к серверу баз данных PostgreSQL; Пароль в поле шифруется в Production режиме. При зашифрованном состоянии начинается и заканчивается с подстроки.
      - ✓ Содержит хост, порт, имя базы данных, имя пользователя и пароль.
    - **SqlServer** – строка подключения к серверу баз данных Microsoft SQL Server; Пароль в поле шифруется в Production режиме. При зашифрованном состоянии начинается и заканчивается с подстроки.
      - ✓ Содержит сервер, имя базы данных, учётные данные и настройки сертификата.
- **секция EmergencySoap**
  - **Endpoint** – URL-адрес веб-сервиса ПК «Аварийность». Используется для вызова метода Consolidate.
  - **UseAuthentication** – настройка аутентификации;
    - Возможные значения: true/false.
    - По умолчанию true.

- 
- **Username** – имя пользователя для авторизации в веб-сервисе ПК «Аварийность». Применяется только если UseAuthentication = true. Используется шифрование.
    - В зашифрованном состоянии значение параметра начинается с подстроки enc:.
  - **Password** – пароль пользователя для авторизации в веб-сервисе ПК «Аварийность». Применяется только если UseAuthentication = true. Используется шифрование.
    - В зашифрованном состоянии значение параметра начинается с подстроки enc:.
  - **секция EmergencyDispatchSchedule** – настройка периодической задачи по попыткам отправки сообщений в ПК «Аварийность».
    - **FirstRunTime** – время первого запуска периодической задачи. Задача запускается в указанное время.
      - По умолчанию первый запуск отправки в 01:30:00. Выполняется каждый день.
      - Формат ЧЧ:ММ:СС.
    - **IntervalMinutes** – интервал между последовательными запусками периодической задачи в минутах.
      - По умолчанию 30 минут.
    - **RunCount** – максимальное количество запусков задачи за один цикл. После достижения этого количества задача останавливается до следующего дня.
      - По умолчанию 3 попытки.
  - **секция EmergencyCleanup** – настройка периодической задачи по очистке сообщений.
    - **RunTime** – Время запуска задачи очистки базы данных.
      - Формат ЧЧ:ММ:СС.
    - **RetentionDays** – количество дней хранения записей в таблице интеграции. Удаляются записи со статусом «Отправлено» и «Ошибка отправки» старше указанного количества дней. Черновики не удаляются.
      - По умолчанию 60 дней.
  - **секция LogDbRequest** – настройки логирования запросов к базе данных.
    - Возможные значения true/false.
    - По умолчанию false.

- **секция AllowedHosts** – Фильтр допустимых имён хоста, которые может иметь сервер. Если пользователь отправит запрос с именем хоста, отсутствующим в AllowedHosts сервер вернёт ошибку 400 BadRequest;
  - AllowedHosts: "\*" - Сервер может иметь любое имя хоста;
- **секция SoapLoggerSettings** – предназначена для настройки детализации логирования SOAP-запросов и ответов при взаимодействии с веб-сервисом ПК «Аварийность».
  - **LogRequestHeaders** – настройка включения логирования заголовков исходящего SOAP-запроса. При true записываются HTTP-заголовки запроса (Content-Type, SOAPAction, Authorization и др.). Позволяет отслеживать корректность передачи служебной информации: версию SOAP, тип содержимого, действие (SOAPAction), учётные данные авторизации. Полезен для диагностики проблем авторизации и согласования версий.
    - Возможные значения true/false.
  - **LogRequestBody** – настройка включения логирования тела исходящего SOAP-запроса. При true записывается XML-тело запроса (элемент Body конверта SOAP). Является основным инструментом отладки. Позволяет проверить корректность формируемого XML-сообщения, соответствие XSD-схеме, правильность заполнения полей и атрибутов (Vn, PotrNaprVn).
    - Возможные значения true/false.
  - **LogResponseHeaders** – настройка включения логирования заголовков входящего SOAP-ответа. При true записываются HTTP-заголовки ответа сервера. Позволяет отслеживать служебную информацию ответа сервера: статус HTTP, коды ошибок, информацию о сервере.
    - Возможные значения true/false.
  - **LogResponseBody** – настройка включения логирования тела входящего SOAP-ответа. При true записывается XML-тело ответа (результат выполнения метода). Позволяет анализировать ответ ПК «Аварийность» — квитанции об успешной обработке, коды ошибок, предупреждения. Является основным источником информации о причинах отказа в приёме данных.
    - Возможные значения true/false.

```
{
 "Logging": {
 "LogLevel": {
 "Default": "Information",
```

```

 "Microsoft.AspNetCore": "Warning"
 },
 "Database": {
 "Provider": "PostgreSql",
 "ConnectionStrings": {
 "PostgreSql":
"Host=localhost;Port=5432;Database=zvk;Username=postgres;Password=postgres",
 "SqlServer": "Server=localhost;Database=SmsZrpIntegration;User
Id=sa;Password=Your_password123;TrustServerCertificate=True"
 }
 },
 "EmergencySoap": {
 "Endpoint": "https://hq-avar-t02.rs.corp/WSAvarGate/avargate.asmx",
 "UseAuthentication": false,
 "Username": "",
 "Password": ""
 },
 "EmergencyDispatchSchedule": {
 "FirstRunTime": "09:00:00",
 "IntervalMinutes": 5,
 "RunCount": 12
 },
 "EmergencyCleanup": {
 "RunTime": "03:00:00",
 "RetentionDays": 30
 },
 "LogDbRequest": false,
 "AllowedHosts": "*"
},
"SoapLoggerSettings": {
 "LogRequestHeaders": true,
 "LogRequestBody": true,
 "LogResponseHeaders": true,
 "LogResponseBody": true
}.

```

## 14.10 Шифрование пароля в конфигурационных файлах для ЗРП.Net

Для ЗРП.Net реализован провайдер шифрования с симметричным алгоритмом [Aes](#). Он использует две компоненты ключа (сам ключ и вектор), которые зашиты в библиотеке в ресурсах, сконвертированных через Base64 в строки из наборов байт.

---

При шифровании строки, если строка начинается и заканчивается ключевыми словами **!encrypted!**, то он ничего не шифрует, а возвращает ее в том виде, в котором она пришла на вход. В случае, когда строка не обрамлена ключевыми словами **!encrypted!**, происходит шифрование строки.

Расшифровка работает по тому же принципу, если строка начинается и заканчивается ключевыми словами **!encrypted!**, то строка будет расшифрована, иначе ничего не произойдет и вернется исходный экземпляр.

Например,

```
{
6 "ConnectionStrings": {
7 "ZrpSqlServer": "Server=localhost; User Id=sa;
Password=!encrypted!bJkLLJ/RShs/k35HIREycA==!encrypted!;Database=real_cdu;Persist Security
Info=True",
8 "ZrpPostgreSQL": "Server=localhost;port=5434;Database=real_cdu;User
Id=postgres;Password=!encrypted!RxY6nlrdXf0SBr5szKHhwA==!encrypted!;"
9 },
10 }
```

где вхождения строк между подстроками Password= и до; шифруется.

## 14.11 Дополнительные настройки журналирования действий сервера приложений на MS Windows

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.

1. Открыть панель «Свойства» для папки C:\Program Files (x86)\ZVK\<название экземпляра>\Logs.
2. На закладке «Безопасность» нажать на кнопку «Добавить».
3. 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 заиклиивании оборудования: «Ошибка создания справочника оборудования: элемент Id='1111' ссылается сам на себя». Данная ошибка означает, что произошло заиклиивание оборудования самого на себя. Старт сервера приложений не возможен: необходимо найти заиклиенное оборудование и удалить параметр «ParentDevice» (установить значение Null) или обратиться в службу поддержки СМС-ИТ.

---

## 15 Резервное копирование данных ПК на СУБД MS SQL

### 15.1 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 / 2022. 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.

### 15.2 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 15.1).

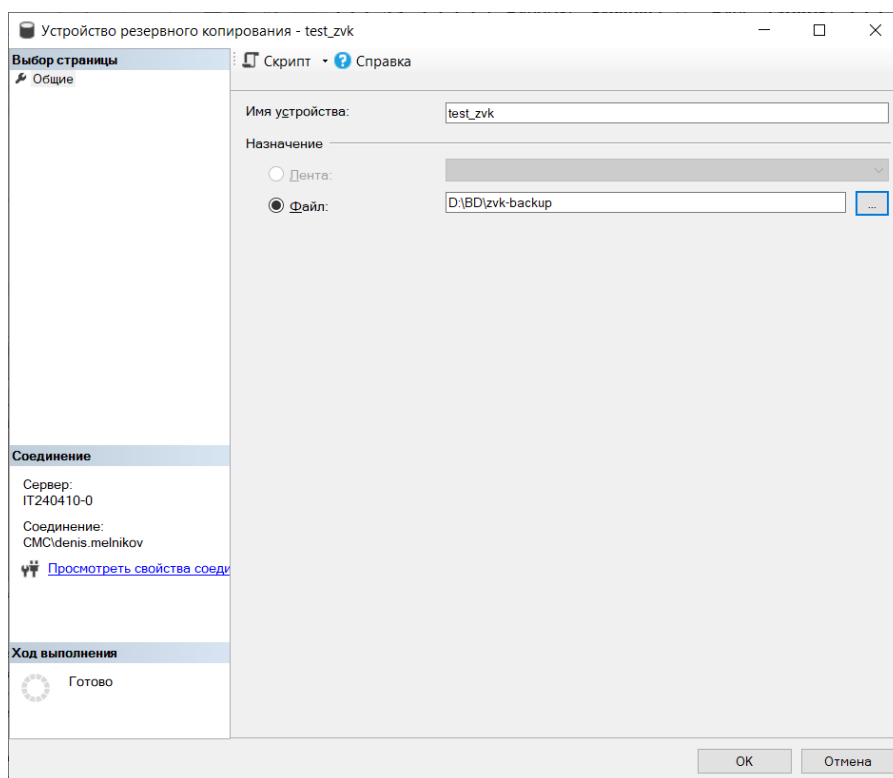


Рисунок 15.1 – Создание устройства для хранения резервной копии

### 15.3 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 «15.4 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. Так как 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.

## **15.4 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 15.2).



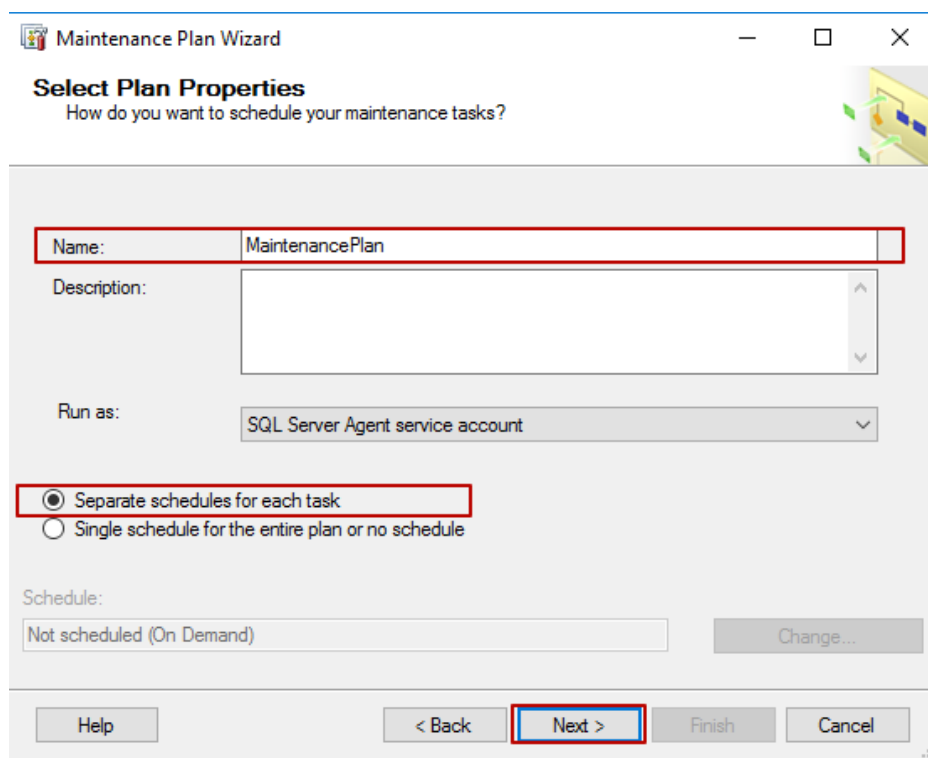


Рисунок 15.3 – Шаг «Select Plan Properties»

- 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 15.4).

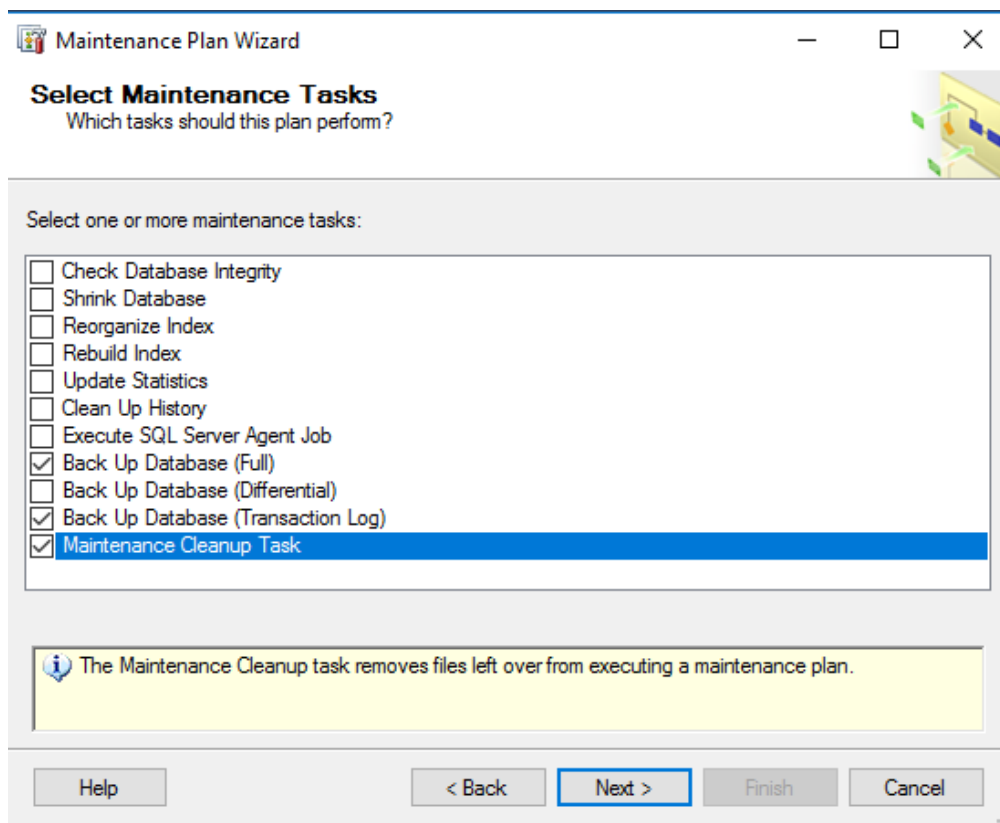


Рисунок 15.4 – Шаг «Select Maintenance Tasks»

- 6) На шаге «*Select Maintenance Task Order*» задать порядок выполнения задач, используя кнопки «*Move Up*», «*Move Down*» и нажать кнопку «*Next*» (Рисунок 15.5).

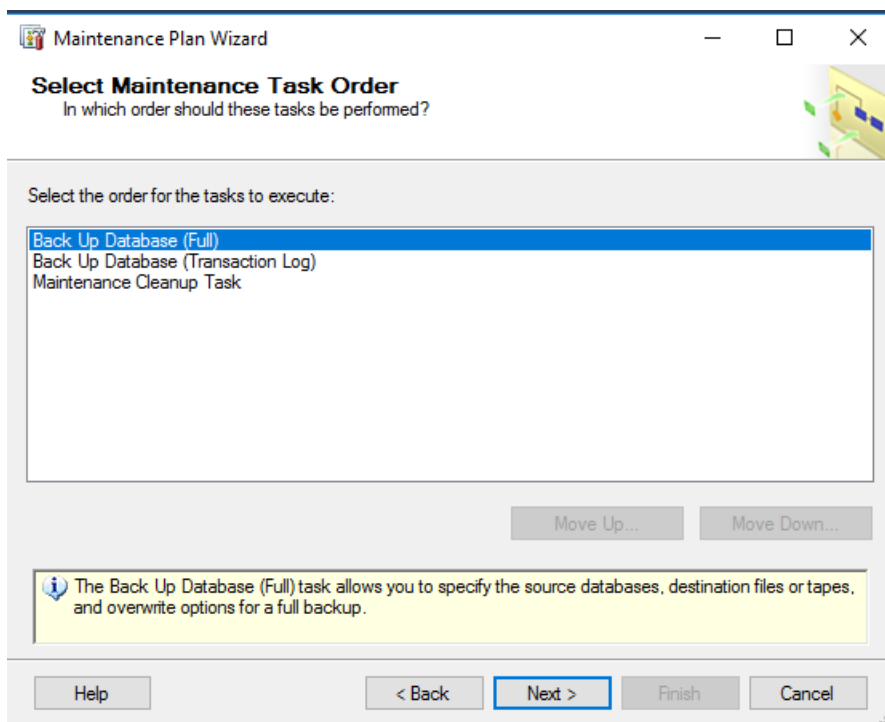


Рисунок 15.5 – Шаг «*Select Maintenance Task Order*»

- 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 15.6).

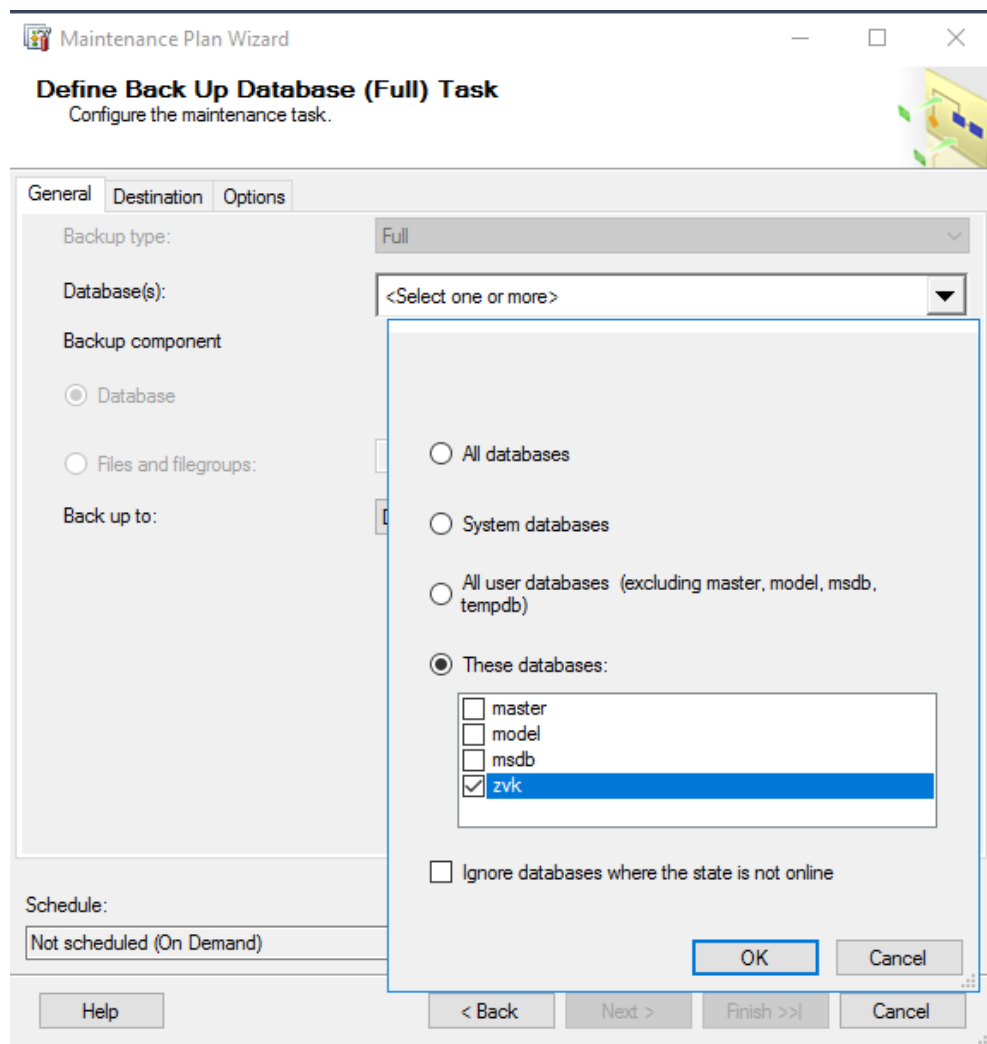


Рисунок 15.6 – Шаг «Define Backup Database (Full) Task» вкладка «General»

8) Задать следующие настройки (Рисунок 15.7):

- Backup component – Database;
- Back up to: Disk.

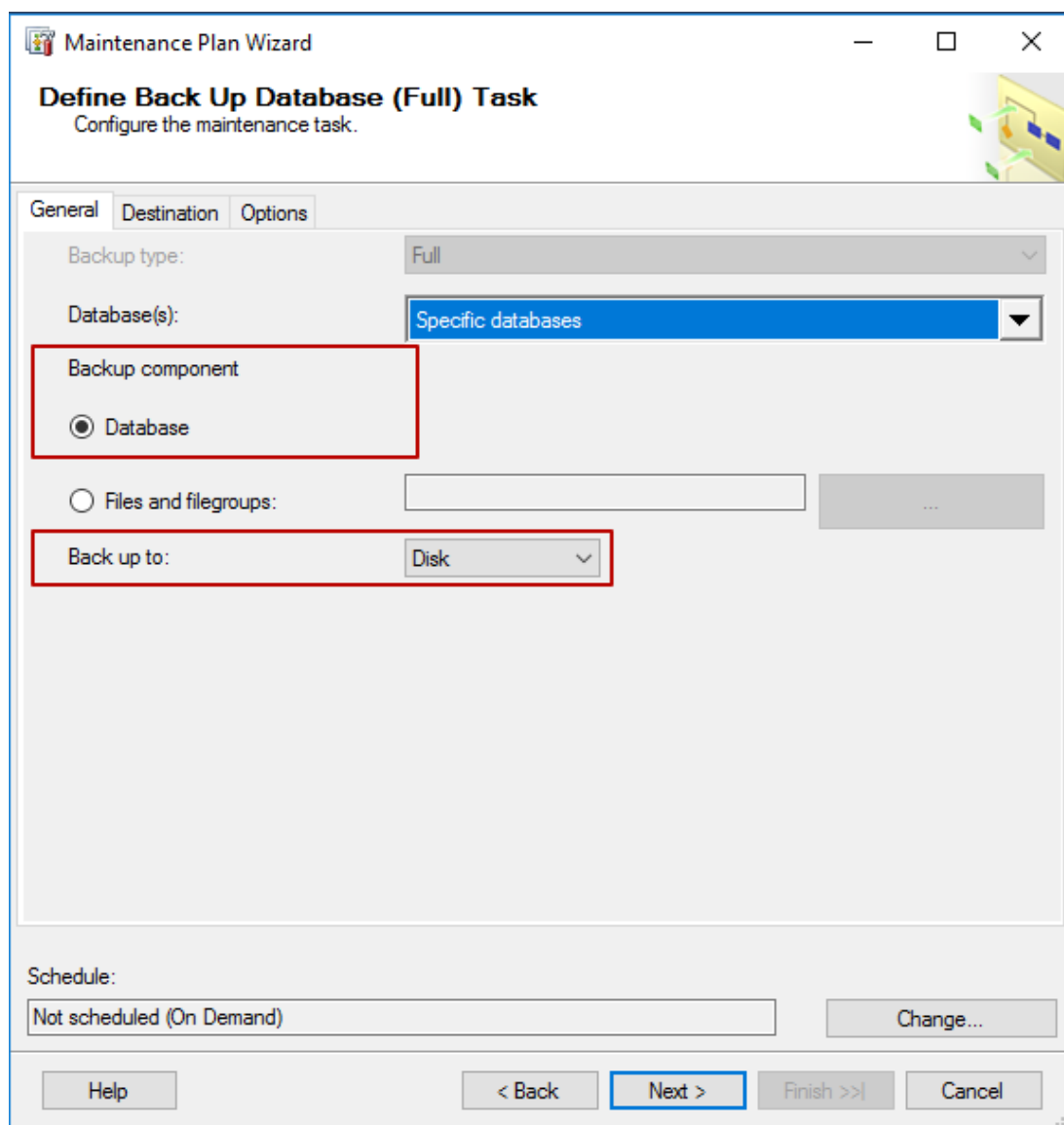


Рисунок 15.7 – Шаг «Define Backup Database (Full) Task» вкладка «General»

- 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 15.8).

Обратите внимание, что необходимо оставить заполненным расширение файла резервной копии.

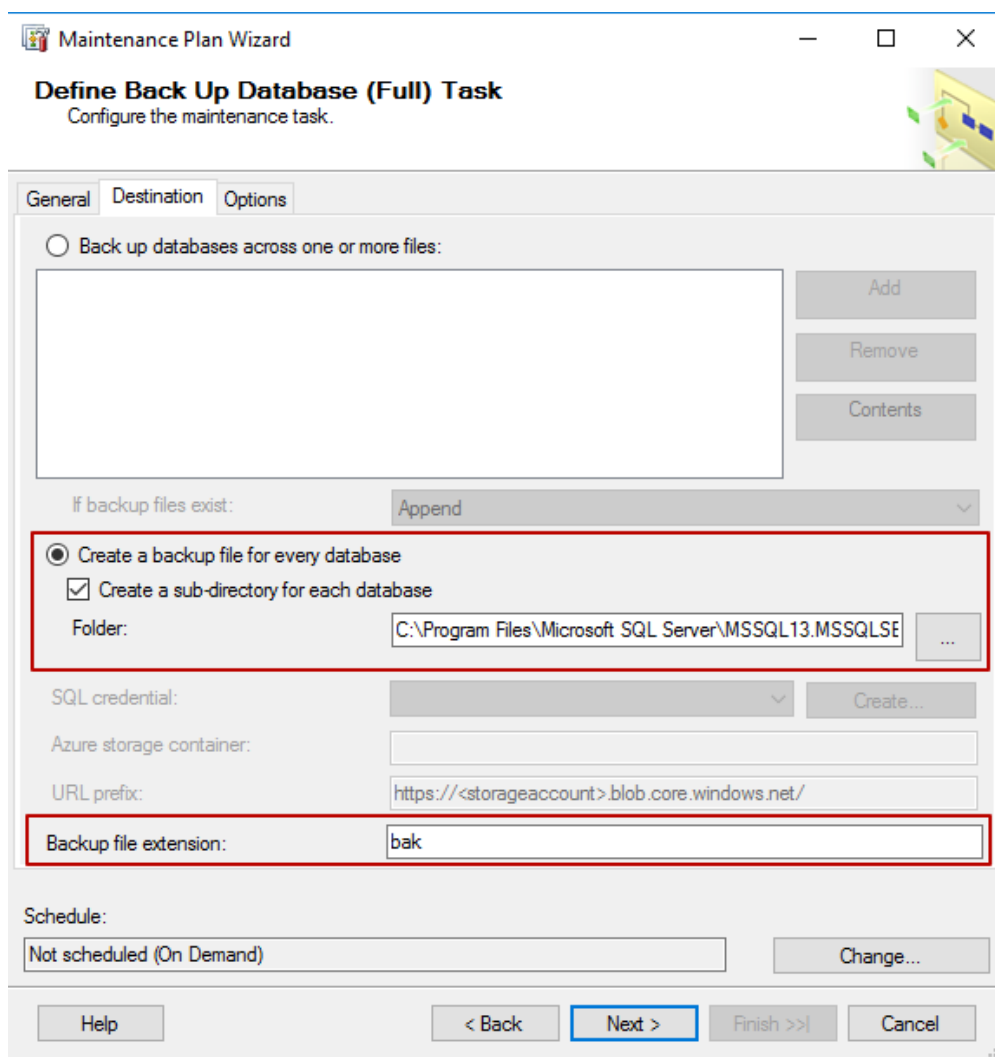


Рисунок 15.8 – Шаг «Define Backup Database (Full) Task» вкладка «Destination»

- 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 15.9). 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*».

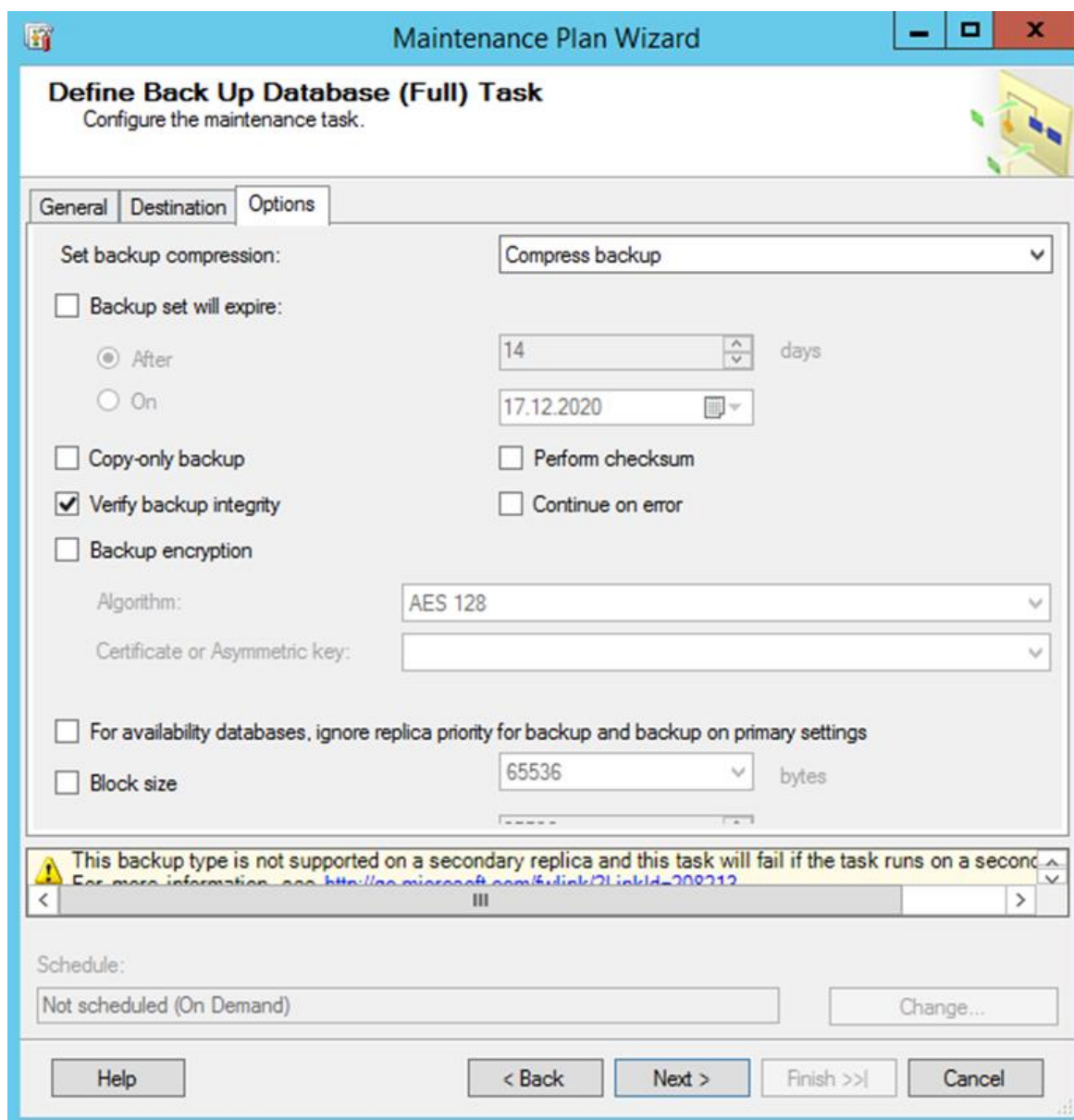


Рисунок 15.9 – Шаг «Define Backup Database (Full) Task» вкладка «Options»

- 11) Перейти на вкладку «General» в области настройки «Schedule» нажать кнопку «Change» (Рисунок 15.10).

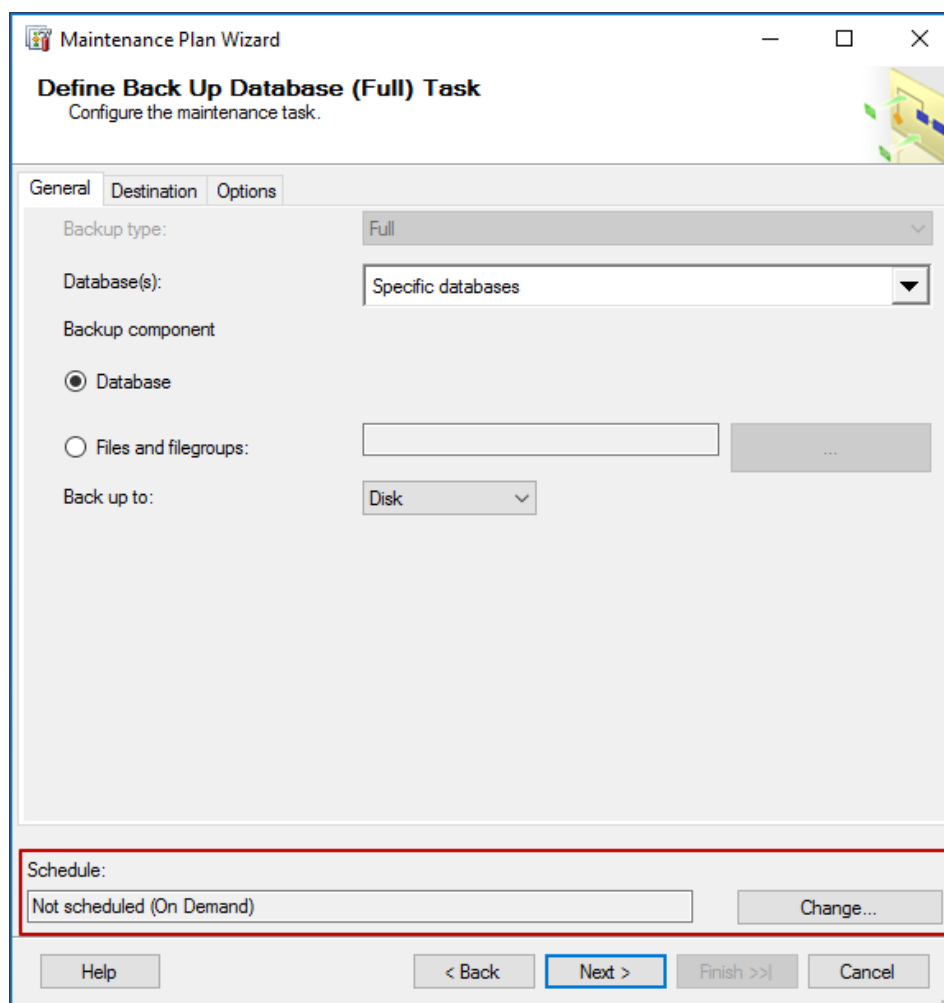


Рисунок 15.10 – Шаг «Define Backup Database (Full) Task» вкладка «General»

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 «*Recuring*» и установить опцию «*Enabled*»;
- в области «*Frequency*» из раскрывающегося списка поля «*Occurs*» выбрать пункт «*Daily*»;
- в поле «*Rekurs 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 15.11).

**New Job Schedule**

Name: MaintenancePlan.Back Up Database (Full) Jobs in Schedule

Schedule type: Recurring ☒ Enabled

One-time occurrence

Date: 9/14/2020 Time: 3:42:47 PM

Frequency

Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

☒ Occurs once at: 12:01:00 AM

☐ Occurs every: 1 hour(s)

Starting at: 12:00:00 AM

Ending at: 11:59:59 PM

Duration

Start date: 9/14/2020 ☐ End date: 9/14/2020 ☒ No end date:

Summary

Description: Occurs every day at 12:01:00 AM. Schedule will be used starting on 9/14/2020.

OK Cancel Help

Рисунок 15.11 – Диалоговое окно «New Job Schedule»

- 13) На шаге «*Define Backup Database (Full) Task*» вкладка «*General*» нажать кнопку «*Next*» (Рисунок 15.12).

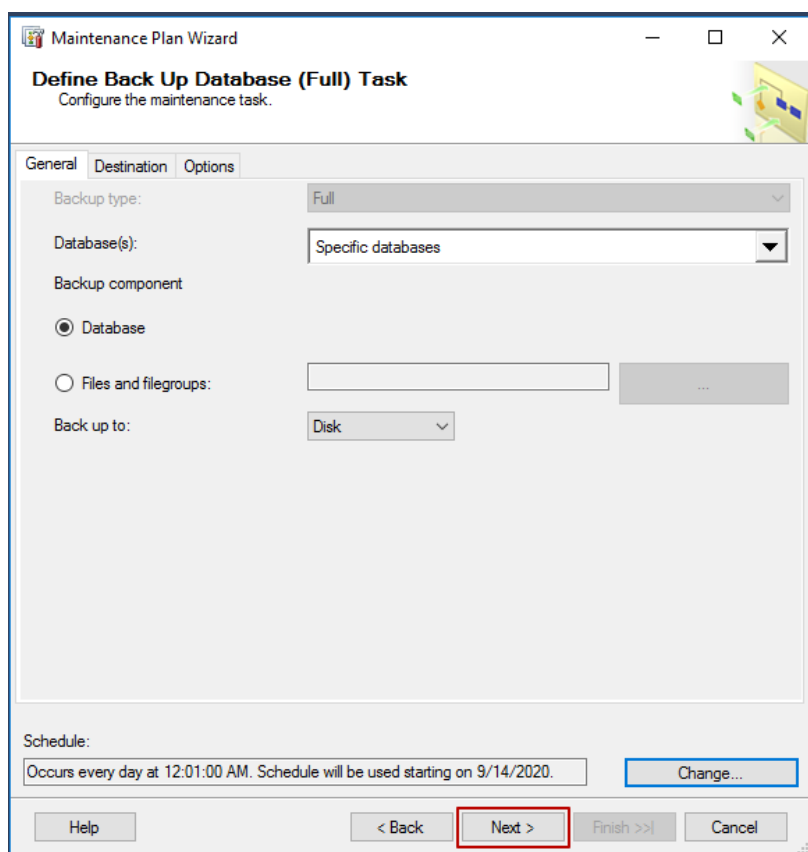


Рисунок 15.12 – Завершение настройки задачи «Define Backup Database (Full) Task»

- 14) Перейти к настройке задачи резервного копирования журнала транзакций. На шаге «*Define Backup Database (Transaction Log) Task*» вкладка «*General*» в раскрывающейся 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 15.13).

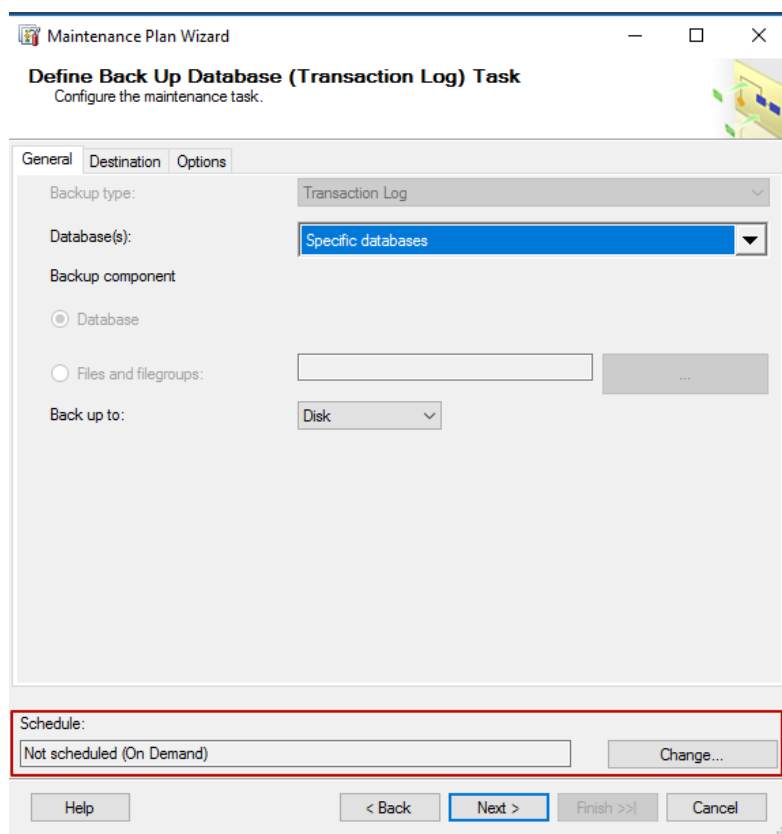


Рисунок 15.13 – Шаг «Define Backup Database (Transaction Log) Task» вкладка «General»

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 «*Recuring*» 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 15.4).

**New Job Schedule**

Name: MaintenancePlan.Back Up Database (Transaction Log) Jobs in Schedule

Schedule type: Recurring ☒ Enabled

One-time occurrence

Date: 9/14/2020 Time: 3:45:57 PM

Frequency

Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

☐ Occurs once at: 12:00:00 AM

☒ Occurs every: 1 hour(s) Starting at: 12:00:00 AM Ending at: 11:59:59 PM

Duration

Start date: 9/14/2020 ☐ End date: 9/14/2020 ☒ No end date

Summary

Description: Occurs every day every 1 hour(s) between 12:00:00 AM and 11:59:59 PM. Schedule will be used starting on 9/14/2020.

OK Cancel Help

Рисунок 15.14 – Диалоговое окно «New Job Schedule»

- 18) На шаге «*Define Backup Database (Transaction Log) Task*» вкладка «*General*» нажать кнопку «*Next*» (Рисунок 15.15).

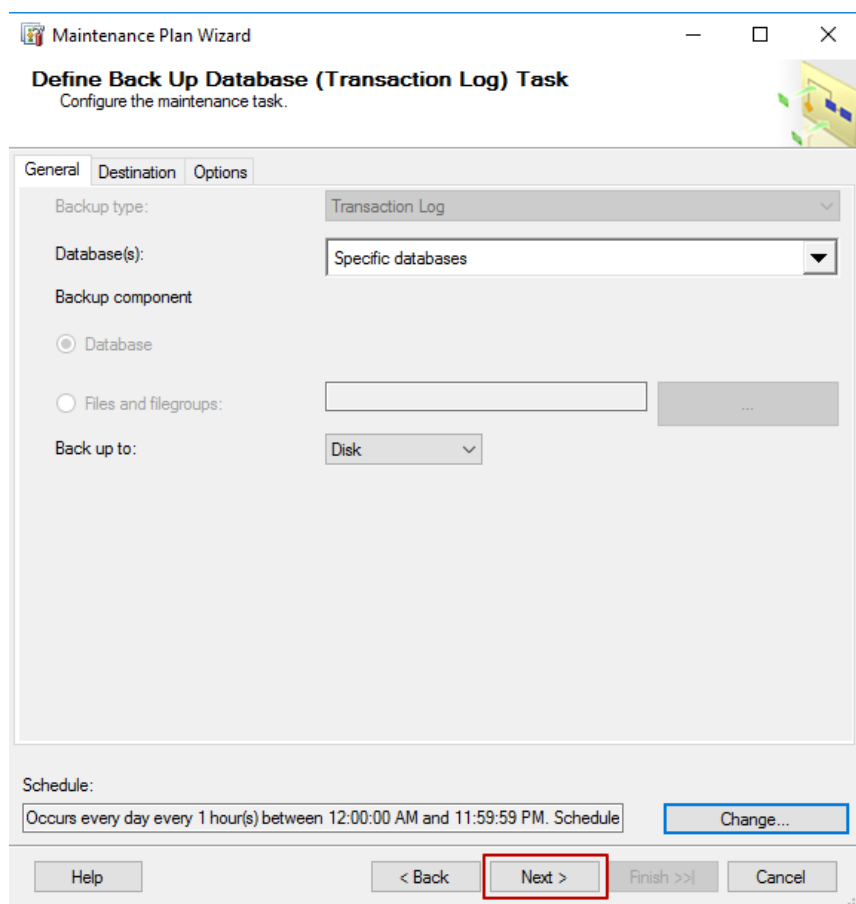


Рисунок 15.15 – Шаг «Define Backup Database (Transaction Log) Task» вкладка «General»

- 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 15.16).

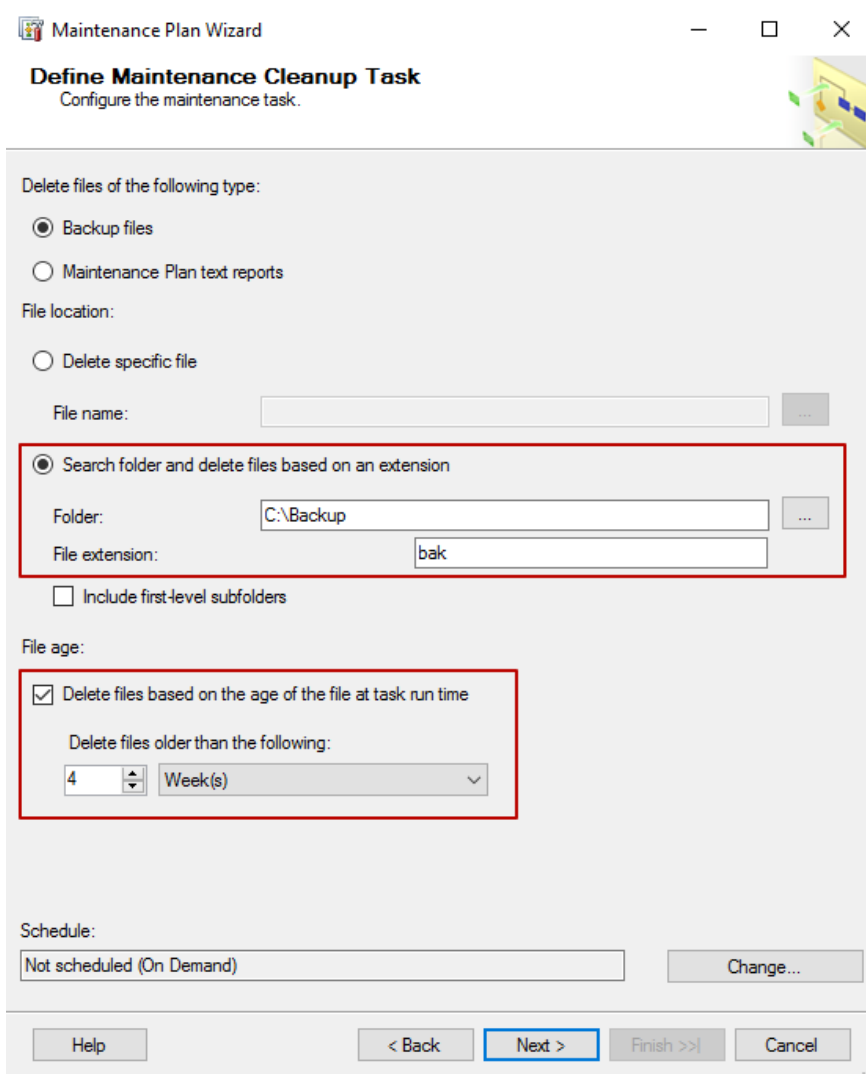


Рисунок 15.16 – Шаг «Define Maintenance Cleanup Task»

- 20) В диалоговом окне «New Job Schedule» необходимо задать расписание выполнения задачи. После настройки расписания необходимо нажать кнопку «OK» (Рисунок 15.17).

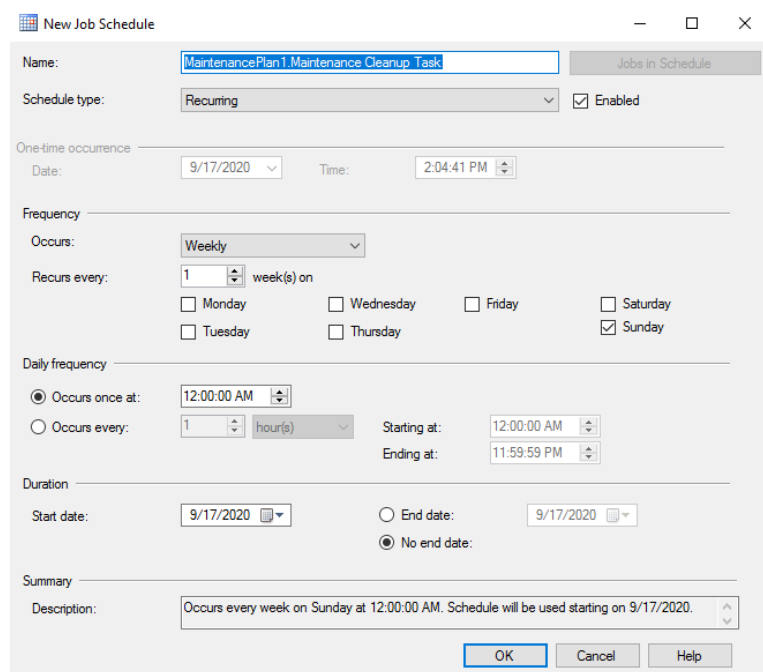


Рисунок 15.17 – Диалоговое окно «New Job Schedule»

21) На шаге «*Define Maintenance Cleanup Task*» нажать кнопку «Next» (Рисунок 15.18).

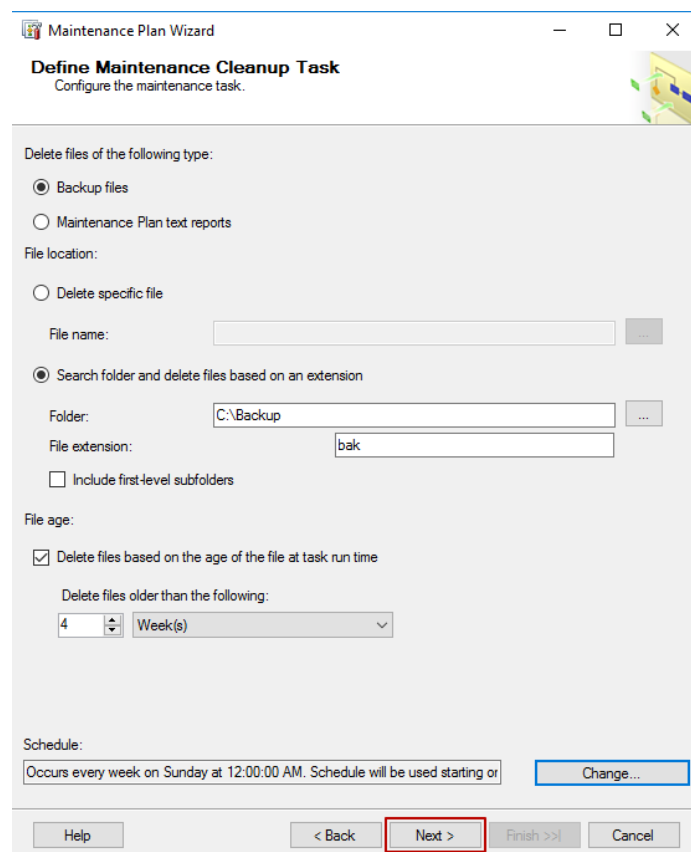


Рисунок 15.18 – Шаг «Define Maintenance Cleanup Task»

22) На шаге «*Select Report Options*» выбрать директорию, куда будет сохраняться файл журнала выполнения задания (Рисунок 15.19).

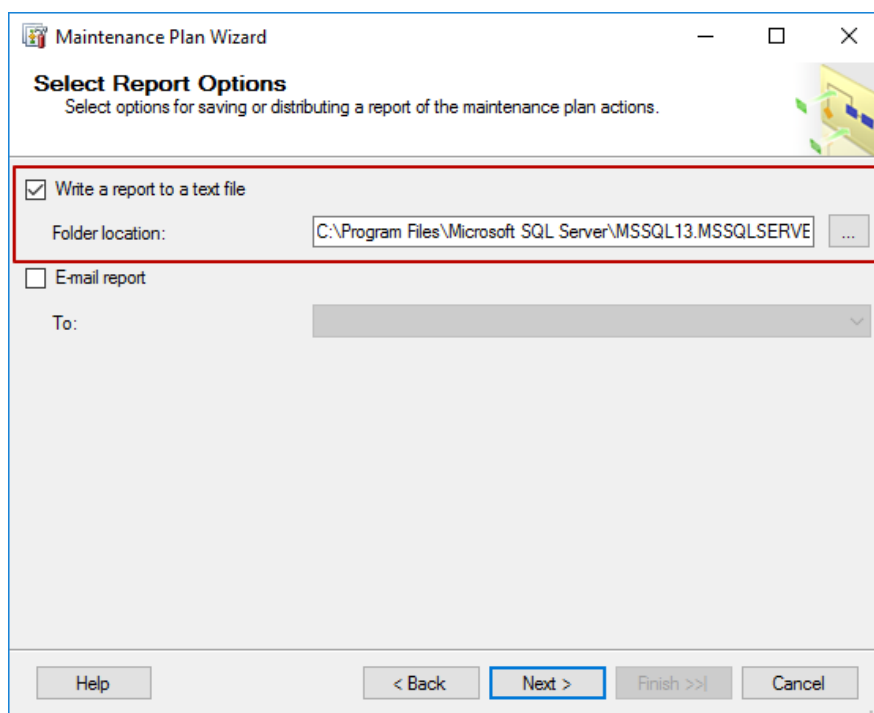


Рисунок 15.19 – Шаг «Select Report Options»

23) Проверить еще раз все настройки плана обслуживания и нажать кнопку «*Finish*» (Рисунок 15.20).

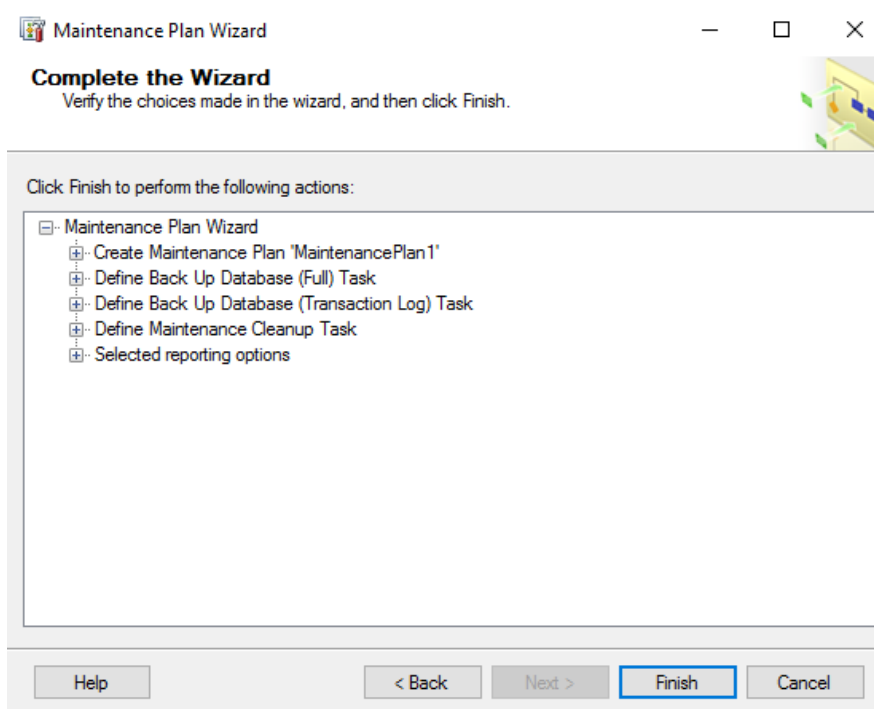


Рисунок 15.20 – Завершение работы мастера

Если мастер не обнаружит ошибок, то отобразится сообщение об успешном построении плана (Рисунок 15.21). В противном случае необходимо устранить ошибки и повторить процедуру снова.

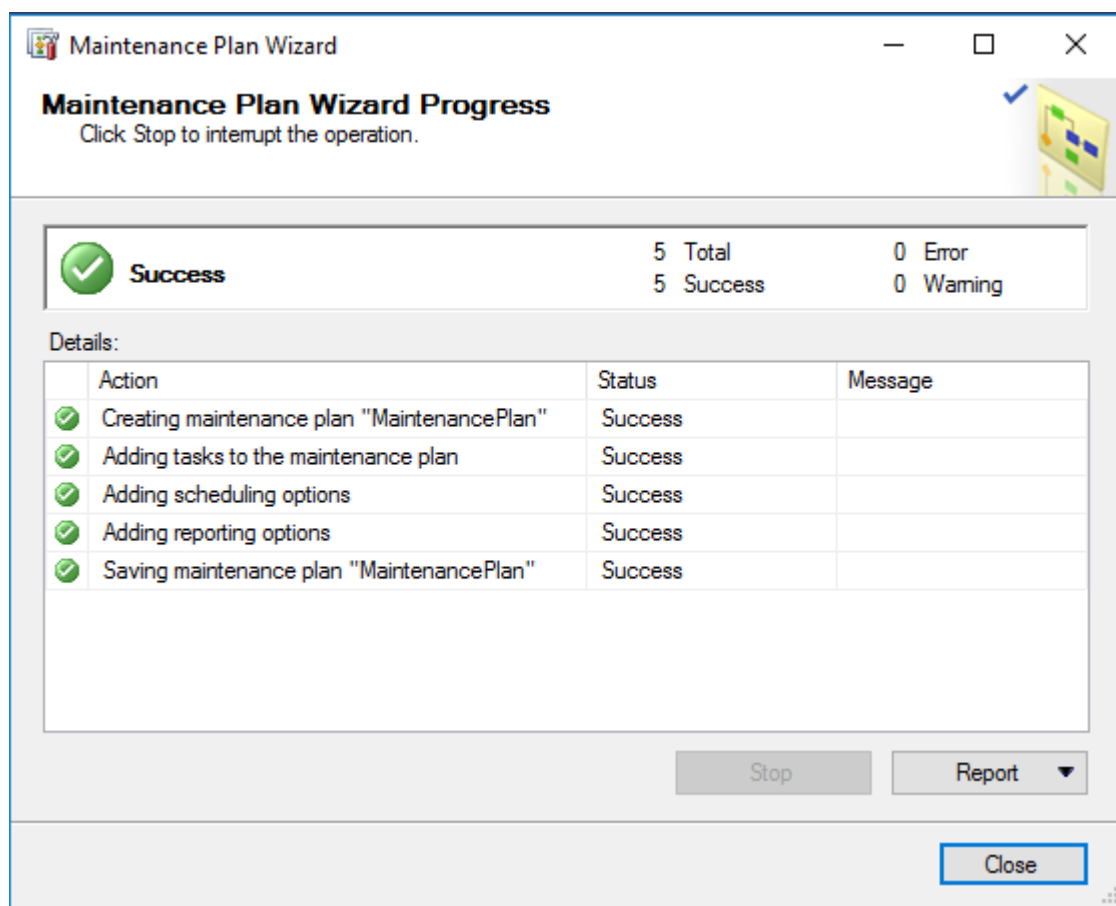


Рисунок 15.21 – Ход работы мастера планов обслуживания

- 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 15.22).

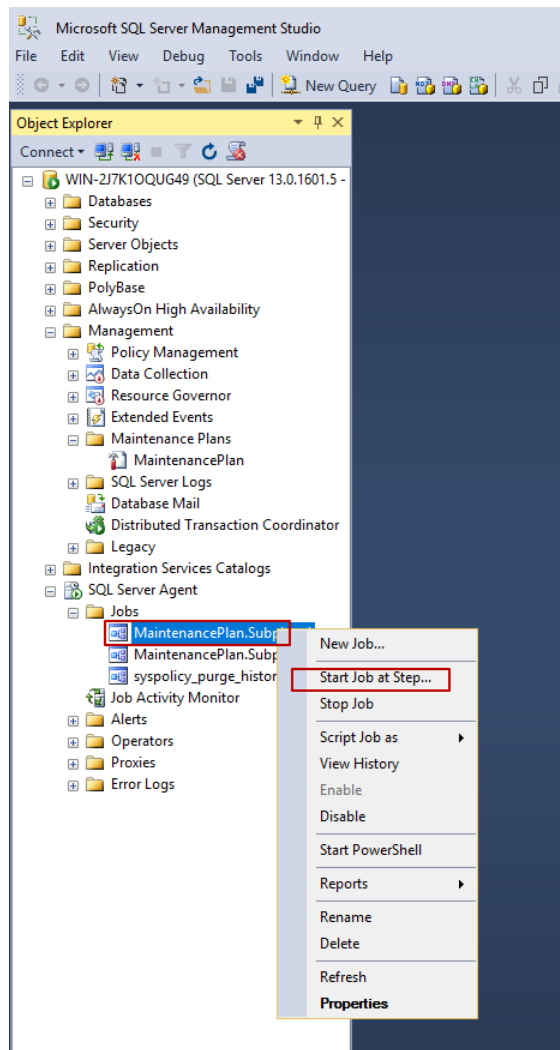


Рисунок 15.22 – Start job at Step

Запустится окно выполнения задания, в котором, должно появиться сообщение об успешном выполнении (Рисунок 15.23). Обязательно проверьте наличие файлов резервных копий в настроенном для их сохранения месте.

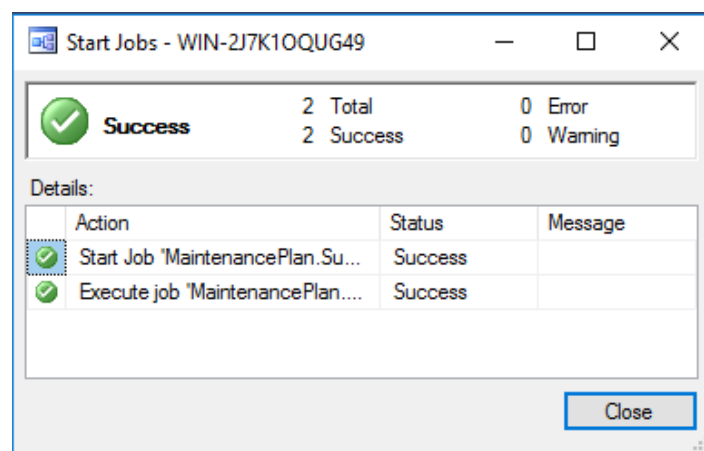


Рисунок 15.23 – Проверка запуска задания на шаге

## 15.5 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 «Резервное копирование базы данных» (Рисунок 15.24).

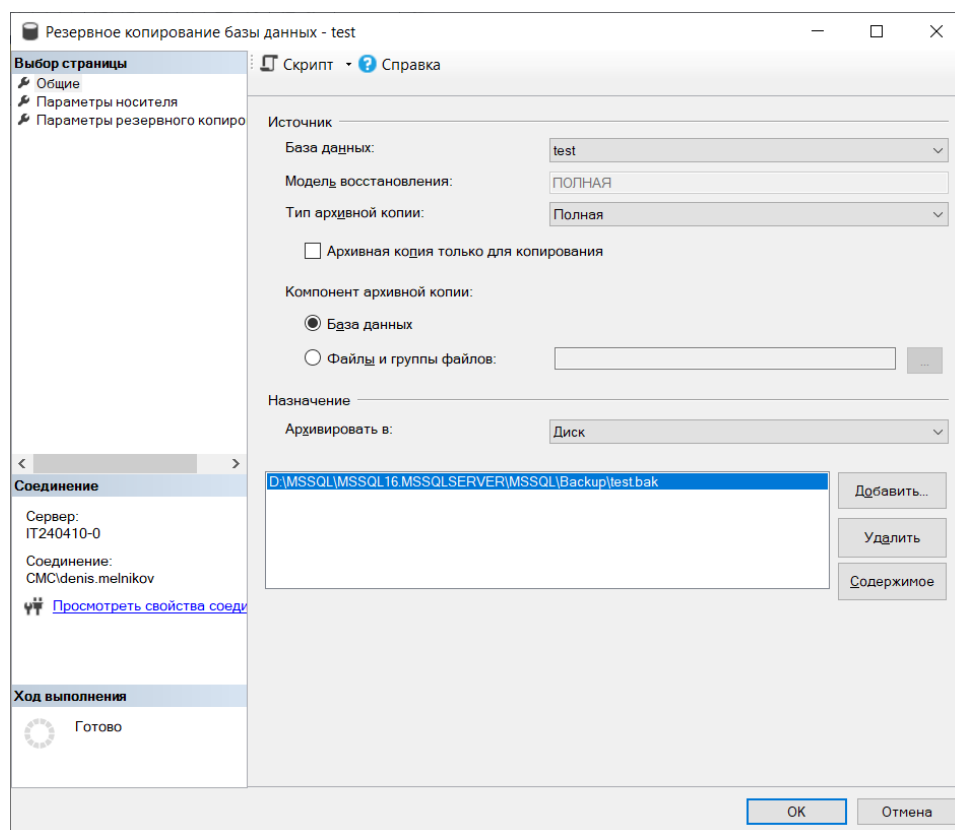


Рисунок 15.24 – Диалоговое окно «Резервное копирование базы данных»

В пункте *Место назначения* указывается устройство, либо имя файла, в котором будет сохраняться резервная копия БД. Нажатие кнопки «Добавить» дает возможность выбрать ранее созданное пользователем устройство.

## 15.6 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 15.25).

В нижней части открывшегося окна можно видеть все существующие резервные копии, из которых можно проводить восстановление.

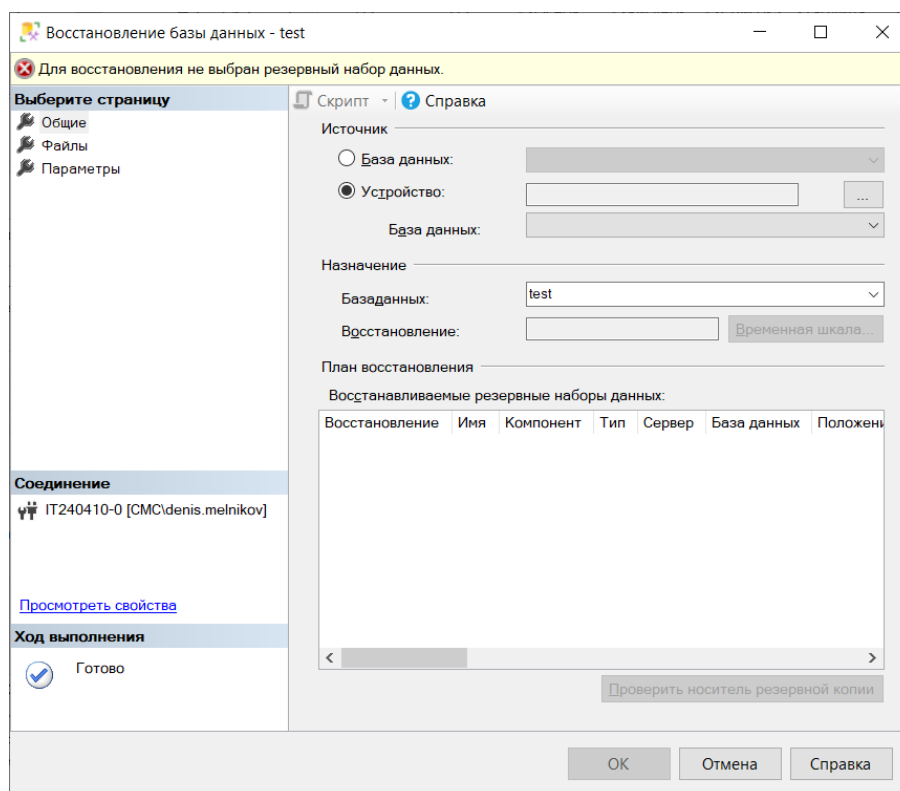


Рисунок 15.25 – Восстановление данных

## 15.7 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.

---

## 16 Резервное копирование данных ПК на СУБД PostgreSQL

### 16.1 Создание резервной копии базы данных средствами pg\_dump на MS Windows

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.

#### 16.1.1 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 выполнить 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=ZVKTEST
```

:: Директория, куда будет помещен бекап (полный путь)

```
set outputDirectoryPath="D:\PostgresqlBack"
```

:: Директория, установленного экземпляра PostgreSQL

```
set scriptDirectoryFullPath="C:\Program Files\PostgreSQL\15"
```

```
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 ZVK СУБД PostgreSQL на Localhost представлен на рисунке 16.1.



```
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=ASURE0TEST
:: 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 16.1 – Пример команды

2. Сохранить файл с расширением .bat (например, postgresqlBackup.bat).

## 16.1.2 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 16.2).

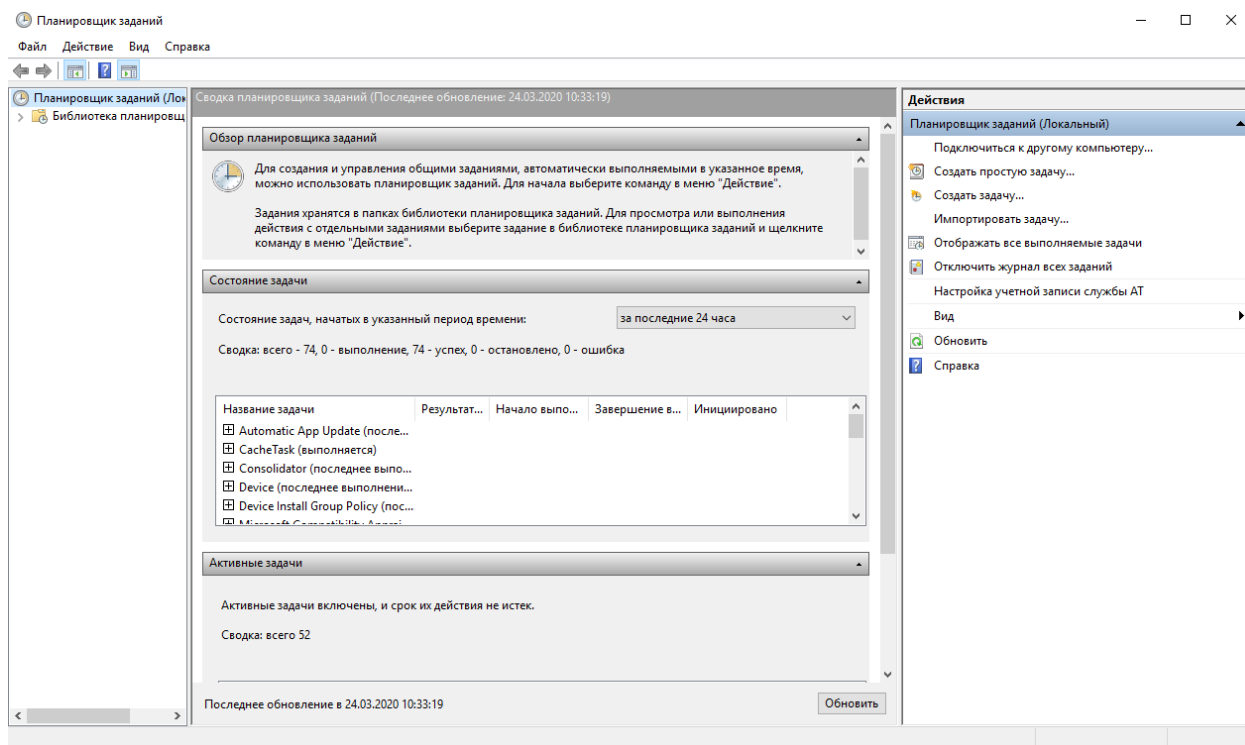


Рисунок 16.2 – Планировщик заданий

2. В Планировщике заданий (Task Scheduler) из раскрывающегося списка пункта меню «Действие» (Action) выбрать пункт «Создать задачу» (Create Task) (Рисунок 16.3).

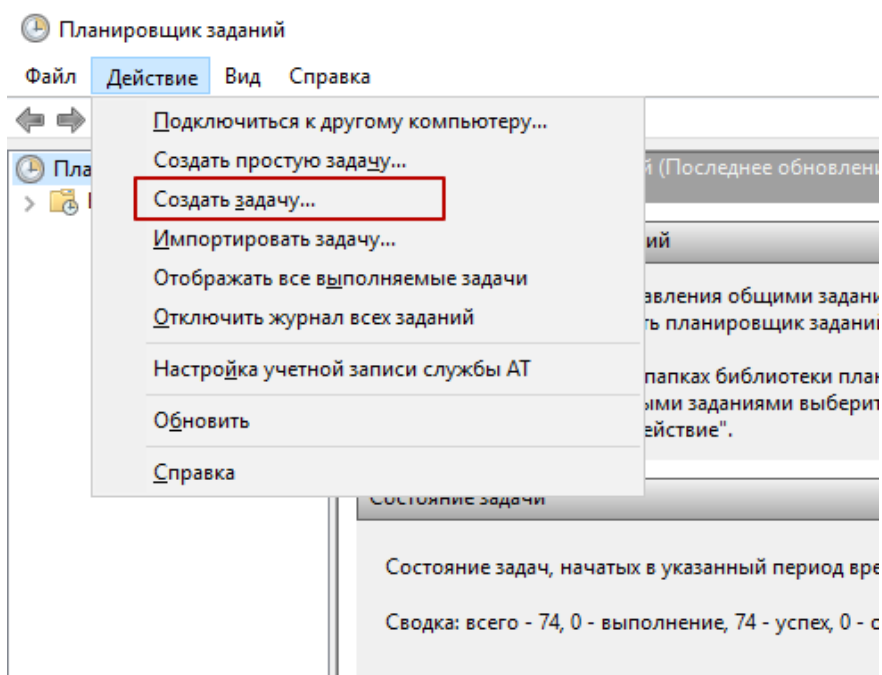


Рисунок 16.3 – Выбор пункта «Создать задачу»

3. В открывшейся форме «Создание задачи» (Create Task) на вкладке «Общее» (General) указать «Имя задачи» (Name), например, Создание бэкапов PostgreSQL (Рисунок 16.4).

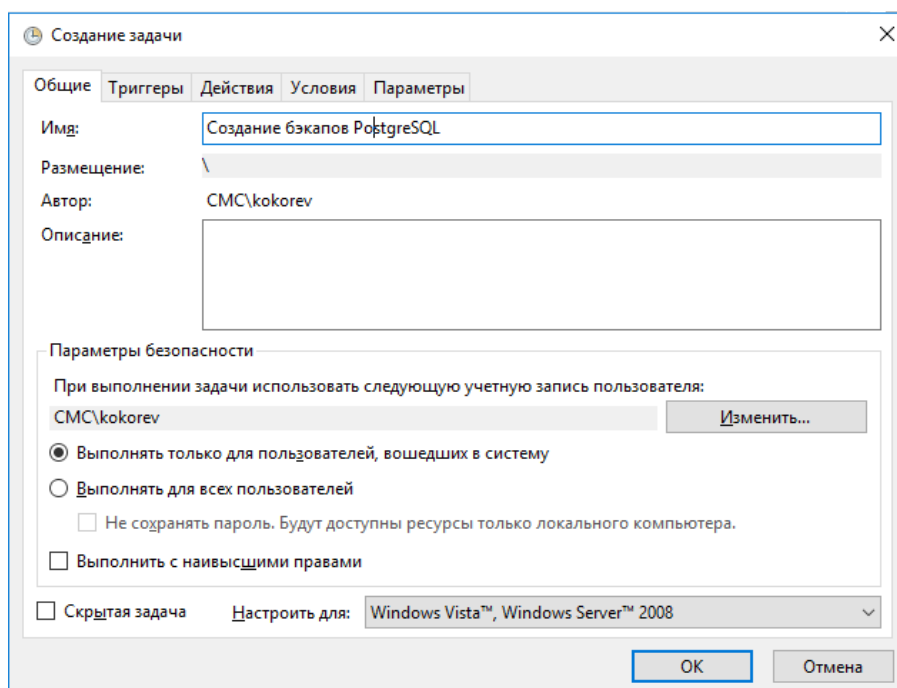


Рисунок 16.4 – Ввод имени задачи

4. Далее необходимо перейти на вкладку «Триггеры» (Triggers) и нажать кнопку «Создать» (New) (Рисунок 16.5).

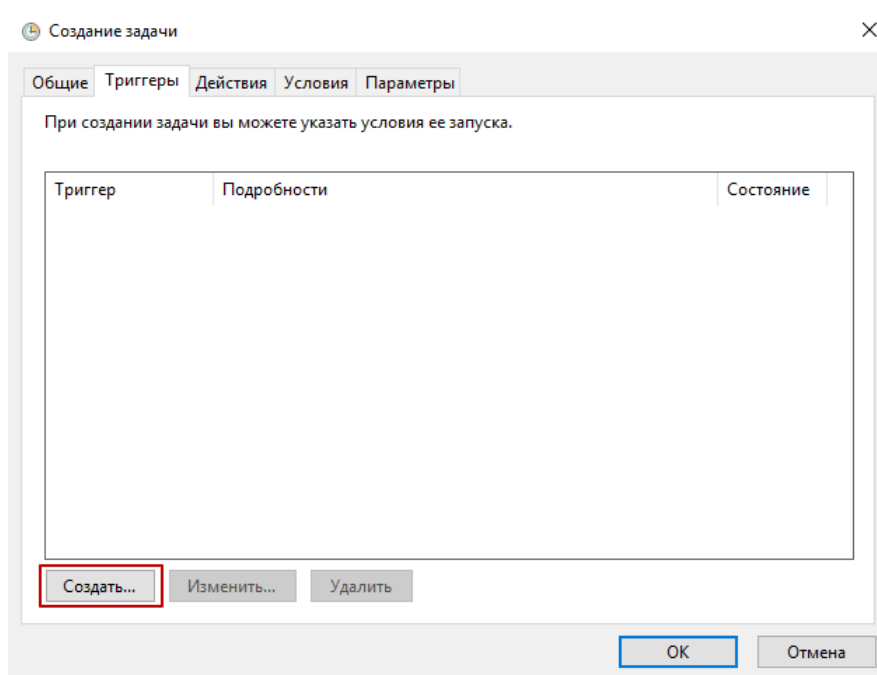


Рисунок 16.5 – Создание триггера

5. В открывшейся форме «Создание триггера» (New Trigger) настроить расписание запуска задания (в данном случае задание будет запускаться каждый день в 01-00) (Рисунок 16.6).

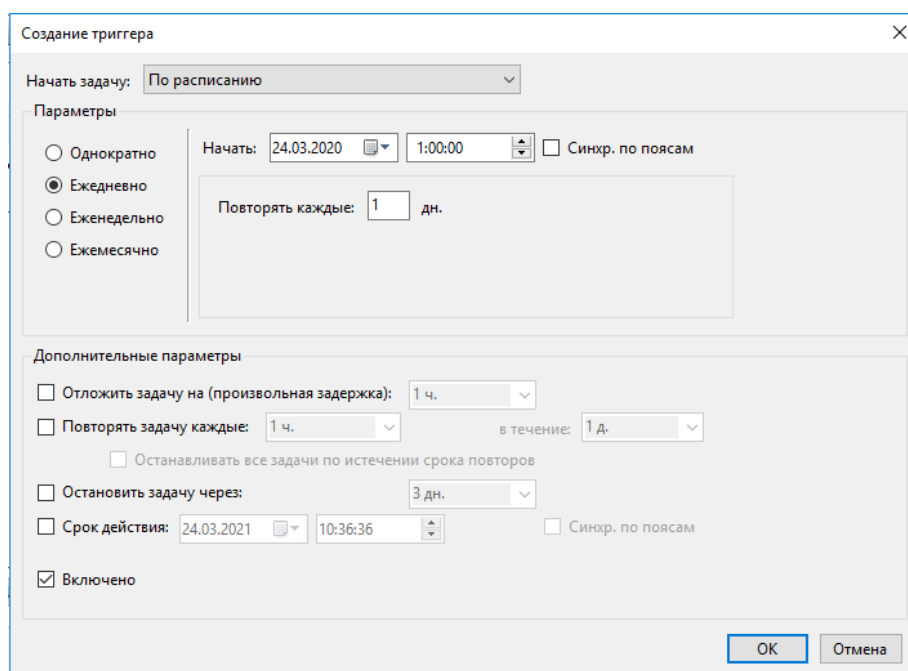


Рисунок 16.6 – Настройка расписания запуска задания

6. На вкладке «Действия» (Actions) необходимо указать действие нашего задания, для этого необходимо нажать кнопку «Создать» (New) (Рисунок 16.7).

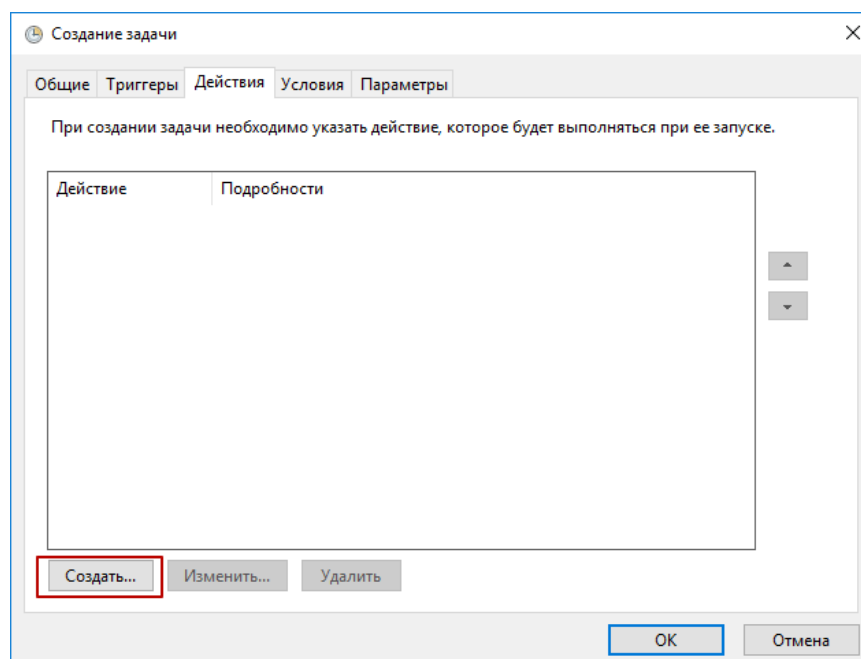


Рисунок 16.7 – Создание действия

7. В открывшейся форме «Создание действия» (New Action) указать действие – запуск файла «*postgresqlBackup.bat*» с локального диска D (Рисунок 16.8).

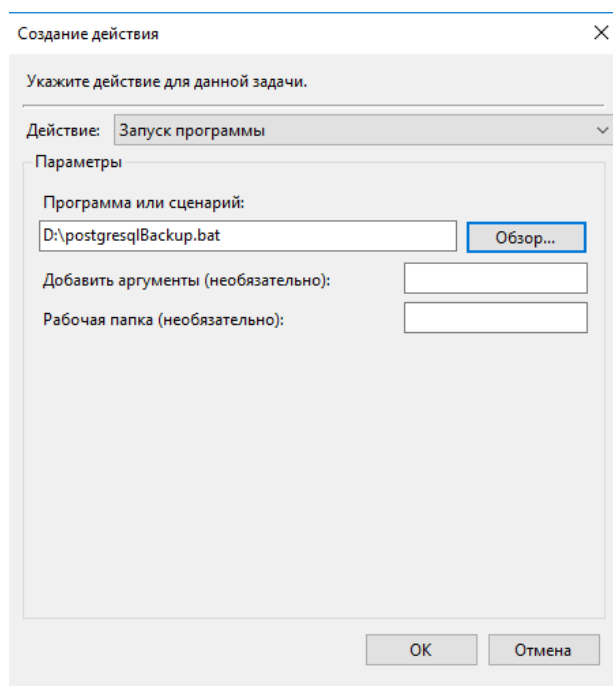


Рисунок 16.8 – Указание действия

8. На форме «Создание задачи» (Great Task) нажать кнопку «ОК» (Рисунок 16.9), в результате чего будут созданы: .bat файл с командой создания резервной копии БД на СУБД PostgreSQL и задания планировщика Windows на запуск этого .bat файла.

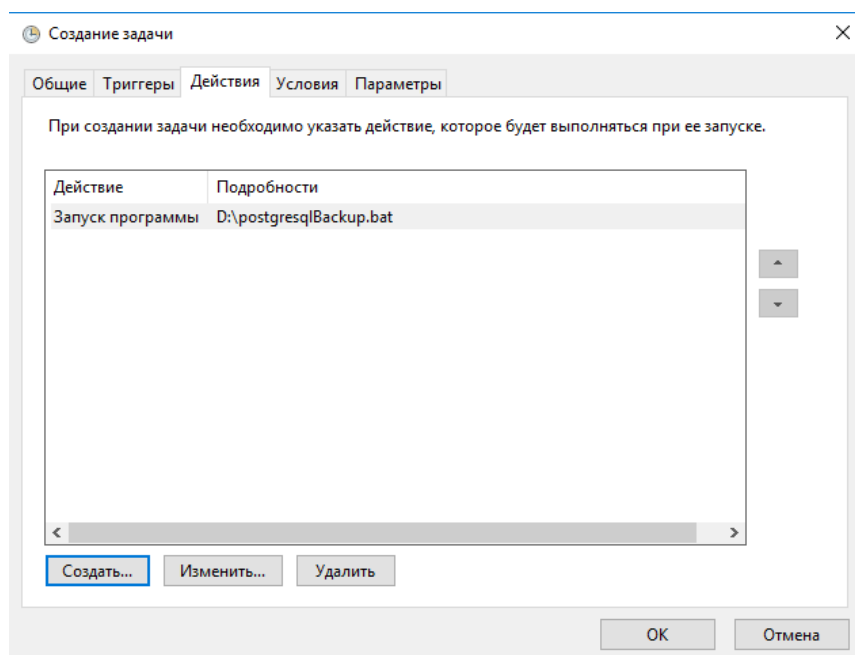


Рисунок 16.9 – Завершение создания

## 16.2 Создание резервной копии базы данных средствами `pg_dump` на Linux

Резервирование выполняется на СУБД PostgreSQL. Для проведения процедуры резервного копирования необходимо выполнить следующие действия:

- 1) Определить место хранения будущей резервной копии.
- 2) Создать скрипт, который будет вызывать утилиту `pg_dump`.
- 3) Создать задание в планировщике `cron` на выполнение скрипта

### 16.2.1 Создание скрипта бэкапирования

Создать скрипт и открыть его на редактирование, например, командой:

```
nano backup.sh
```

```
#!/bin/sh
PATH=/etc/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
PGPASSWORD=post_pass # пароль пользователя БД
export PGPASSWORD
pathB=/opt/zvk/backup_db # путь хранения бэкапов БД
dbUser=post_user # имя пользователя БД
database=post_db # название БД
host=127.0.0.1 # IP адрес СУБД
find $pathB -type f -mtime +7 -exec rm -rf {} \; # задается глубина хранения бэкапов БД, бэкапы
старше +N дней будут удаляться
pg_dump -U $dbUser -d $database -h $host -Fc > $pathB/${database}_${date +%Y-%m-%d-%H}.bak
```

*unset PGPASSWORD*

Задать скрипту право на выполнение командой: *chmod +x backup.sh*

### 16.2.2 Создание задачи планировщика cron

Создать задачу планировщика можно командой: *sudo crontab -e*. Далее необходимо указать периодичность выполнения и сам скрипт. Например, для выполнения ежедневно в час ночи прописать строку:

```
00 01 * * * /opt/zvk/backup.sh
```

## 16.3 Создание резервной копии базы данных в инструментари PGAdmin

Для создания резервной копии базы данных экземпляра в инструментари 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 16.10).

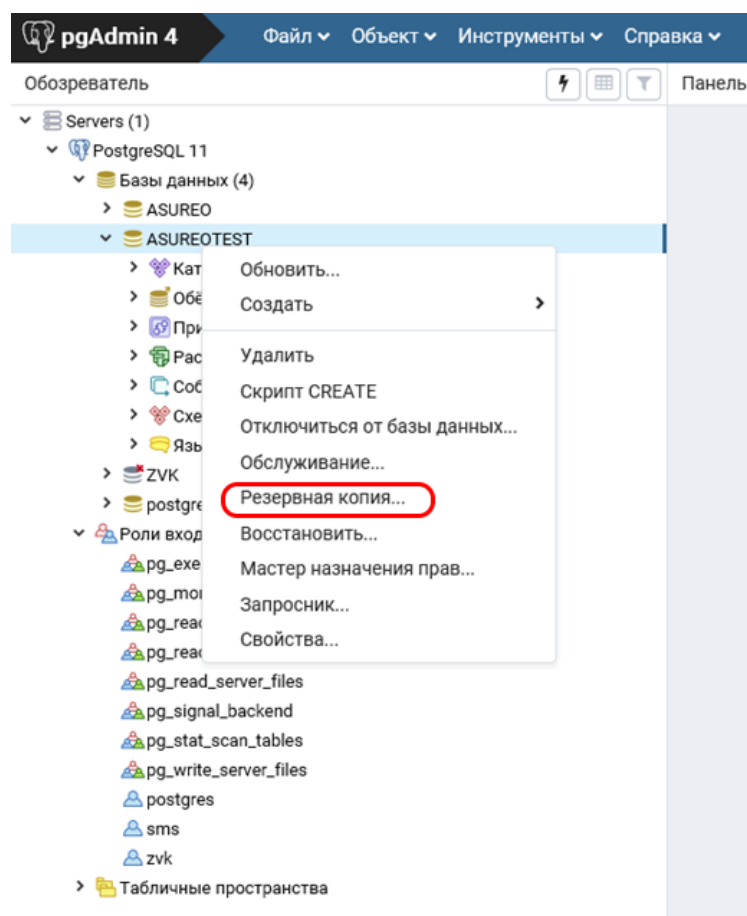


Рисунок 16.10 – Выбор пункта «Резервная копия»

2. В появившемся диалоговом окне необходимо указать путь и имя файла резервной копии, а также указать формат «Tar» (Рисунок 16.11).

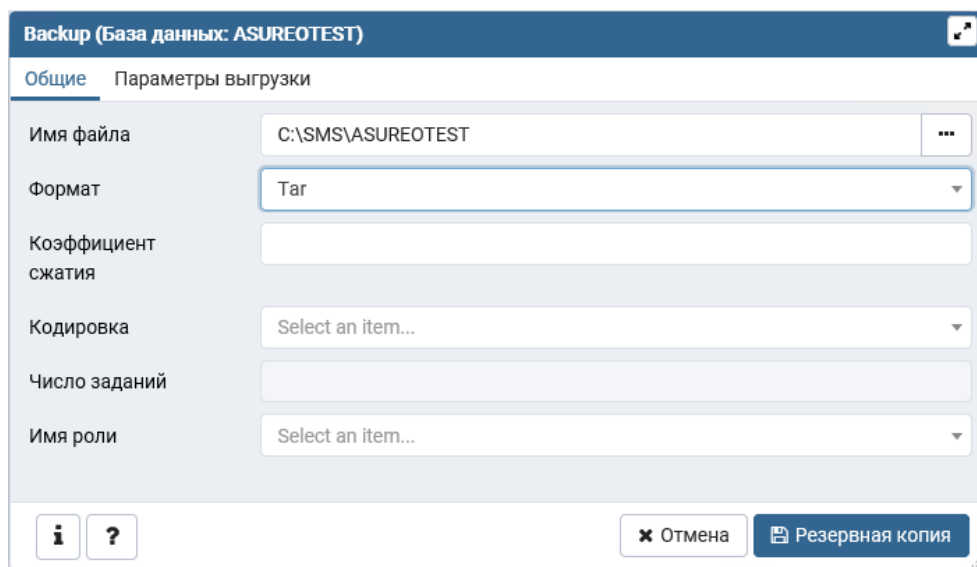


Рисунок 16.11 – Диалоговое окно «Backup (База данных: ASUREOTEST)»

3. Нажать кнопку «Резервная копия» и дождаться завершения процесса создания копии базы данных (Рисунок 16.12).

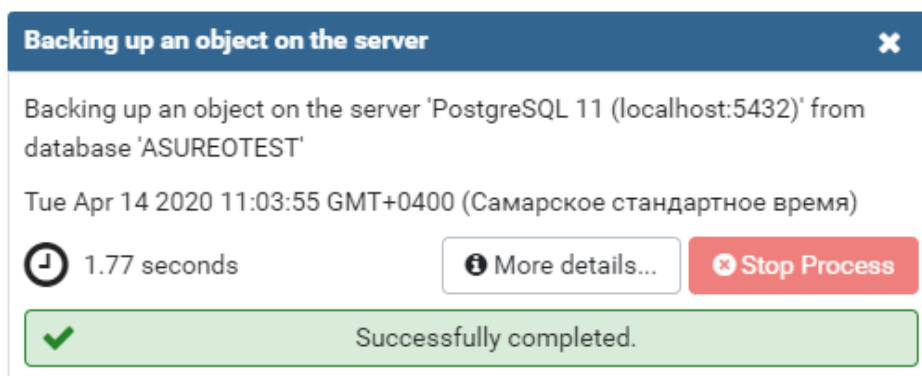


Рисунок 16.12 – Завершение процесса создания копии базы данных

## 16.4 Восстановление БД из резервной копии средствами pg\_restore

Для восстановления базы данных из резервной копии экземпляра можно использовать утилиту pg\_restore.exe.

Перед восстановлением необходимо создать базу данных.

Для выполнения команды восстановления базы данных необходимо выполнить следующие действия:

1. Для MS Windows предварительно запустить командную строку – на клавиатуре нажать клавиши «Win+R», в открывшемся окне «Выполнить» ввести команду «cmd» и нажать кнопку [OK].

2. Выполнить в консоли Linux или Windows команду (Рисунок 16.13):

**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.

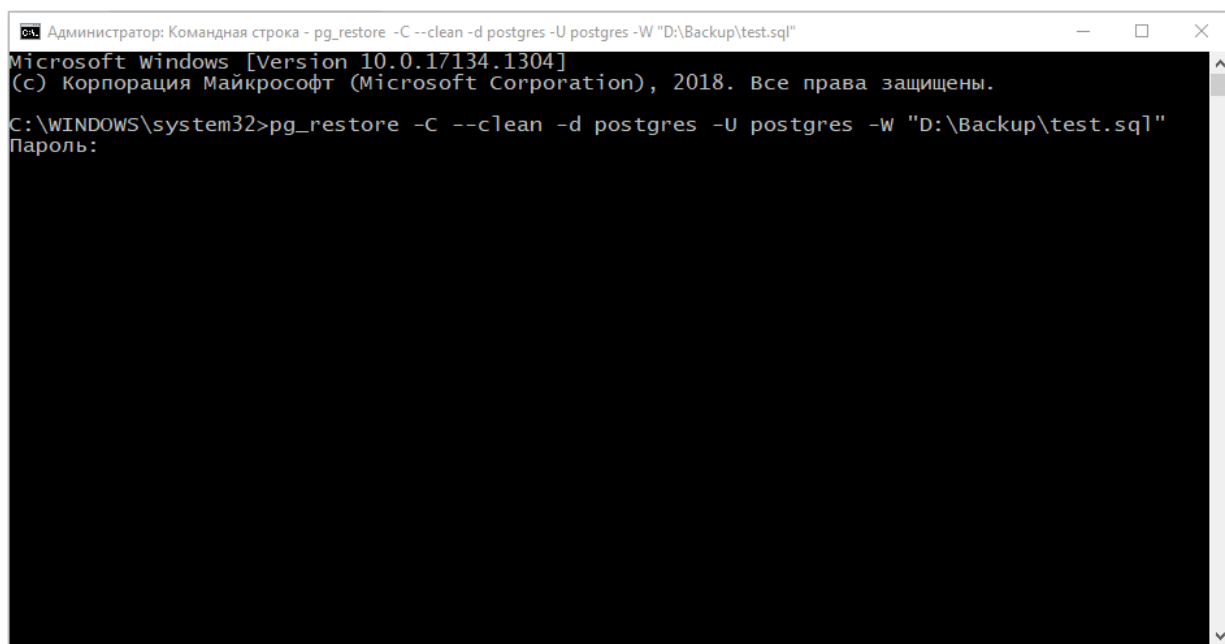


Рисунок 16.13 – Пример команды

## 16.5 Восстановление БД из резервной копии в инструментарии PGAdmin

Для восстановления базы данных из резервной копии экземпляра в инструментарии PGAdmin необходимо выполнить следующие действия:

1. Правым кликом мыши вызвать контекстное меню БД и в контекстном меню выбрать пункт «Восстановить» (Рисунок 16.14).

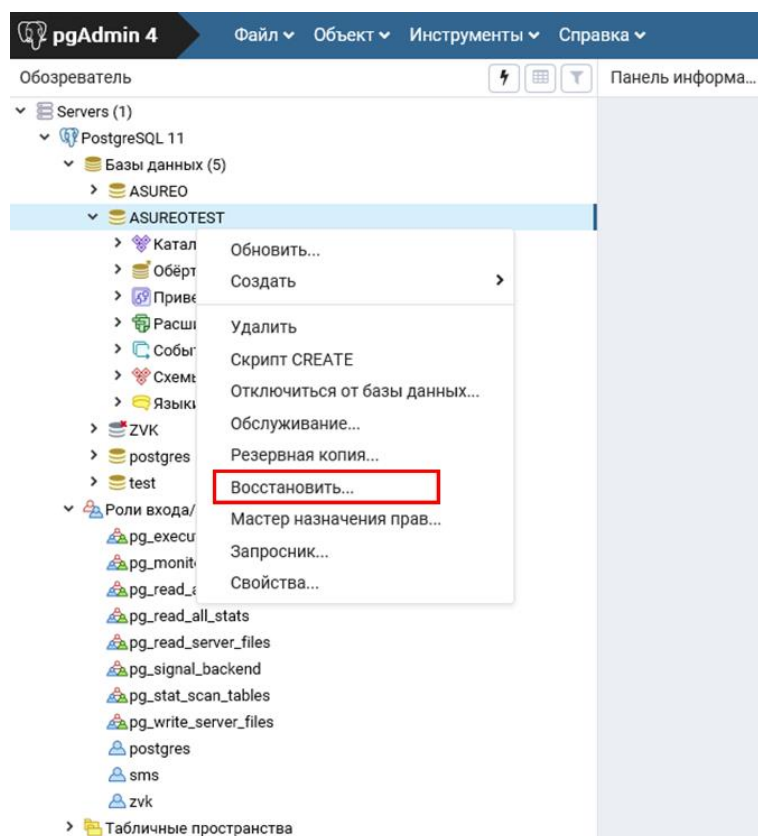


Рисунок 16.14 – Выбор пункта «Восстановить»

2. В появившемся диалоговом окне необходимо указать формат «Специальный или tar», а также путь и имя файла резервной копии (Рисунок 16.15).

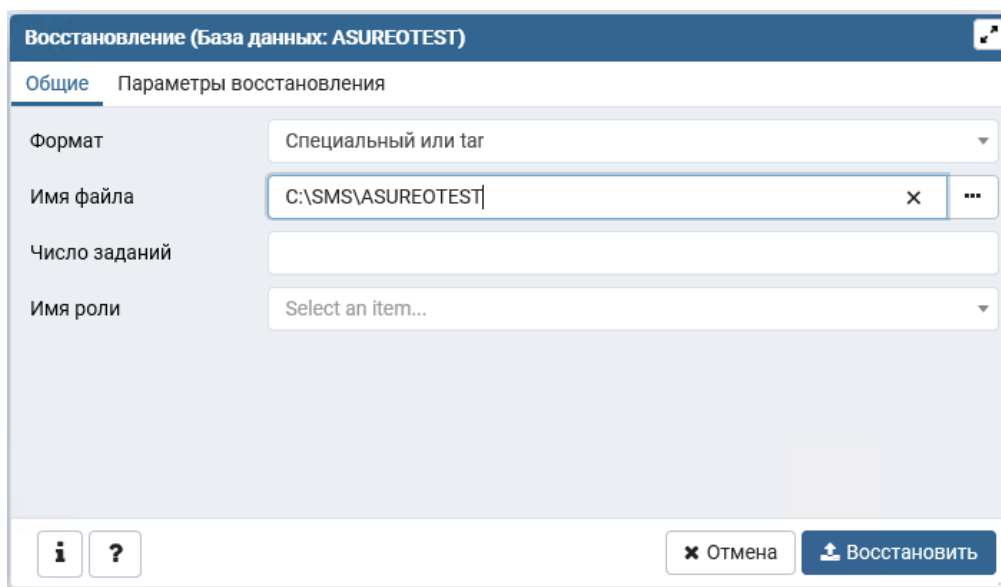


Рисунок 16.15 – Диалоговое окно «Восстановление (База данных: ASUREOTEST)»

3. Нажать кнопку «Восстановить» и дождаться завершения процесса восстановления базы данных (Рисунок 16.16).

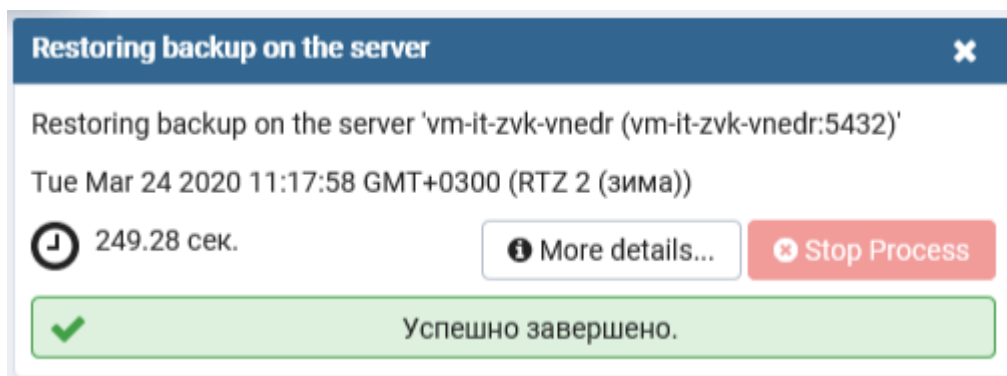


Рисунок 16.16 – Завершение процесса восстановления базы данных

Для работы ПК необходимо создать пользователя, из-под которого будет осуществляться подключение к серверу СУБД. Для создания пользователя в инструментарии PGAdmin необходимо выполнить следующие действия:

1. В контекстном меню пункта «Login/Group Role» выбрать «Create – login/Group Role» (Рисунок 16.17).

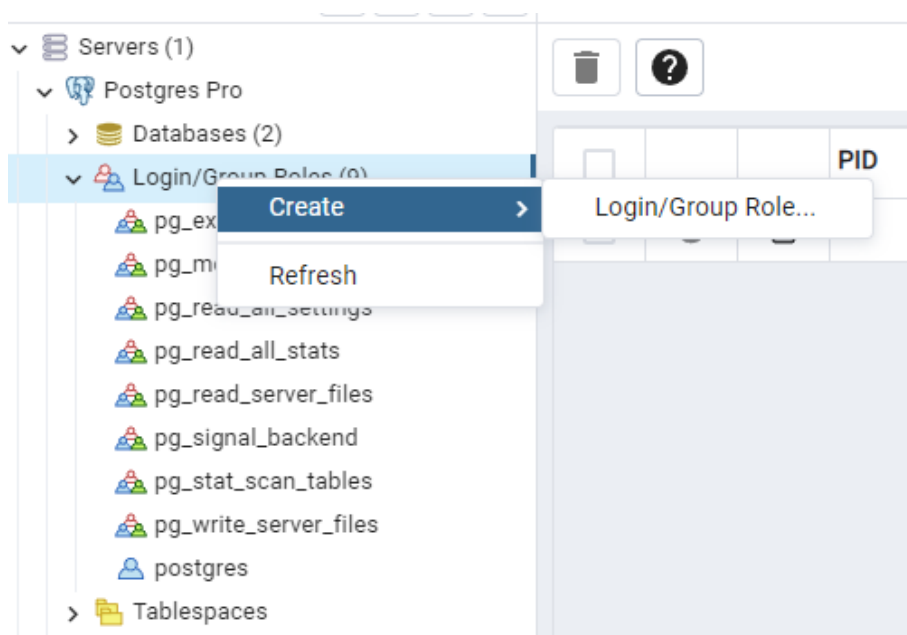


Рисунок 16.17 – Выбор «Create – login/Group Role»

2. В диалоговом окне создания пользователя необходимо указать имя пользователя (Рисунок 16.18), пароль (Рисунок 16.19) и назначить права (Рисунок 16.20).

**Create - Login/Group Role**

General Definition Privileges Membership Parameters Security SQL

Name: sms

Comments:

Close Reset Save

Рисунок 16.18 – Указание имя пользователя

**Create - Login/Group Role**

General Definition Privileges Membership Parameters Security SQL

Password: ...

Account expires: No Expiry

Connection limit: -1

Please note that if you leave this field blank, then password will never expire.

Close Reset Save

Рисунок 16.19 – Указание пароля

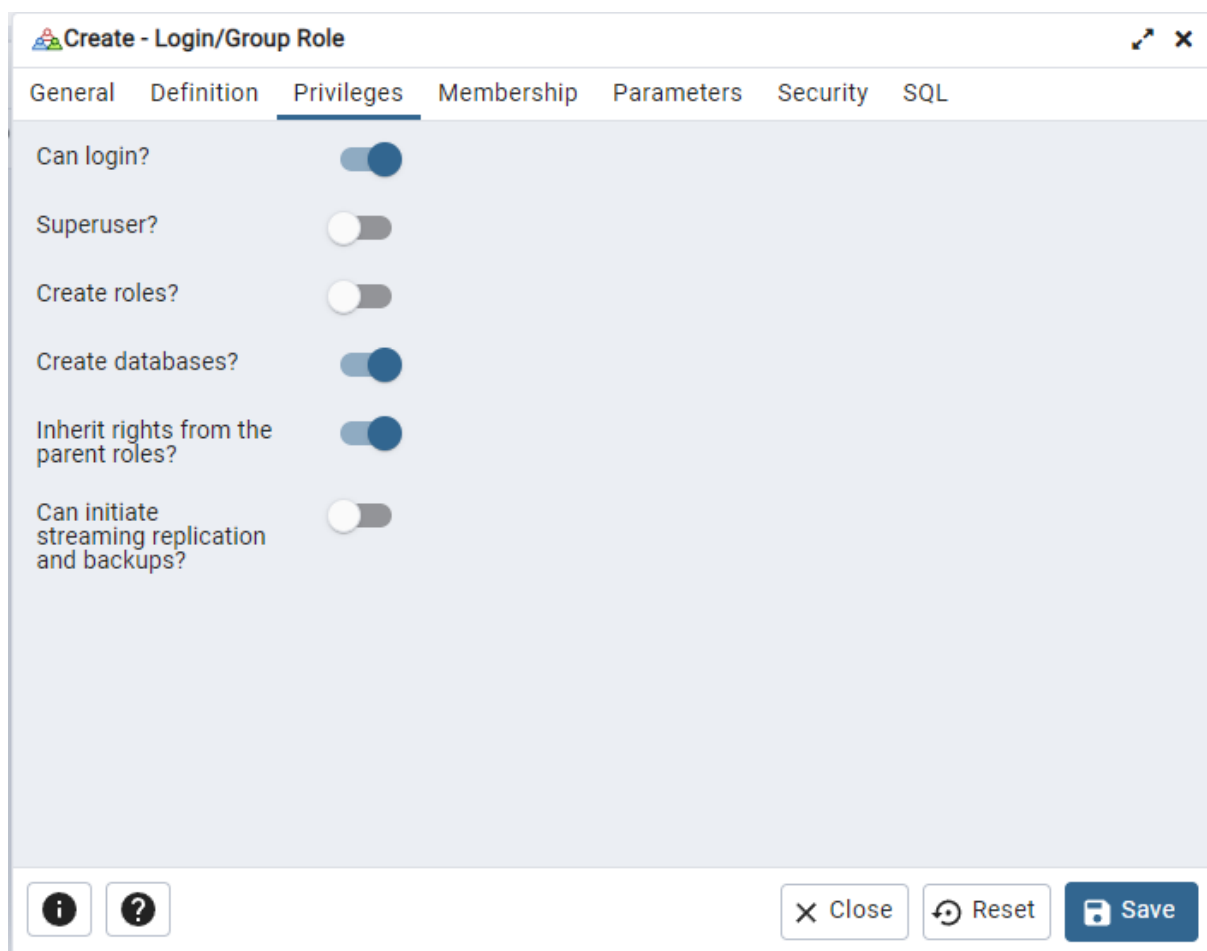


Рисунок 16.20 – Назначение прав

---

## 17 Настройка карты многоэкземплярной конфигурации

### 17.1 Использование карты

Если пользователь работает с несколькими экземплярами приложения ПК, то для быстрого запуска требуемого экземпляра можно использовать карту многоэкземплярной конфигурации (Рисунок 17.1).

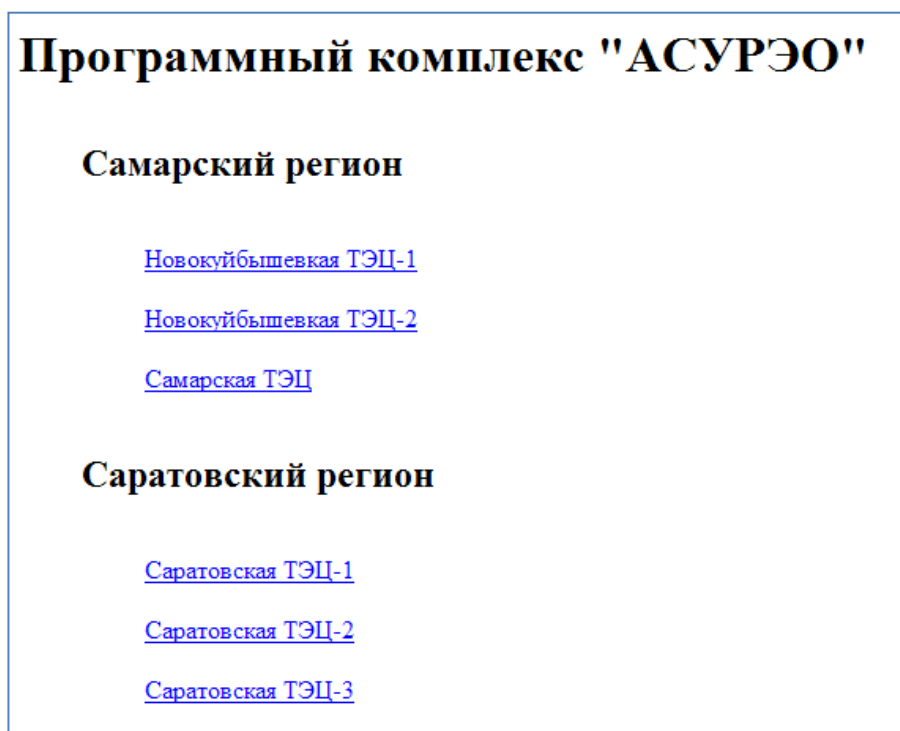


Рисунок 17.1 – Пример карты многоэкземплярной конфигурации

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.

### 17.2 Создание карты

Пользователи, знающие язык разметки гипертекстов (html), могут создать карту многоэкземплярной конфигурации с помощью любого редактора HTML (Рисунок 17.2).

```

1 <H1>Программный комплекс "АСУРЭО"</H1>
2

3 <dd><H2>Самарский регион</H2>
4

5 <dd><dd>Новокуйбышевская ТЭЦ-1

6 <dd><dd>Новокуйбышевская ТЭЦ-2

7 <dd><dd>Самарская ТЭЦ

8

9 <dd><H2>Саратовский регион</H2>
10

11 <dd><dd>Саратовская ТЭЦ-1

12 <dd><dd>Саратовская ТЭЦ-2

13 <dd><dd>Саратовская ТЭЦ-3


```

Рисунок 17.2 – 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 17.3).

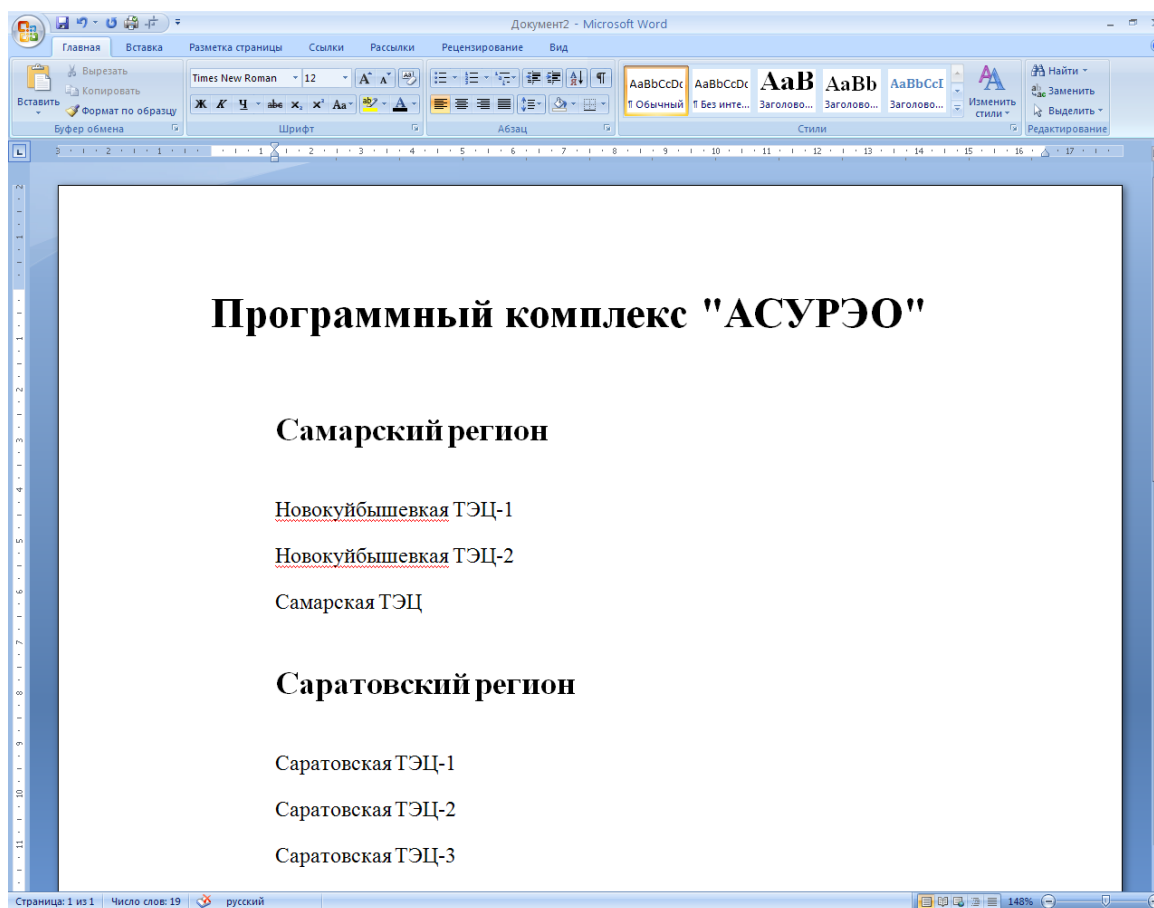


Рисунок 17.3 – Названия экземпляров в документ MS Word

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 17.4).

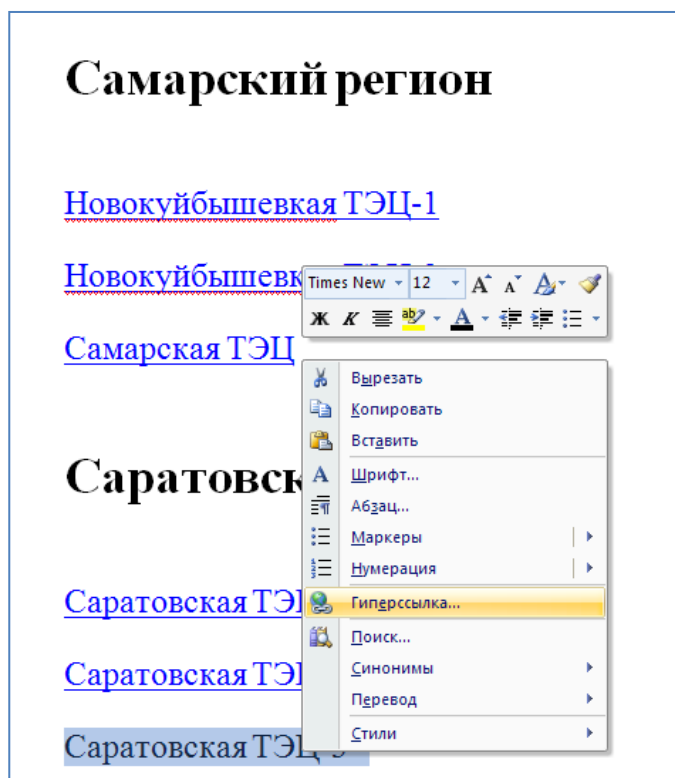


Рисунок 17.4 – Выделение названия экземпляра для вставки гиперссылки

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 «13.2 Настройка клиентского рабочего места и установка клиентской части Системы на MS Windows»).

4) Нажать на кнопку «OK» (Рисунок 17.5).

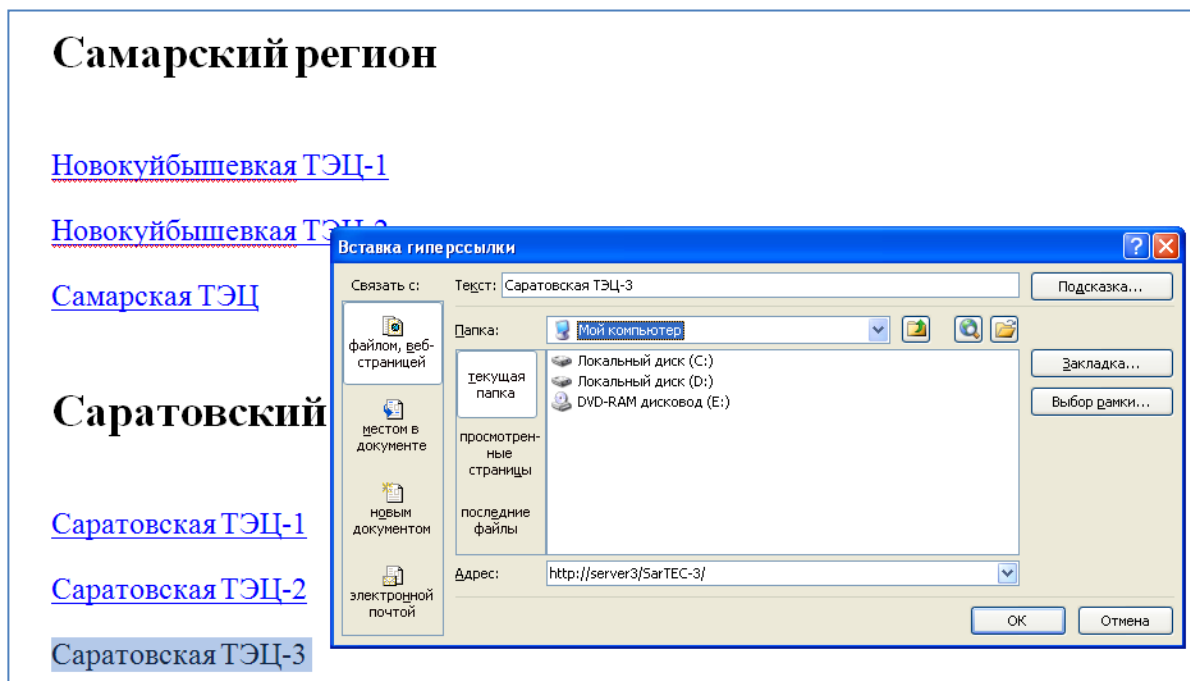


Рисунок 17.5 – Окно вставки адреса гиперссылки

5) Для каждого названия экземпляра повторить шаги 1-4.

Отформатированный текст документа представлен на рисунке 17.6.

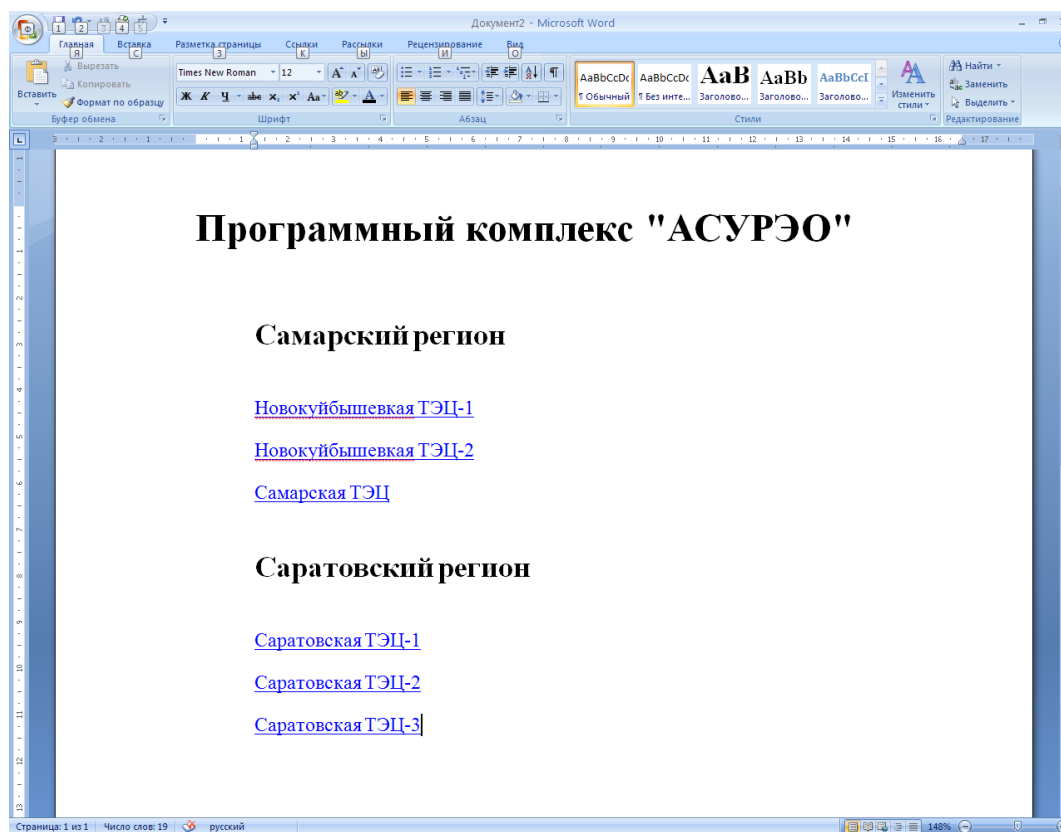


Рисунок 17.6 – Создание карты с помощью текстового редактора MS Word

По завершению форматирования документа его необходимо сохранить в формате HTML:

1) В раскрывающемся меню «Сохранить как» необходимо выбрать раздел «Другие форматы» (Рисунок 17.7).

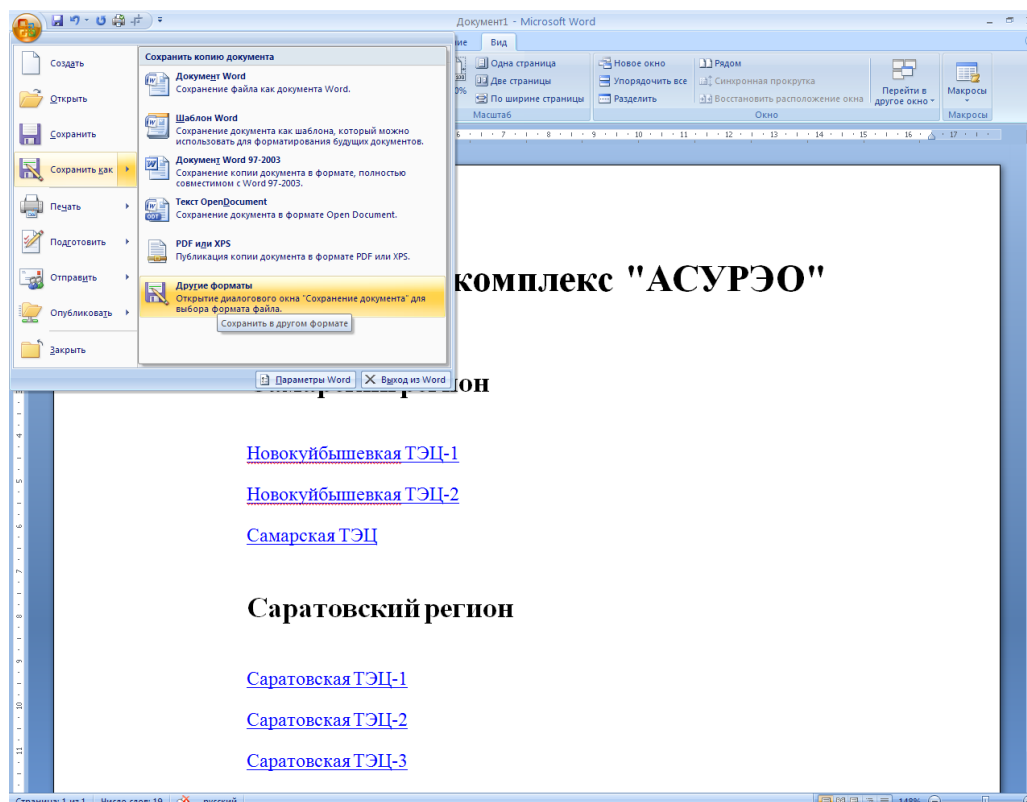


Рисунок 17.7 – Сохранение документа в формате HTML

2) В появившемся диалоговом окне «Сохранение документа» указать параметры сохранения: имя файла - index, тип файла - Веб-страница (Рисунок 17.8).

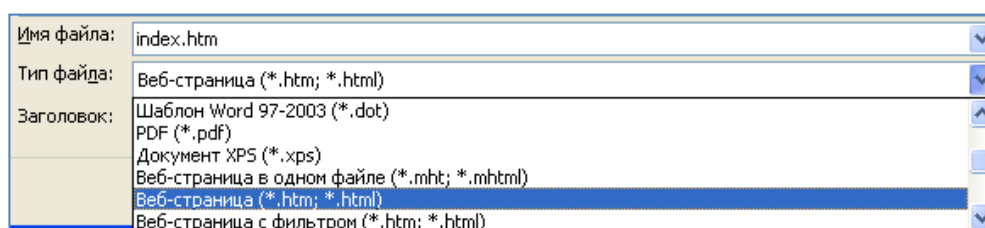


Рисунок 17.8 – Параметры сохранения

3) Нажать на кнопку «Сохранить».

### 17.3 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).

Для nginx: возможно создать директорию в /opt/zvk, например, map. Положить сохранённый файл в данную директорию. После чего в секцию volumes для контейнера веб-сервера добавить строку

- `./map:/etc/nginx/www/map`

В таком случае ссылка на данную страничку будет иметь адрес: `http://<имя сервера>:<порт>/map/index.html`

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 17.9).

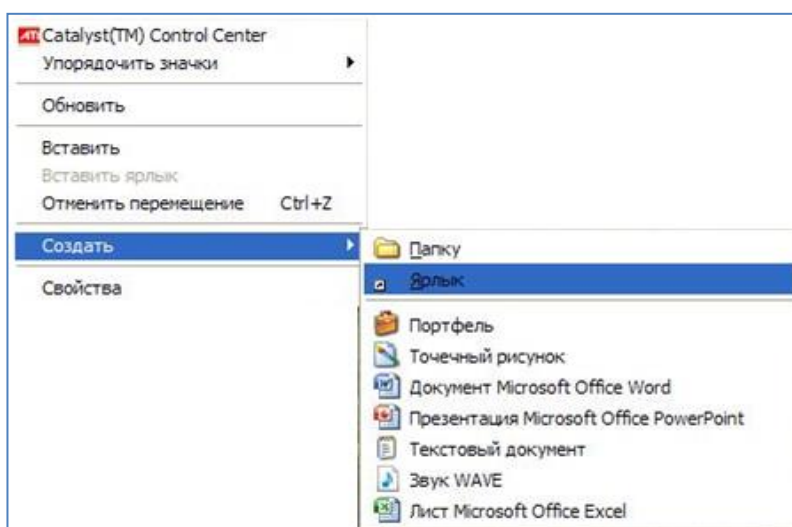


Рисунок 17.9 – Создание ярлыка

2) Указать размещение объекта (Рисунок 17.10):

- 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).

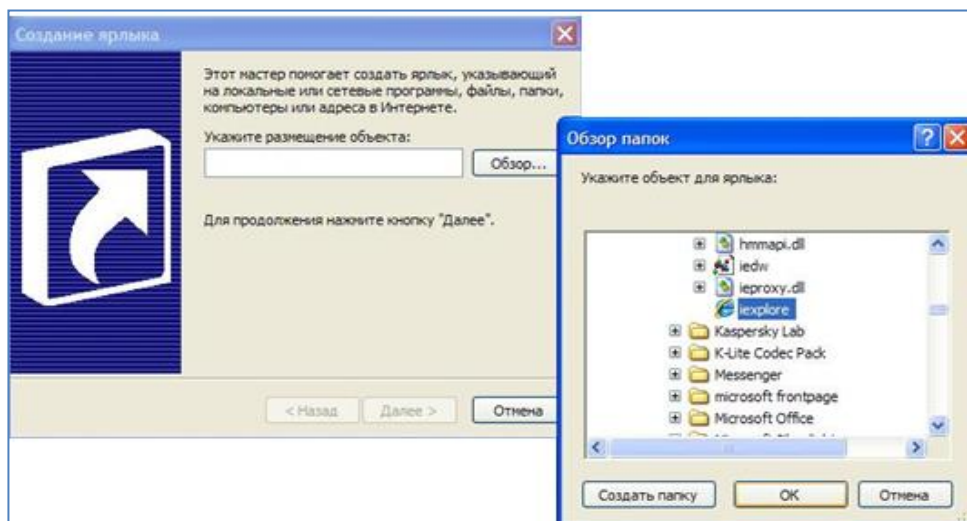


Рисунок 17.10 – Указание размещения объекта

3) В поле с адресом размещения объекта через пробел прописать: -new «адрес страницы», т.е. -new http://<имя сервера>:<порт>/index.html (Рисунок 17.11).

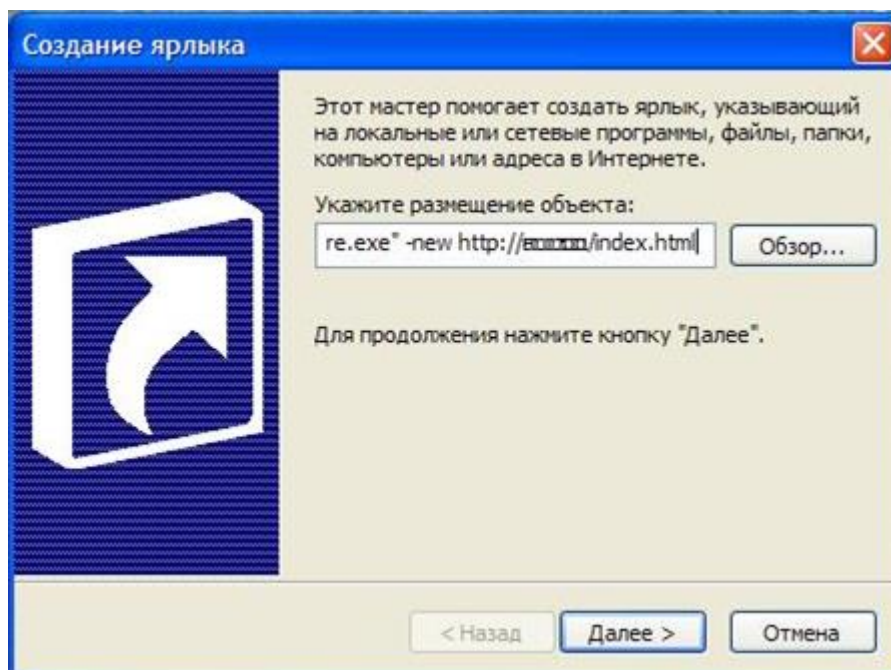


Рисунок 17.11 – Указание адреса страницы

- 4) Нажать на кнопку «Далее».
- 5) Ввести имя ярлыка и нажать на кнопку «Готово» (Рисунок 17.12).

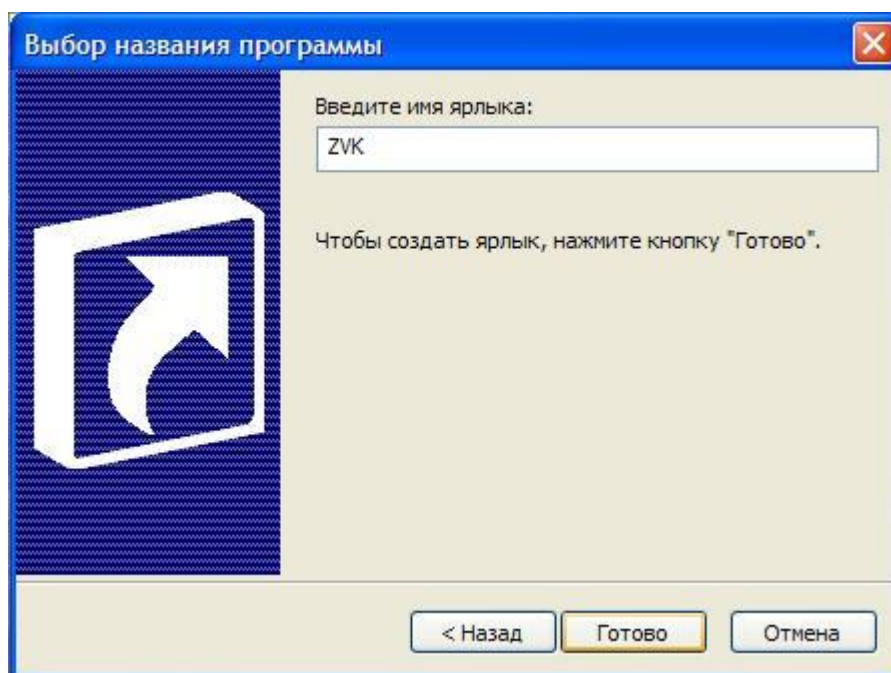


Рисунок 17.12 – Указание названия ярлыка

## 18 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 18.1.

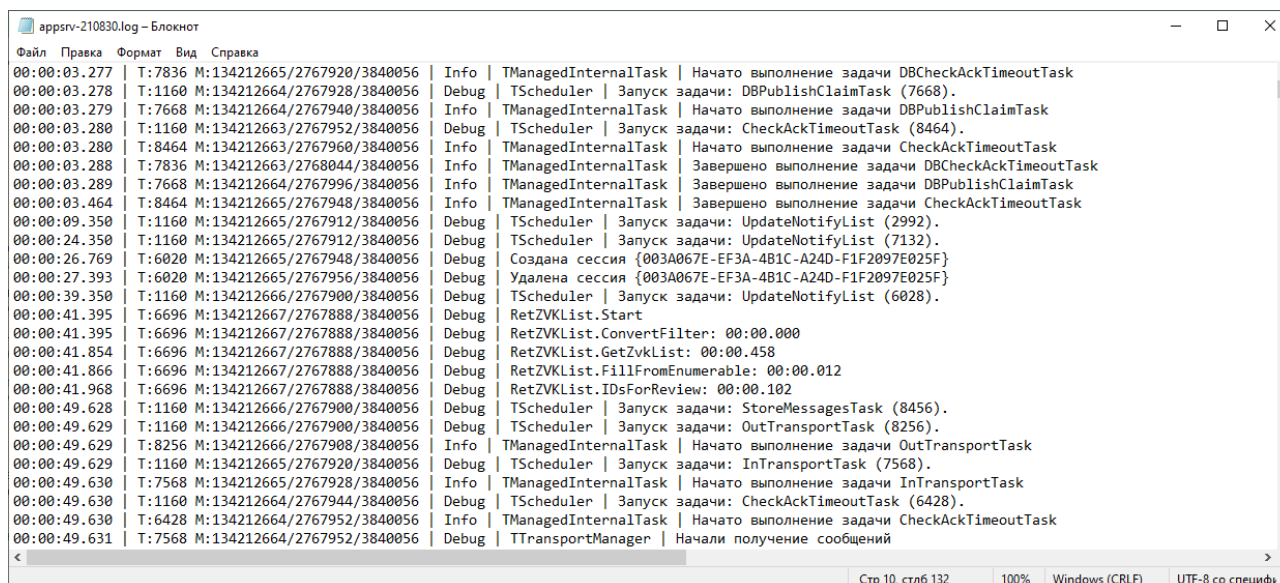


Рисунок 18.1 – Исключения типа Fatal и Access violation

Во избежание ошибок, рекомендуется:

1. Для оперативного анализа работы Системы просматривать текущие лог-файлы appsrv, FatalErr при помощи приложения Notepad++.
2. Избегать копирования файлов быстроизменяющихся текущих логов большого размера: WebCalls, ShedulerTasks.
3. При необходимости отправки файлов логов и их архивирования – производить архивирование в иную папку, отличную от папки с текущимлогами.
4. При необходимости анализа или отправки файлов логов за текущие сутки (при работающем сервисе приложений, особенно с высокой нагрузкой) – открывать в приложении Notepad++ и копировать содержимого файла лога в другой файл, расположенный вне папки с текущимлогами.

При работе сервера приложения на ОС семейства Linux формируются логи сервера приложения. Файлы логов сервера приложения на ОС семейства Linux монтируются из docker контейнера на хост и расположены в каталоге /opt/zvk/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, 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.

## 18.1 Удаление старых логов

При длительной работе накапливается много логов и их необходимо чистить, чтобы избежать поломки сервера – переполнением дискового пространства системы.

В Linux можно настроить Cron на ежедневную автоматическую очистку логов.

Для этого необходимо написать bash скрипт с именем «del\_logs.sh»:

```
#!/bin/bash

del Logs if > 30 days

find /opt/zvk/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/zvk/del\_logs.sh # delete logs if > 30 days

---

## 19 Логирование ZRP.Net

Настройка логирования сервера приложений заявок выполняется в файлах `serilogsettings.json` расположенных в папке ZRP.NET для прикладного приложения и Identity для сервера авторизации.

По умолчанию файлы логов записываются в папку Logs ZRP.NET.

Файлы логов имеют названия:

- **backend-all-`ггггммдд`.log**. Подключен по умолчанию. Содержит в себе все сообщения (общие логи);
- **backend-api-call-`ггггммдд`.log**. Подключен по умолчанию. Содержит в себе вызовы API;
- **backend-error-`ггггммдд`.log**. Подключен по умолчанию. Содержит в себе сообщения ошибок уровня событий Error и выше;
- **backend-external-communication-`ггггммдд`.log**. Подключен по умолчанию. Содержит в себе все сообщения, относящиеся к коммуникации с внешними сервисами (например, etcd);
- **backend-db-requests-`ггггммдд`.log**. Подключается опционально (см. раздел «14.5.2 Настройки логирования запросов к базе данных»). Содержит в себе SQL запросы к базе данных;
- **auth-all-`ггггммдд`.log**. Подключен по умолчанию. Содержит в себе все сообщения ошибок по авторизации (общие логи сервера авторизации);
- **auth-all-error-`ггггммдд`.log**. Подключен по умолчанию. Содержит в себе все сообщения ошибок уровня событий Error (логи сервера авторизации);
- **auth-db-requests-ггггммдд.log**. Выключено по умолчанию. Подключается опционально (см. раздел «14.5.2 Настройки логирования запросов к базе данных»). Содержит запросы к базе данных от сервиса авторизации.
- **backend-startup-ггггммдд.log**. Подключен по умолчанию. Содержит в себе всю информацию по старту сервера приложений;
- **delphi-api-call-ггггммдд.log**. Подключен по умолчанию. Содержит информацию о том, что отправляется на сервер delphi и сколько это занимает времени.

В каждый файл логирования пишется полная информация о сервере приложений и о параметрах конфигурации.

---

Строки записей сообщений лога строятся по определённой схеме и разделяются пробелом:

- **время записи в формате «ЧЧ:ММ:СС.000»**. Пример – 16:00:58.001;
- **уровень события (в квадратных скобках)**. Пример – [INF];
- **сообщение лога**. Пример – Задача KeepAliveScheduledJob запущена;
- **контекст события (в угловых скобках)**. Пример – <Sms.ZRP.Application.ZVK.ScheduledJobs.KeepAliveScheduledJob>.

Уровни событий:

- **VER**. Отслеживание/отладка. Информации для разработчика для отслеживания и отладки;
- **DBG**. Отладочный. Информация для разработчиков об операциях, которые происходят в системе;
- **INF**. Информационный. Информирование об операциях в системе;
- **WAR**. Предупреждения. Важные операции в системе, которые могут влиять на работу пользователей;
- **ERR**. Ошибка. Отклонения, при которых возможно нормальное продолжение работы;
- **FAT**. Критическая ошибка. Ошибки, приводящие к полному отказу работы системы.

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.

После обновления Системы на версию 11R7 логирование включено по умолчанию с параметрами (подробнее в разделе «14.8 Описание параметров файла Serilogsettings.json»):

```
"rollingInterval": "Day",
"retainedFileCountLimit": null,
"rollOnFileSizeLimit": true,
"fileSizeLimitBytes": 104857600,
```

## 19.1 Известные ошибки ЗРП.Net

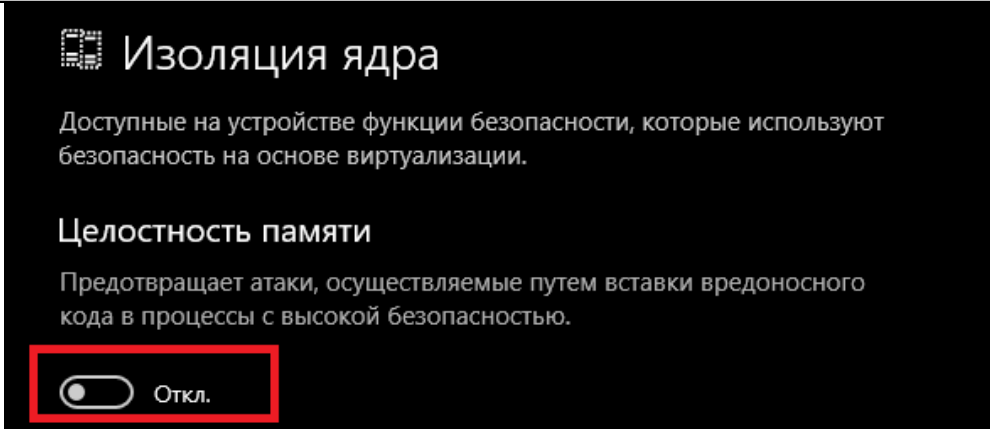
В этом разделе приведен список известных ошибок, которые не являются критичными и не приводят к проблемам в работе ЗРП.Net.

Список ошибок, которые встречаются в клиентской части приведен в таблице 2.

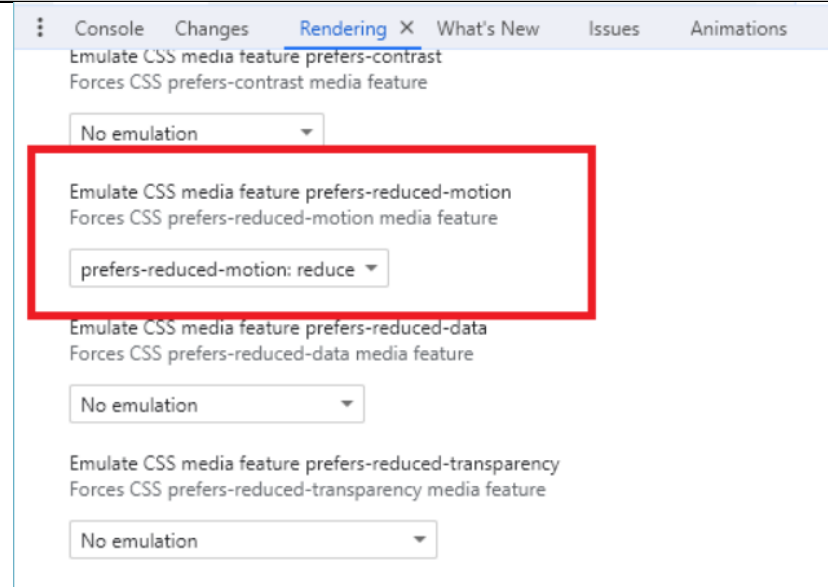
**Таблица 2 – Ошибки в клиентской части**

Ошибка	Описание
Адрес сервиса интеграции невалиден. Проверьте значение "IntegrationServiceUri": "http://it230405-0::8624/SOAP" в блоке "IntegrationServiceSettings" конфигурационного файла sms.ZRP.WebApi.settings.json	Данная ошибка возникает при записи неверного адреса сервиса интеграции в конфигурационном файле sms.ZRP.WebApi.settings.json. <b>Рекомендации:</b> при возникновении этой ошибки необходимо проверить правильность указанного адреса сервиса интеграции (см. раздел «14.5.4 Настройка доступа к серверу приложений Delphi_»)
Время открытия заявки больше текущего времени	Данная ошибка может возникнуть, если на клиенте время не синхронизировано с сервером. <b>Рекомендации:</b> для исправления данной ошибки необходимо синхронизировать время клиента в настройках операционной системы
Данная установка запрещена политикой, заданной системным администратором	Данная ошибка может возникнуть при установке ПК в ОС Windows. <b>Рекомендации:</b> проблема может быть в изоляции ядра, чтобы это исключить: 1. Перейти в Безопасность Windows

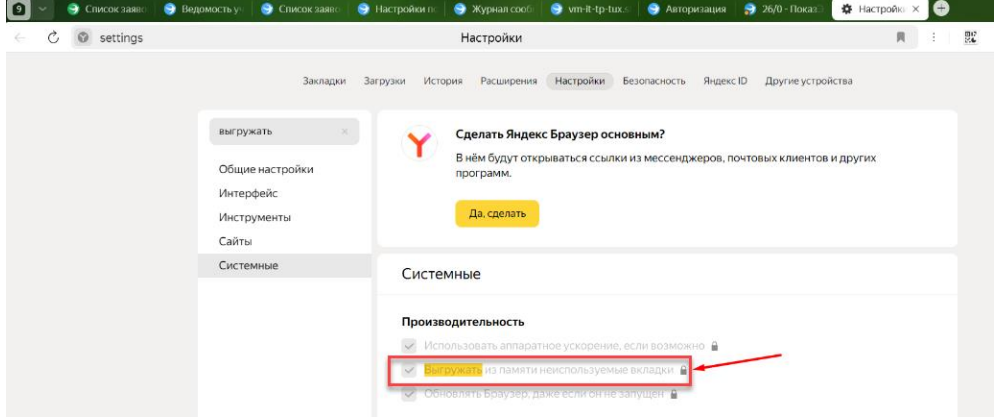
Ошибка	Описание
	Краткий обзор безопасности  Просмотрите сведения о состоянии безопасности и работоспособности устройства и выполните все необходимые действия.    Защита от вирусов и угроз  Облачная защита отключена. Устройство может быть уязвимым.  Включить  Закрыть    Защита учетных записей  Никаких действий не требуется.    Брандмауэр и безопасность сети  Брандмауэры отключены. Устройство может быть уязвимым.  Включить    Управление приложениями/браузером  Никаких действий не требуется.    Безопасность устройства  Просмотр состояния функций защиты оборудования и управление ими    Производительность и работоспособность устройств  Никаких действий не требуется.      2. Перейти в Безопасность устройства     Безопасность устройства  Защита, встроенная в устройство.   Изоляция ядра  Средство обеспечения безопасности на основе виртуализации позволяет защитить главные компоненты устройства.  Сведения об изоляции ядра   Стандартная безопасность оборудования не поддерживается.  <a href="#">Подробнее</a>     3. Сведения об изоляции ядра

Ошибка	Описание
	  <b>Изоляция ядра</b>   Доступные на устройстве функции безопасности, которые используют безопасность на основе виртуализации.   <b>Целостность памяти</b>   Предотвращает атаки, осуществляемые путем вставки вредоносного кода в процессы с высокой безопасностью.   <input type="checkbox"/> Откл.     4. Включить переключатель Целостность памяти
Дублирование уведомлений о новых заявках при обновлении версии	Дублирование уведомлений наблюдается только в процессе обновления версии Системы. После завершения обновления уведомления приходят штатно – по одному на событие.   <b>Рекомендации:</b> при необходимости отключать уведомления на время обновления Системы. Игнорировать дубли во время обновления. Не предпринимать действий по двойной обработке заявки.
Невозможно заблокировать заявку. Заявка заблокирована пользователем	Данная ошибка может возникнуть если в момент отправки запроса на автоматический сброс блокировки по таймеру произошел разрыв соединения с сервером приложений. После восстановления соединения отправляется запрос на уточнение статуса блокировки заявки.   <b>Рекомендации:</b> если в момент отправки запроса на автоматический сброс блокировки по таймеру произошел разрыв соединения с сервером приложений, то после восстановления соединения отправляется запрос на уточнение статуса блокировки заявки. Если заявка останется заблокированной, но по вкладке уже будет выгружена информация браузером, то сбросить блокировку можно будет только в разделе «Блокировки» в Интерфейсе администратора. Если информация по вкладке на момент восстановления соединения и продолжения

Ошибка	Описание
	работы пользователя на данной вкладке не будет выгружена, то пользователь сможет продолжить работу с заблокированной заявкой
Не работает авторизация в ЗРП.Net, в логах присутствует ошибка:  [ERR] Ошибка при валидации логина и пароля через Kerberos  (0c7aa48e-693c-4519-9f8f-af2abd981489)  System.Security.SecurityException: Invalid Checksum	Данная ошибка может возникнуть при внесении изменений в учетную запись, для которой генерировался keytab-файл (например, изменился пароль).  <b>Рекомендации:</b> при возникновении этой ошибки необходимо заново создать keytab-файл
Некорректное отображение текста примечаний/подписей в отчетах «Форма для печати по умолчанию» и «Полная форма заявки с ОВР» при экспорте отчета в Word	Данная ошибка может возникнуть при экспорте отчета, если текст в поле «Куда» длиннее 16 символов и в нем нет пробелов, то ячейка с текстом не увеличивается в высоту. Поэтому в отчетах «Форма для печати по умолчанию» и «Полная форма заявки с ОВР» возможно автоматическое добавление пустой строки
Не крутится прогресс-бар загрузки отчета пользователя при нажатии кнопки «Просмотр» на странице отчета	Данная ошибка может возникнуть, если в Windows установлен режим уменьшенной анимации или если подключение было с удаленного рабочего стола.  <b>Рекомендации:</b> при возникновении этой ошибки необходимо проверить настройку, обозначенную на рисунке ниже:

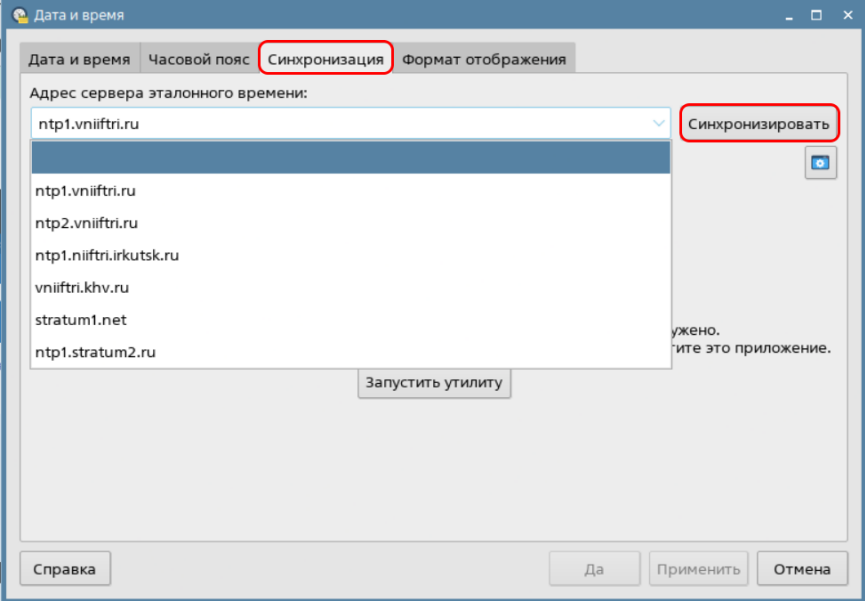
Ошибка	Описание
	
Не найден элемент с ID={id группы}	Данная ошибка возникает при редактировании в ЗРП.Delphi группы заявок, созданной в ЗРП.Net. В ЗРП.Net нельзя редактировать имя группы заявок, созданной в ЗРП.Delphi, если не включен компонент etcd
Не обновляется информация в веб-интерфейсе при удалении функциональной зависимости в Интерфейсе администратора	При создании новой заявки через веб-интерфейс Система может некорректно отображать список доступных значений или выдавать ошибки, связанные с устаревшими данными. Это происходит, если функциональная зависимость удалена в Интерфейсе администратора, но информация о её существовании продолжает влиять на работу веб-клиента.   <b>Рекомендации:</b> необходимо войти в Интерфейс администратора и повторно удалить функциональную зависимость.   В крайнем случае, необходимо перезапустить сервер приложений

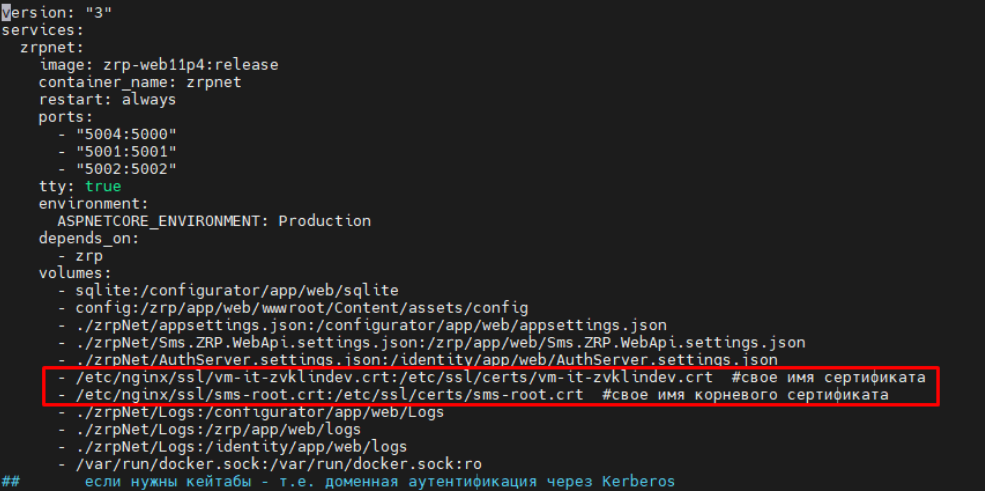


Ошибка	Описание
После редактирования заявки и закрытия вкладки/браузера, при повторном входе в Систему некоторое время сохраняется сообщение о том, что заявка заблокирована другим пользователем	   Данная ошибка связана с настройками конкретного браузера пользователя. Механизм снятия блокировки срабатывает в момент корректного завершения сессии (закрытие вкладки). Однако браузер может быть настроен на полную очистку данных при завершении работы.   Проблема возникает в двух сценариях:      1. Аварийное завершение работы: Если браузер был закрыт некорректно, скрипт снятия блокировки не успевает выполниться. При этом сессия на сервере остается активной, поэтому Система считает, что заявка по-прежнему открыта.    2. Настройки конфиденциальности браузера: В браузере пользователя может быть включена функция автоматического удаления кеша при закрытии.    • Пример для браузера: В настройках конфиденциальности активирована опция «Удалять данные при закрытии браузера» (или аналогичная), в частности — пункт «Файлы, сохранённые в кеше». Это приводит к потере контекста сессии, хотя сама сессия на сервере продолжает существовать до истечения таймута.          <b>Рекомендации:</b> старайтесь закрывать вкладки или окно браузера стандартным способом (нажатием на крестик). Избегайте завершения работы браузера через

Ошибка	Описание
	Диспетчер задач или выключения компьютера с открытыми страницами Системы.   Если проблема возникает регулярно, проверьте настройки конфиденциальности вашего браузера. Убедитесь, что отключена опция автоматической очистки кеша или файлов cookie при закрытии браузера. Рекомендуется добавить адрес Системы в исключения, если браузер позволяет хранить данные для отдельных сайтов.   Для этого нужно:       1. Нажать → Настройки → Конфиденциальность → Удалять данные при закрытии браузера.     2. Нажать → Выбрать данные для удаления и выбрать опцию «Файлы, сохранённые в кеше»
Проблема с подключением к веб-интерфейсу после работ с DNS-сервером	<b>Рекомендации:</b> при возникновении этой ошибки необходимо сделать настройку reverse DNS lookup
Продление заявки недоступно. У текущего пользователя установлены ограничения по созданию заявки на оборудование объектов	Данная ошибка возникает при открытии формы продления заявки.   <b>Рекомендации:</b> при возникновении этой ошибки необходимо обновить страницу «Доступ к системе ограничен»
Сервис интеграции недоступен: Подключение не установлено, так как конечный компьютер отверг запрос на подключение	Данная ошибка означает, что сервер ЗРП.Delphi не отвечает.   <b>Рекомендации:</b> при возникновении этой ошибки необходимо проверить работу сервера приложений ЗРП.Delphi, его доступность
Смена пароля недоступна при NT аутентификации или при отключенном функционале смены пароля	Данная ошибка возникает при отсутствии параметра ChangePassword в конфигурационном файле authServer.settings.json.   <b>Рекомендации:</b> при возникновении этой ошибки необходимо в конфигурационный файл authServer.settings.json добавить параметр ChangePassword со значением true (подробное описание см. в разделе «14.6.6 Настройки менеджера дополнительно подключаемых функций»)

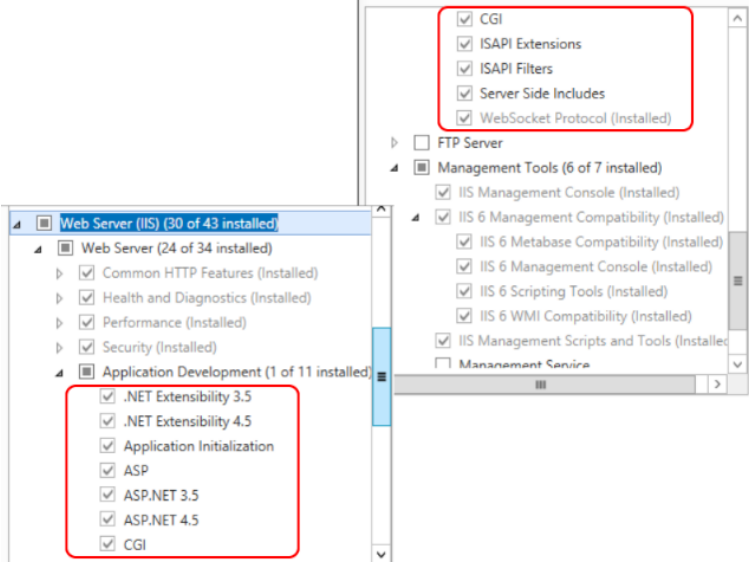
Ошибка	Описание
У пользователя установлены ограничения на администрирование предприятий-абонентов	Данная ошибка возникает у всех пользователей-абонентов без права «Администратор комплекса».   <b>Рекомендации:</b> при возникновении этой ошибки необходимо обновить страницу
Cannot read properties of null (reading 'length')	Данная ошибка может возникнуть при открытии заявок с NT авторизацией в браузере в котором уже открывали другой экземпляр заявок.   <b>Рекомендации:</b> при возникновении этой ошибки необходимо очистить localStorage
ERROR QuotaExceededError: Failed to execute 'setItem' on 'Storage': Setting the value of 'oidc.7609d706b7c1402d9914d24fe10026b4' exceeded the quota	Данная ошибка может возникнуть при открытии заявок с NT авторизацией в браузере в котором уже открывали другой экземпляр заявок.   <b>Рекомендации:</b> при возникновении этой ошибки необходимо очистить localStorage
Error handling response: TypeError: Cannot read properties of undefined (reading 'matched') и Unchecked runtime.lastError: The message port closed before a response was received	Данная ошибка возникает при редактировании полей ввода, при создании заявки за чужое предприятие, если в браузере пользователя установлено расширение Monosnap
Error: iat is in the future: 1692027041	Данная ошибка может возникнуть при изменении времени на сервере или на клиенте так, чтобы время не соответствовало времени в часовом поясе, указанном в настройках.   <b>Рекомендации:</b> для исправления и профилактики ошибки необходимо в настройках Astra на вкладке «Синхронизация» указать сервер синхронизации и нажать на кнопку «Синхронизировать»

Ошибка	Описание
	
Extension context invalidated	Данная ошибка возникает при открытии сообщения из Журнала сообщений или ФОЗ после отключения расширения «Помощник ЗРП.Net» без последующей перезагрузки страницы.   <b>Рекомендации:</b> для исправления этой ошибки необходимо после отключения расширения «Помощник ЗРП.Net» выполнить полную перезагрузку страницы браузера
HTTP error: status code 404, net:ERR_HTTP_RESPONSE_CODE_FAILURE	Данная ошибка возникает при отсутствии возможности авторизации в ЗРП.Net.   <b>Рекомендации:</b> для исправления этой ошибки необходимо сбросить все настройки браузера
JWT token validation error: IDX10501: Signature validation failed. Unable to match key:	Данная ошибка возникает в течении часа после переключения узлов кластера и не влияет на работоспособность

Ошибка	Описание
[ERR] An exception was thrown while deserializing the token.(3d639fec-ea6b-4874-bae5-f33a8718f1f7) &lt;Microsoft.AspNetCore.Antiforgery.DefaultAntiforgery&gt;   Microsoft.AspNetCore.Antiforgery.AntiforgeryValidationException: The antiforgery token could not be decrypted.   ---&gt; System.Security.Cryptography.CryptographicException: The key {774f8eb3-e9a0-4728-91a8-4b5fd0e5147e} was not found in the key ring. For more information go to <a href="http://aka.ms/dataprotectionwarning">http://aka.ms/dataprotectionwarning</a>   at Microsoft.AspNetCore.DataProtection.KeyManagement.KeyRingBasedDataProtector.UnprotectCore(Byte[] protectedData, Boolean allowOperationsOnRevokedKeys, UnprotectStatus&amp; status)   at Microsoft.AspNetCore.DataProtection.KeyManagement.KeyRingBasedDataProtector.Unprotect(Byte[] protectedData)   at Microsoft.AspNetCore.Antiforgery.DefaultAntiforgeryTokenSerializer.Deserialize(String serializedToken)   --- End of inner exception stack trace ---   at Microsoft.AspNetCore.Antiforgery.DefaultAntiforgeryTokenSerializer.Deserialize(String serializedToken)   at Microsoft.AspNetCore.Antiforgery.DefaultAntiforgery.GetCookieTokenDoesNotThrow(HttpContext httpContext)	Данная ошибка возникает при отсутствии корневого сертификата.   <b>Рекомендации:</b> для исправления этой ошибки необходимо наличие корневого сертификата    Также данная ошибка может возникать при обновлении ЗРП.Net.   <b>Рекомендация:</b> для исправления этой ошибки необходимо рестартовать оба контейнера, спустя примерно 30 секунд после обновления
405 Method Not Allowed	Данная ошибка возникает в ходе запуска ЗРП.Net.   <b>Рекомендации:</b> для исправления этой ошибки необходимо отключить модуль WebDAV Publishing для сайтов ЗРП, для этого нужно открыть для редактирования файл web.config из директории установки ЗРП, как правило это

Ошибка	Описание
	c:\Program Files\ZVK\имя_экземпляра\ZRP.NET\ и в секции &lt;modules&gt; прописать секцию&lt;system.webServer&gt;. Добавить секции:   &lt;handlers&gt;   &lt;remove name="WebDAV"/&gt;   &lt;/handlers&gt;   &lt;modules&gt;   &lt;remove name="WebDAVModule"/&gt;   &lt;/modules&gt;  <pre>&lt;?xml version="1.0" encoding="utf-8"?&gt; &lt;configuration&gt;   &lt;location path="." inheritInChildApplications="false"&gt;     &lt;system.webServer&gt;       &lt;handlers&gt;         &lt;remove name="WebDAV" /&gt;         &lt;add name="aspNetCore" path="*" verb="*" modules="AspNetCoreModuleV2" resourceType="Unspecified" /&gt;       &lt;/handlers&gt;       &lt;aspNetCore processPath=".\\SmS.ZRP.WebApi.exe" stdoutLogEnabled="false" stdoutLogFile=".\logs\stdout" hostingModel="inprocess" /&gt;     &lt;/system.webServer&gt;   &lt;/location&gt;   &lt;system.webServer&gt;     &lt;security&gt;       &lt;authentication&gt;         &lt;anonymousAuthentication enabled="true" userName="IUSR" /&gt;         &lt;windowsAuthentication enabled="false" /&gt;       &lt;/authentication&gt;     &lt;/security&gt;     &lt;modules&gt;       &lt;remove name="WebDAVModule" /&gt;     &lt;/modules&gt;   &lt;/system.webServer&gt; &lt;/configuration&gt;</pre>  Или воспользоваться оснасткой IIS и отключить данный модуль вручную в разделе «Модули»



Ошибка	Описание
	IP-адрес &lt;внешнее имя сервера&gt;   – в исключения прокси добавить внешний адрес сервера
405 – HTTP verb used to access this page is not allowed	Данная ошибка возникает при сохранении заявки после подписи за любого пользователя.   <b>Рекомендации:</b> для исправления этой ошибки необходимо включить все компоненты Windows из службы IIS (за исключением «публикации WebDAV») обозначенные на рисунке:    The screenshot shows the 'Windows Features' window. The 'Web Server (IIS)' section is expanded, showing sub-sections like 'Common HTTP Features', 'Health and Diagnostics', 'Performance', 'Security', and 'Application Development'. The 'Application Development' section is further expanded, showing 'ASP', 'ASP.NET 3.5', 'ASP.NET 4.5', and 'CGI'. Two red boxes highlight the 'Web Server (IIS)' section and the 'Application Development' section, both of which are fully installed.
<pre>{ "StackTrace": null, "Status": 500, "ErrorCode": 1, "Detail": "Sequence contains no matching element", "Instance": "/api/vl/zvk/33", "ExceptionType": "InvalidOperationException" }</pre>	<b>Рекомендации:</b> необходимо обратиться в службу поддержки СМС-ИТ за скриптом
[Deprecation] Listener added for a 'DOMNodeInserted' mutation event. Support for this event type has been removed, and this event will no longer	Данная ошибка возникает в консоли разработчика при переходе на страницу веб-заявок.

Ошибка	Описание
be fired. See <a href="https://chromestatus.com/feature/5083947249172480">https://chromestatus.com/feature/5083947249172480</a> for more information.  template @ notification-panel.component.html:51	<b>Рекомендации:</b> пользователю ЗРП.Net данную ошибку обрабатывать не требуется, так как ошибка не является критичной и не приводит к проблемам в работе ЗРП.Net

Список ошибок, которые встречаются в логах сервера приложения ЗРП.Net приведен в таблице 3.

**Таблица 3 – Ошибки в логах сервера приложения ЗРП.Net**

Ошибка	Описание
Exception while reading from stream  ---> System.IO.EndOfStreamException: Attempted to read past the end of the stream	Ошибка связана с закрытием неактивных соединений службой haproxy. Со стороны ЗРП.Net связываемся через открытое соединение для синхронизации информации с заявками. При разрыве соединения с внешней стороны (службой haproxy) в логах фиксируется данная ошибка. После этого происходит восстановление соединения с ЗРП.Net.  <b>Рекомендации:</b> пользователю ЗРП.Net данную ошибку обрабатывать не требуется, так как ошибка не является критичной и не приводит к проблемам в работе ЗРП.Net
Ошибка обработки команды GetZvkFilterQuery: Query was cancelled [172.16.72.191] (90d24436-88bf-4fb7-8010-89bb3f4e2c90) <Sms.ZRP.Application.Abstractions.Behaviors.LoggingBehavior>  System.OperationCanceledException: Query was cancelled  ---> Npgsql.PostgresException (0x80004005): 57014: выполнение оператора отменено по запросу пользователя	Ошибка может быть связана из-за остановки загрузки страницы.  <b>Рекомендации:</b> пользователю ЗРП.Net данную ошибку обрабатывать не требуется, так как ошибка не является критичной и не приводит к проблемам в работе ЗРП.Net
Ошибка обработки команды AddSynchronizationMessageCommand {"SignalIdent":"PingMsgEvents","Body":{"MessageGUID":"{ACFB8C0D-4AD7-41F5-917D-024B148A35C0}"},"PublisherGUID":"{B299E8E9-709E-4CE7-BF99-AB7712F26745}"},"Timestamp":"2025-05-05T21:00:00.57327Z"},"\$type":"AddSynchronizationMessageCommand"}	<b>Рекомендации:</b> пользователю ЗРП.Net данную ошибку обрабатывать не требуется, так как ошибка не является критичной и не приводит к проблемам в работе ЗРП.Net

Ошибка	Описание
System.NullReferenceException: Object reference not set to an instance of an object.	



---

## 20 Рекомендации для администраторов

### 20.1 Рекомендации по обслуживанию сервера

При проведении регламентных работ на серверах Системы рекомендуется учитывать следующий период перезагрузки серверов – 1 раз в 2 недели.

После перезагрузки необходимо выполнить проверку состояний сервисов:

- системного ПО: веб-сервера Nginx, СУБД Postgres и службы Docker.
- прикладного ПО: проверить работоспособность интерфейсов.

Для штатной остановки комплекса при проведении работ рекомендуется использовать скрипт `serverstop.sh` (подробнее в разделе «20.3 Рекомендации по штатному останову серверов приложений»).

### 20.2 Рекомендации по настройке мониторинга docker в Zabbix

Перед импортом шаблона мониторинга docker необходимо выполнить следующие действия для корректной работы сокетa docker:

1. Добавить пользователя Zabbix в группу docker:  
`sudo usermod -aG docker zabbix`
2. Перезапустить zabbix-agent2:  
`sudo systemctl restart zabbix-agent2`
3. Импорт шаблона мониторинга docker в Zabbix
  - Загрузка шаблона в Систему:
    - в веб-интерфейсе Zabbix перейти в раздел «Сбор данных» → «Шаблоны»;
    - Нажать кнопку «Импорт»;
    - Загрузить файл шаблона `template_app_docker.yaml`.
  - Привязка шаблона к узлу сети:
    - Перейти в раздел «Узлы сети»;
    - Выбрать хост, на котором требуется мониторинг docker;
    - Во вкладке «Шаблоны» нажать «Выбрать»;
    - Найти в списке шаблон «Docker by Zabbix agent 2» и добавить его.
    - Нажать «Обновить» для сохранения изменений.
4. Проверка работы мониторинга. После выполнения описанных шагов убедиться, что Zabbix Agent 2 запущен:  
`sudo systemctl status zabbix-agent2`

---

При выявлении значительного увеличения размера каталога docker (в частности, в подкаталоге overlay2) рекомендуется использовать скрипт очистки излишних слоев (см. Приложение 3. Скрипт для мониторинга размера каталога docker) или выполнить следующие шаги:

**1. Проверка использования пространства docker.**

Выполнить команду для просмотра детальной информации о слоях, томах и образах:  
`docker system df -v`

Результат: обратить внимание на большое количество неиспользуемых томов (Volumes).

**2. Анализ занятого места в каталоге overlay2:**

`sudo du -h --max-depth=1 /var/lib/docker/overlay2 | sort -hr | head -20`

Эта команда покажет 20 самых «тяжёлых» подкаталогов overlay2.

**3. Очистка неиспользуемых томов и данных docker:**

- **Полная очистка** (включая неиспользуемые тома и образы):

`docker system prune -a --volumes`

**Внимание:** на неактивном узле, где нет запущенных контейнеров, эта команда удаляет весь локальный репозиторий образов. После этого образы потребуются загружать заново.

- **Частичная очистка** (только неиспользуемые тома, без образов):

В случаях, когда удаление всех неиспользуемых объектов (-a) недопустимо по условиям эксплуатации (например, на узлах, где требуется сохранность локального кэша образов), рекомендуется использовать команду:

`docker system prune --volumes`

Данная команда выполняет следующие действия:

- удаляет неиспользуемые тома (тома, не связанные ни с одним из существующих контейнеров);
- не удаляет используемые тома;
- не удаляет образы (как используемые, так и неиспользуемые);
- не удаляет остановленные контейнеры и сети (если не указаны дополнительные флаги).

Следует учитывать, что при таком подходе может быть освобождено меньше дискового пространства по сравнению с полной очисткой, так как образы и кэшированные слои не подлежат удалению. Тем не менее, данный метод является более безопасным для сред, где не допускается повторная загрузка образов из реестра.

---

#### 4. Повторная проверка места.

После очистки снова выполнить:

```
sudo du -h --max-depth=1 /var/lib/docker/overlay2 | sort -hr | head -20
```

#### 5. Настройка порога срабатывания

При превышении X% заполнения каталога overlay2 (где X — переменная величина, задаваемая пользователем) необходимо выполнить одну из рекомендаций по очистке, указанных в п. 3.

Пример: если задано значение X=75%, то при заполнении более 75% следует запускать `docker system prune --volumes` (или полную версию, если допустимо удаление образов).

### **Рекомендации по версиям docker и docker compose**

При использовании старых версий docker и docker compose могут возникать проблемы с корректным удалением томов (volumes):

- **Проблемная конфигурация:**

Docker compose версии 1.x в связке со старым docker engine не всегда корректно обрабатывает удаление томов.

Пример проблемной версии: docker server engine 24.0.2 + docker compose 1.29.2.

- **Решение:**

Для избежания проблем с томами в дальнейшем требуется обновить версии docker и docker compose до актуальных. После обновления docker и перехода на docker compose v2 проблема удаления томов устраняется.

- **Рекомендуемые действия:**

Обновить docker engine до актуальной стабильной версии.

Перейти на docker compose v2 (встроенный в docker CLI или устанавливаемый отдельно).

Проверить работу команд очистки (`docker system prune --volumes`) на обновлённой версии.

## **20.3 Рекомендации по штатному останову серверов приложений**

При выполнении регламентных работ по перезапуску серверов, а также при выполнении обновлений Системы для штатной остановки Системы и веб-версии Системы рекомендуем применять скрипт `serverstop.sh` (см. Приложение 2. Скрипт для штатного останова серверов приложений ).

Применение скрипта:

- Скопировать скрипт `serverstop.sh` на сервер.
- Командой `sudo chmod +x serverstop.sh` сделать скрипт исполняемым.
- Командой `./serverstop.sh` выполнить скрипт в терминале из директории его нахождения.

## 20.4 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 20.1).

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/nginx_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 20.1 – Увеличение параметра «client\_max\_body\_size»

---

## 20.5 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 файлам, чтобы не возникало проблем в работе Системы 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 nfile 1048576
```

```
* hard nfile 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 Delphi на одном уровне с блоком `image` добавить блок вида (Рисунок 20.2):

*ulimits:*

*nfile:*

*soft: 1048576*

*hard: 10485760*

```
zvk:
 image: asu:v9sd7_release
 container_name: asureo
 ulimits:
 nofile:
 soft: 1048576
 hard: 10485760
 restart: always
 network_mode: "host"
```

Рисунок 20.2 – Пример добавления параметров в docker-compose

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 указать либо равные системным лимитам, либо меньше.

## 20.6 Рекомендации по работе с Dr.Web

При эксплуатации АСУРЭО в среде с установленным антивирусным программным обеспечением Dr.Web (Антивирус Dr.Web) выявлены особенности взаимодействия, связанные с работой компонента SpiDer Gate.

### 1. Режим работы при отключенном SpiDer Gate.

При отключенном компоненте SpiDer Gate (веб-антивируса) функционирование АСУРЭО осуществляется в штатном режиме. Все процессы обмена данными, включая взаимодействие с серверными компонентами и внешними подсистемами, выполняются корректно без возникновения ошибок подключения или таймаутов.

### 2. Режим работы при включенном SpiDer Gate.

При включенном компоненте SpiDer Gate в работе АСУРЭО наблюдаются сбои при обмене данными по протоколу SOAP.

Характер проявления проблемы:

- Нарушение передачи запросов и ответов между клиентской частью и сервером приложений.
- Логи АСУРЭО фиксируют ошибки соединения, таймауты или невозможность установить связь с сервисами, использующими SOAP-интерфейсы.

- 
- Возможна потеря функциональности модулей, отвечающих за интеграцию и обмен структурированными данными.

**Рекомендация:**

Для обеспечения бесперебойной и корректной работы АСУРЭО в среде с Dr.Web необходимо отключить компонент SpiDer Gate.

## **20.7 Рекомендации по обновлению PostgreSQL версии 12 до 15**

Обновлении версии PostgreSQL необходимо производить только после обновления Системы до версии не ниже 10.20.35.XX.XX, так как версии ниже не работают с версией PostgreSQL15.

## **20.8 Рекомендации о периодическом ребилдинге индексов в базе ПК**

### **20.8.1 Ребилдинг индексов в SQL Server**

В процессе работы Системы 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 20.3).



1. Для запуска мастера создания плана обслуживания надо в контекстном меню Планы обслуживания (Maintenance Plan) выбрать *Мастер планов обслуживания (Maintenance Plan Wizard)* (Рисунок 20.5).

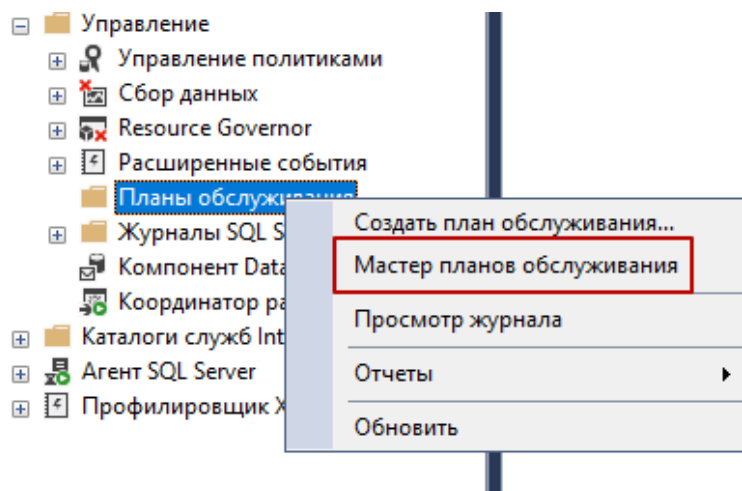


Рисунок 20.5 – Запуск мастера создания плана обслуживания

2. При запуске мастера сначала появится стартовая страница с описанием мастера (Рисунок 20.6).

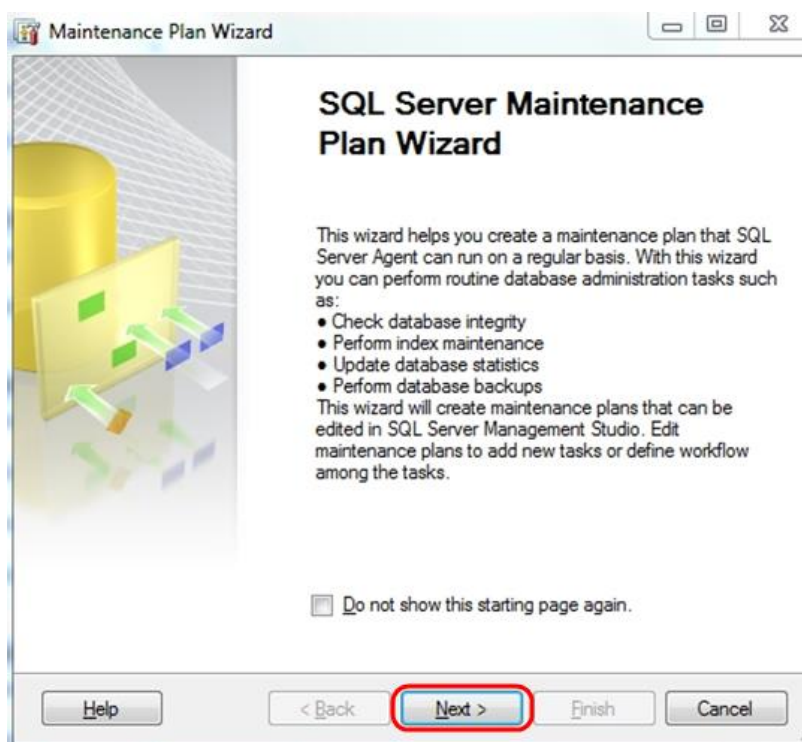


Рисунок 20.6 – Стартовая страница «Мастер планов обслуживания (Maintenance Plan Wizard)»

3. Далее необходимо задать имя и описание плана обслуживания (Рисунок 20.7).

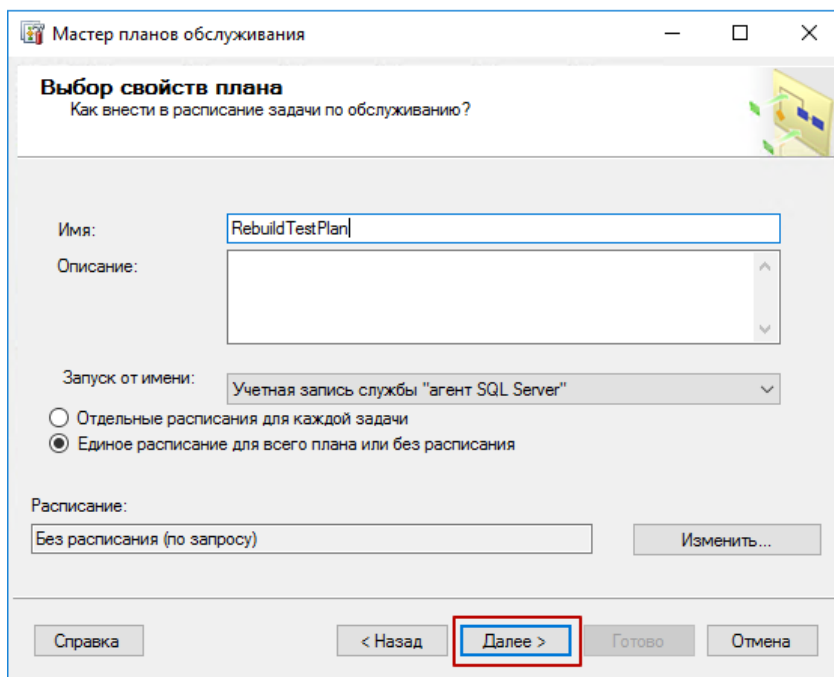


Рисунок 20.7 – Задание имени плана обслуживания

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 20.8).

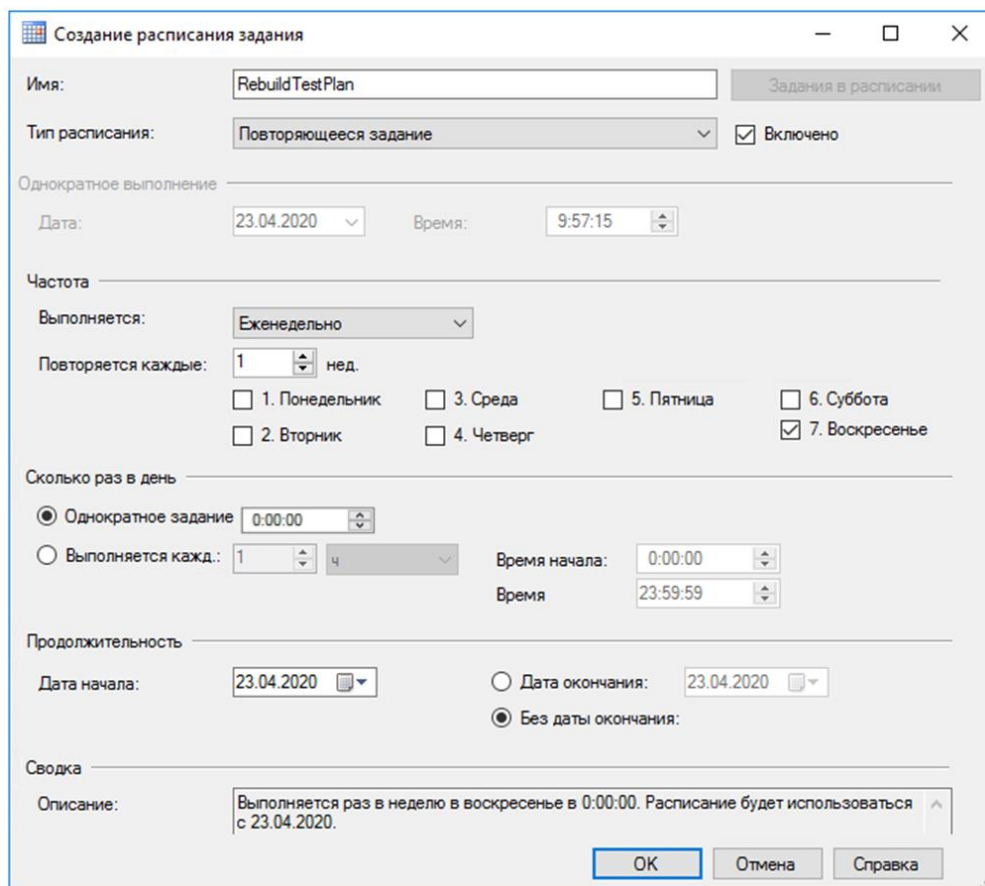


Рисунок 20.8 – Выбор расписания

5. После задания имени и времени выполнения плана обслуживания надо выбрать вид проводимых работ. В данном случае будет произведено пересоздание всех индексов (Рисунок 20.9).

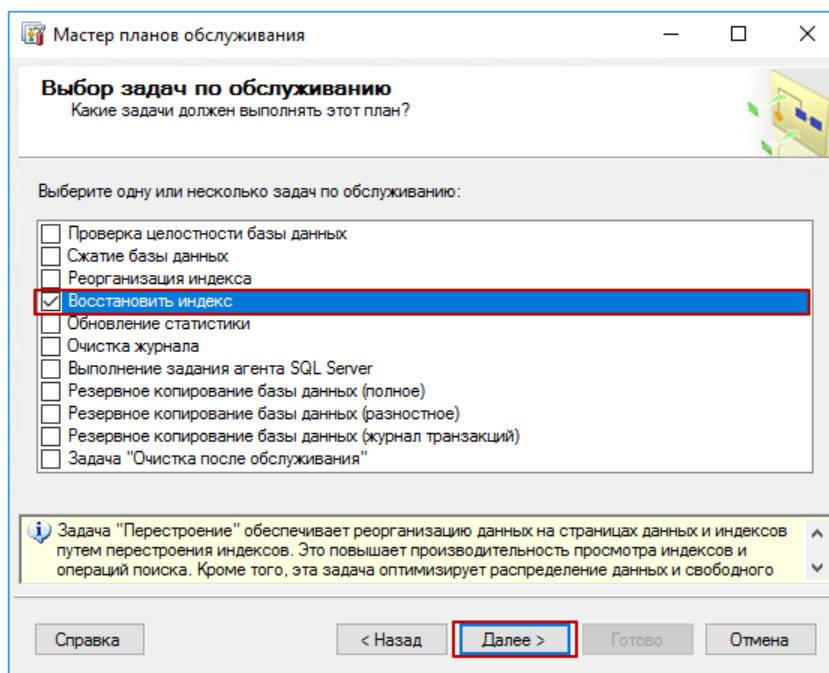


Рисунок 20.9 – Выбор опции «Восстановить индекс (Rebuild Index)»

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 20.10).

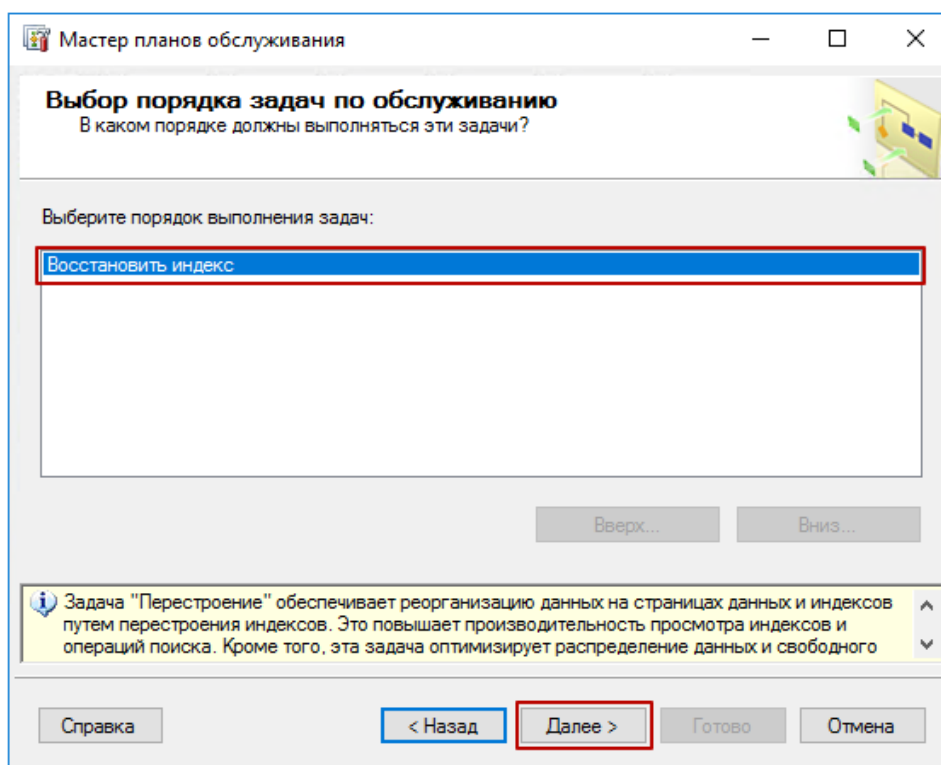


Рисунок 20.10 – Выбор порядка выполнения задач

7. После выбора порядка выполнения задач надо выбрать БД, к которым данный план обслуживания будет применяться (Рисунок 20.11).

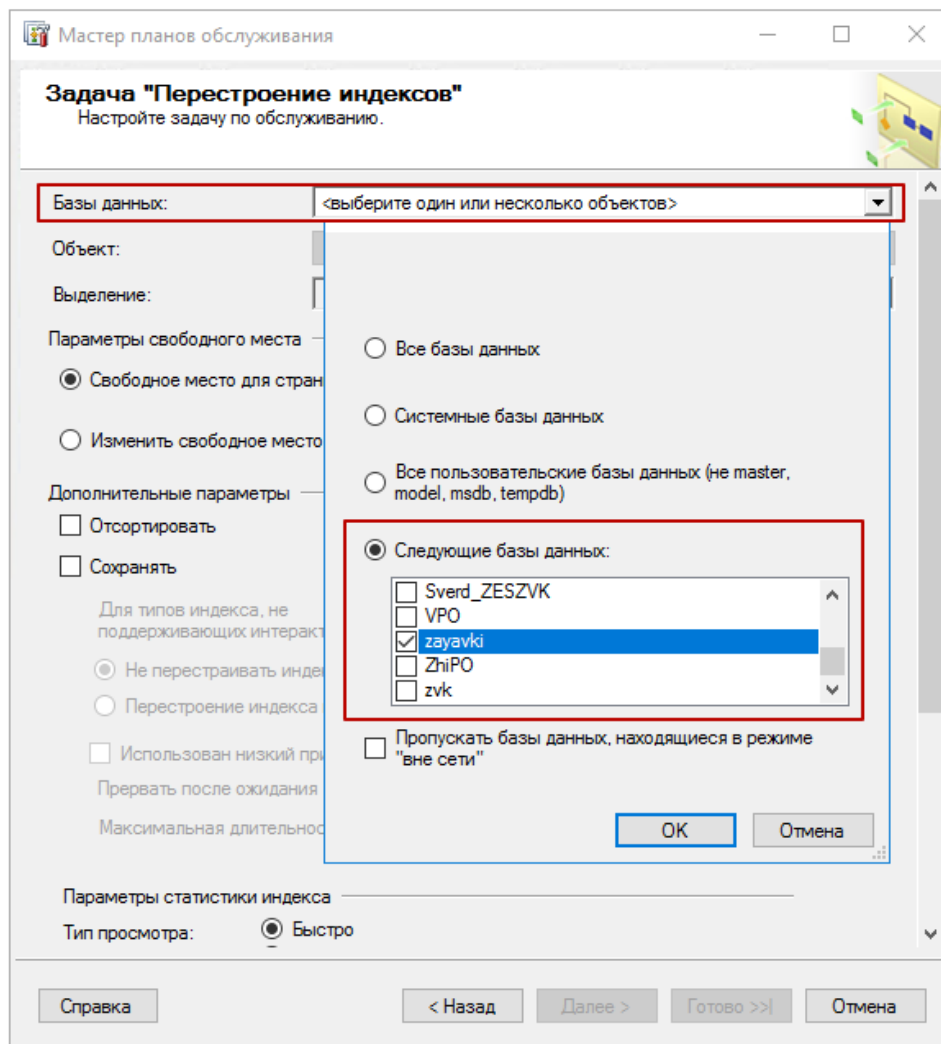


Рисунок 20.11 – Выбор БД

8. На следующем этапе надо выбрать папку, куда будет писаться лог выполнения работ (Рисунок 20.12).

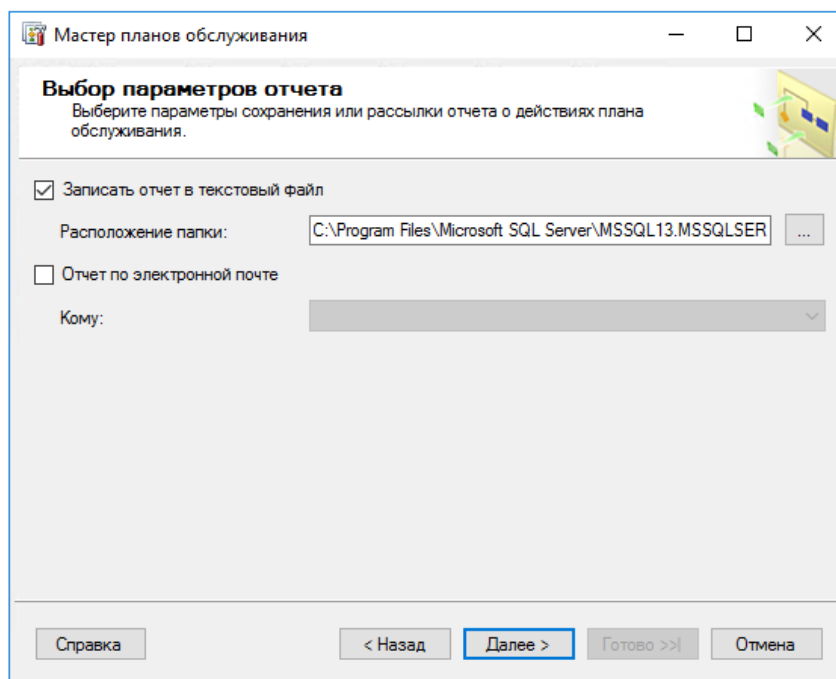


Рисунок 20.12 – Выбор папки, куда будет писаться лог выполнения работ

9. После прохождения всех этапов мастера будет выведено резюме о созданном плане обслуживания (Рисунок 20.13).

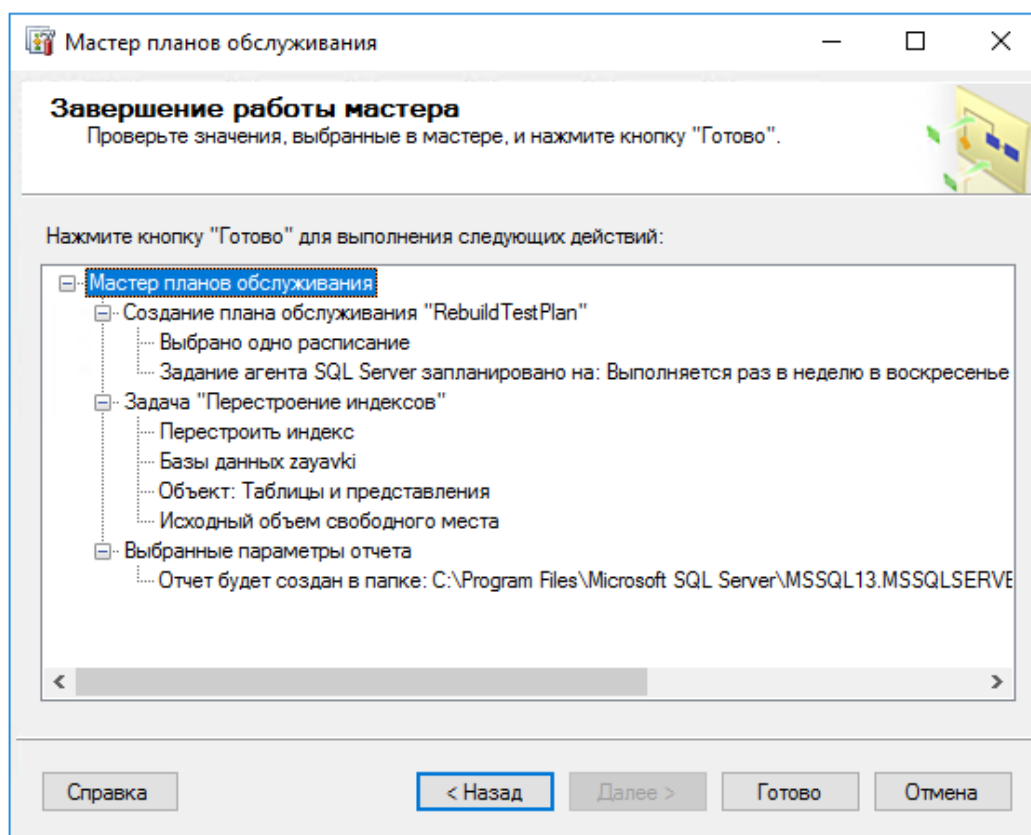


Рисунок 20.13 – Резюме о созданном плане обслуживания

10. После нажатия кнопки «Готово» (*Finish*) будет выведен отчет о создании плана обслуживания (Рисунок 20.14).

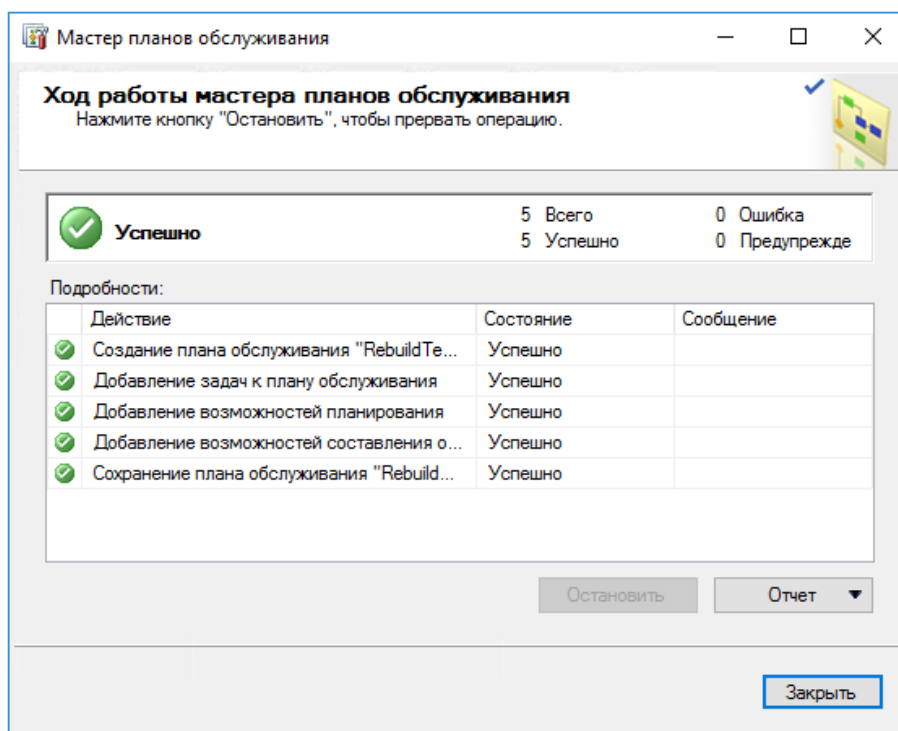


Рисунок 20.14 – Отчет о создании плана обслуживания

После создания плана обслуживания его можно вручную запустить на выполнение. По результатам будет выведено сообщение, в котором будет описан результат выполнения. На рисунке 20.15 приведен пример успешного выполнения плана обслуживания.

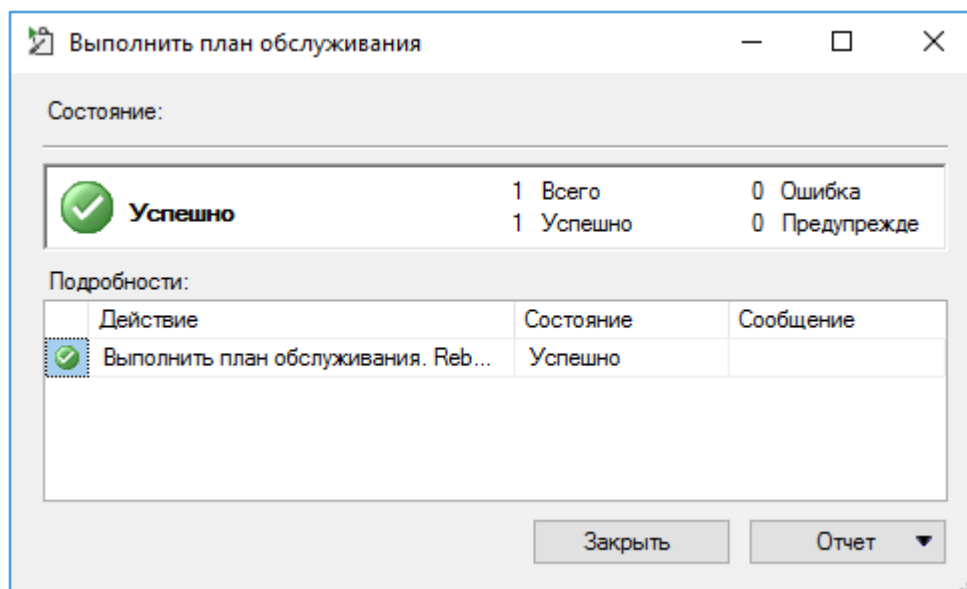


Рисунок 20.15 – Сообщение о результате выполнения плана обслуживания

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 20.16).

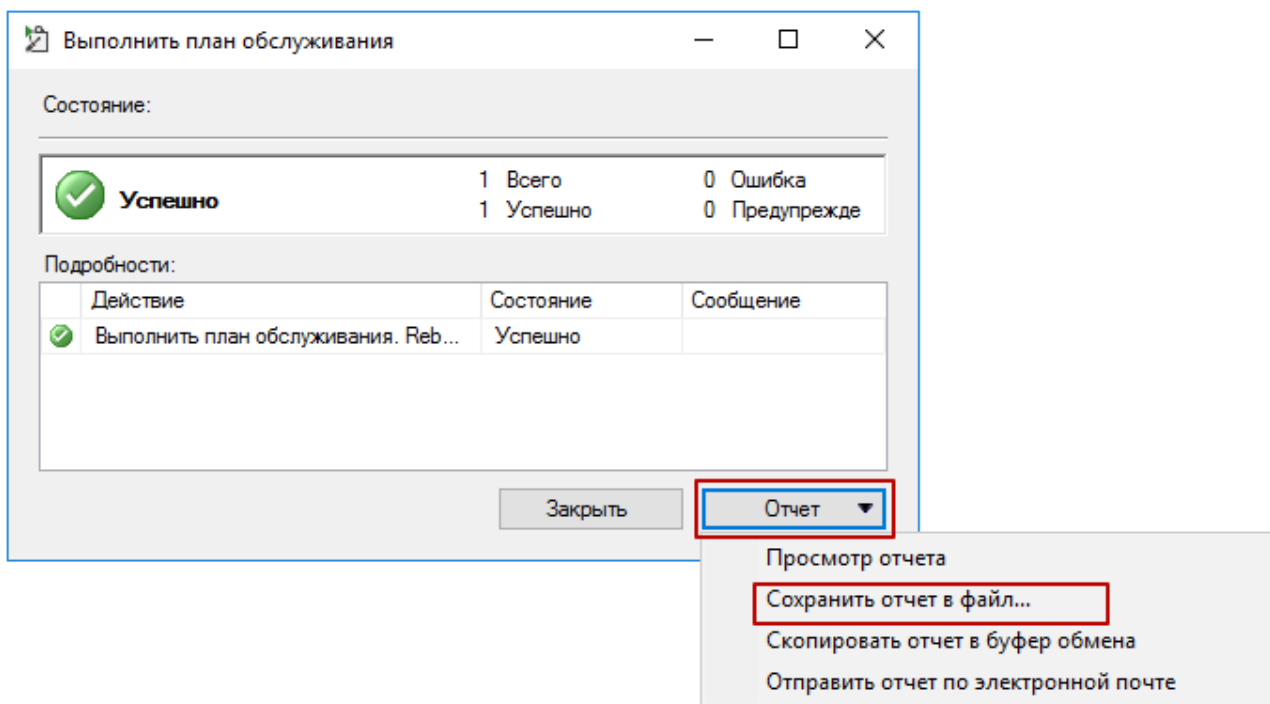


Рисунок 20.16 – Вызов отчета о выполнении плана обслуживания

На рисунке 20.17 представлен пример отчета о выполнении плана.

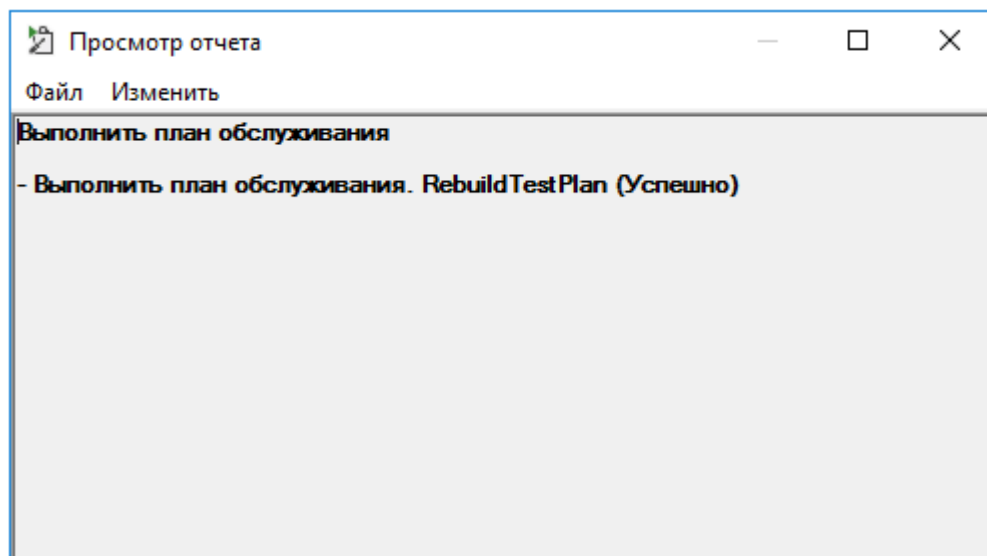


Рисунок 20.17 – Пример отчета о выполнении плана

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.

---

## 20.8.2 Ребилдинг индексов в PostgreSQL

В процессе работы Системы в БД PostgreSQL происходит фрагментация индексов, что замедляет работу БД. Данное замедление сказывается на производительности ПК. Рекомендуем выполнить настройку периодического index rebuild в БД.

Для периодического index rebuild в БД PostgreSQL необходимо выполнить следующие действия:

1. Авторизоваться на сервере с помощью RDP или ssh.

2. Авторизоваться под пользователем root: su -

3. Выполнить команду: *sudo crontab -e*

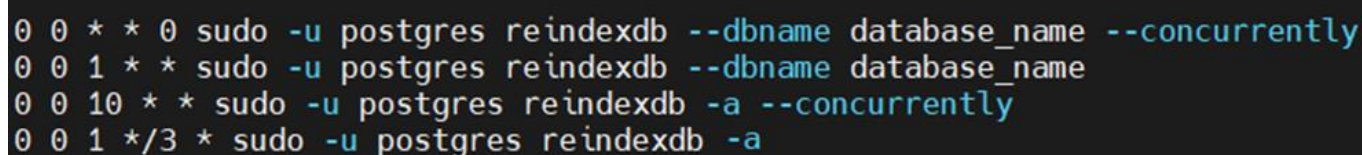
4. Прописать следующие строки в конце файла (Рисунок 20.18):

```
0 0 * * 0 sudo -u postgres reindexdb --dbname database_name --concurrently
```

```
0 0 1 * * sudo -u postgres reindexdb --dbname database_name
```

```
0 0 10 * * sudo -u postgres reindexdb -a --concurrently
```

```
0 0 1 */3 * sudo -u postgres reindexdb -a
```



```
0 0 * * 0 sudo -u postgres reindexdb --dbname database_name --concurrently
0 0 1 * * sudo -u postgres reindexdb --dbname database_name
0 0 10 * * sudo -u postgres reindexdb -a --concurrently
0 0 1 */3 * sudo -u postgres reindexdb -a
```

Рисунок 20.18 – Выполнение команды crontab -e

Первая строка задаёт мягкое перестроение индексов, максимально минуя заблокированные транзакциями данные. Выполняется каждое воскресенье.

Вторая строка задаёт агрессивное перестроение и выполняется в полночь каждый месяц первого числа.

Третья строка указывает на мягкое перестроение всех индексов, в том числе и системных, раз в месяц, 10 числа.

Четвертая строка указывает на агрессивное перестроение всех индексов. Выполняется каждые три месяца первого числа.

Можно указывать собственные интервалы времени, меняя параметры в начале каждой строки в crontab.

5. Сохранить файл с помощью клавиш «CTRL+S».

6. Выйти из файла с помощью клавиш «CTRL+X».

Примечание. Команды выполняются под пользователем root и ставятся в задачник root, потому что изначально у пользователя postgres нет собственного crontab.

Пользователь root через обращение sudo -и postgres может выполнять команды под пользователем postgres без указания пароля.

Важно также, чтобы в pg\_hba.conf присутствовала следующая строка (Рисунок 20.19)

```
TYPE DATABASE USER ADDRESS METHOD
"local" is for Unix domain socket connections only
local all all trust
IPv4 local connections:
host all all 127.0.0.1/32 md5
host all all 0.0.0.0/0 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 20.19 – Настройка pg\_hba.conf

## 20.9 Рекомендации об усечении лога транзакций в MS SQL Server

При активном использовании Системы 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 'zv_k_odyu' is full due to 'LOG_BACKUP'.
```

которая говорит о том, что переполнен лог транзакций, необходимо после уменьшения лога транзакций перезапустить службу сервера приложений.

## 20.10 Рекомендации по обработке ошибок

### 20.10.1 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 20.20).

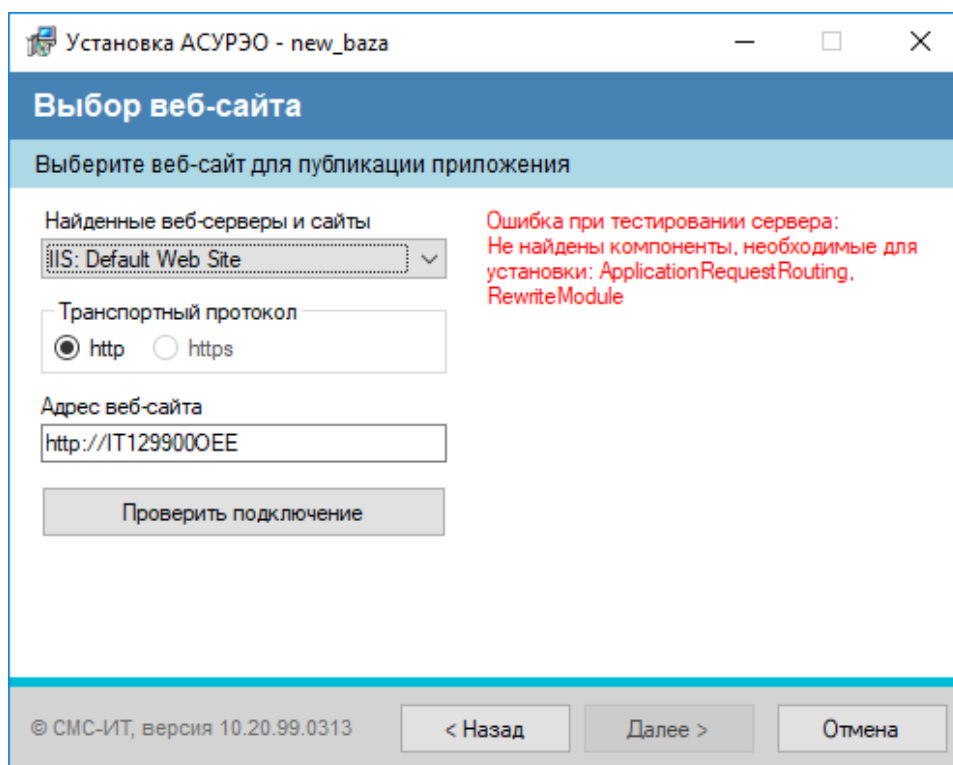


Рисунок 20.20 – Установка дополнительных компонентов IIS

Установка компонента переадресации запросов URL Rewrite 2.0 и установка компонента прокси-переадресации Application Request Routing 2.0 описана в разделе «11 Установка и настройка системного ПО на ОС Linux».

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

### 20.10.2 Ошибка при обновлении ПК

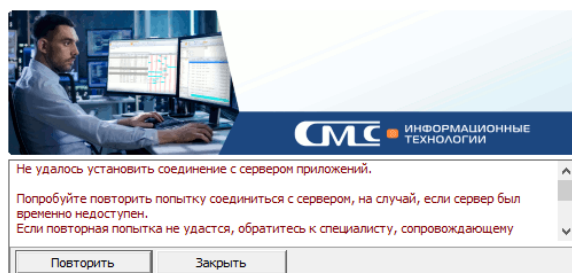
При обновлении ПК в случае возникновения ошибки, не позволяющей произвести обновление необходимо сделать снимок экрана и обратиться в службу поддержки СМС-ИТ.

### 20.10.3 Ошибка при запуске сервера приложений

Если сервер приложений не стартует, то в лог добавляется информация о заиклиивании оборудования: «Ошибка создания справочника оборудования: элемент Id='1111' ссылается сам на себя». Данная ошибка означает, что произошло заиклиивание оборудования самого на себя. Для устранения ошибки необходимо найти заиклиенное оборудование и удалить параметр «ParentDevice» (установить значение Null) или обратиться в службу поддержки СМС-ИТ.

#### 20.10.4 Ошибка при установке соединения с сервером приложений

В случае возникновения ошибки при получении информации с сервера выдается соответствующее сообщение об ошибке (Рисунок 20.21).



- [Интерфейс пользователя](#)
  - [Планы ремонтов](#)
- 
- [Интерфейс администратора](#)
  - [Интерфейс оборудования](#)

Рисунок 20.21 – 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».

#### 20.10.5 Ошибка при запуске приложения

В случае возникновения ошибки при запуске приложения (Рисунок 20.22) необходимо завершить все приложения, использующие Wine, например, Интерфейс пользователя или Интерфейс администратора и выполнить команду `wineserver -k`.

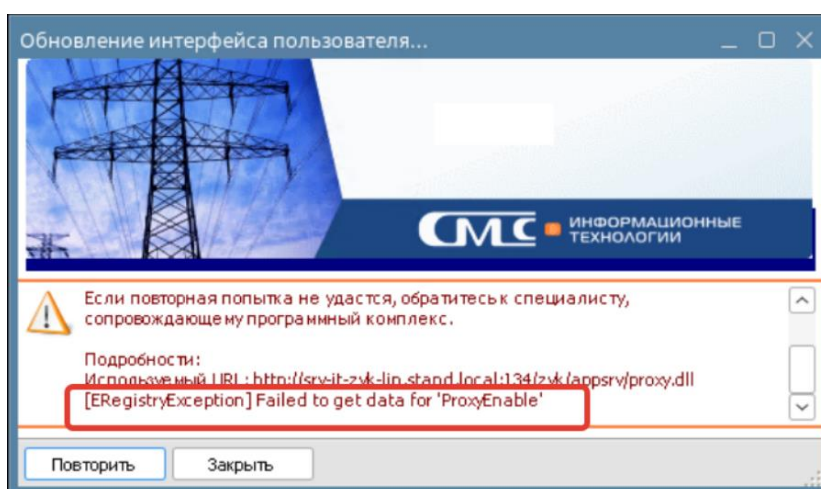


Рисунок 20.22 – Ошибка при запуске приложения

В редакторе реестра Wine в разделе:

«Компьютер\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings» создать DWORD параметр ProxyEnable со значением «0» (Рисунок 20.23).

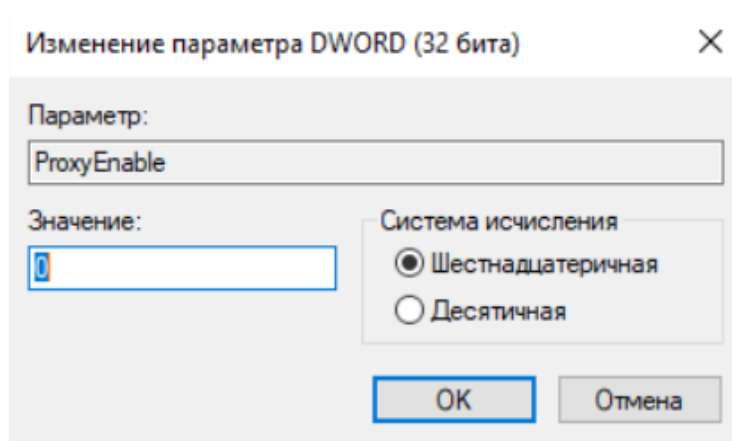


Рисунок 20.23 – Изменение параметра DWORD (32 бита)

#### 20.10.6 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.

#### 20.11 Рекомендации по ограничению объема занимаемой памяти

При достижении сервером приложений zvkservice.exe допустимого объема памяти  $\approx 12$  ГБ рекомендуется перезапустить сервер приложений.

Информация о превышении допустимого объема памяти 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).

## 20.12 Рекомендации по работе Atop

**Atop** – утилита для мониторинга ресурсов Системы в Linux, которая записывает данные о производительности в файлы журналов и предоставляет возможность анализа этих данных в реальном времени или из журналов.

Рекомендуем установить Atop и производить мониторинг. Из основных метрик всегда следует смотреть потребление CPU и памяти, а также периодически контролировать нагрузку на диск. По необходимости можно отслеживать количество потоков у процессов (например, если они накапливаются в большом количестве и не завершаются по какой-либо причине) и сетевую активность (что может быть полезно при наличии сетевых обрывов).

## Приложение 1. Набор файлов установленного экземпляра

Набор файлов установленного экземпляра представлен в таблице 4.

Таблица 4 – 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\zvkc.ini	Файл инициализации программного комплекса
..\server\ZVKService.exe	Служба, реализующая функции сервера приложений
..\server\Server110.bpl	Библиотека, реализующая логику работы подсистемы
..\server\ZVK.sms	Библиотека, реализующая логику работы подсистемы
..\server\zvcomm110.bpl	Библиотека, реализующая логику работы подсистемы
..\server\ZvkDevStat.sms	Библиотека, реализующая логику работы подсистемы
..\server\Client	Набор файлов интерфейсов подсистемы
..\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 подсистеме
..\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	Клиентское приложение подсистемы Ремонты
..\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 подсистемы Ремонты
..\server\AnyDacMsSql.sms	Библиотека, реализующая взаимодействие сервера приложений с MS SQL
..\server\CharsetRecoder.sms	Библиотека, реализующая логику работы подсистемы
..\server\CheckSettings.sms	Библиотека, реализующая логику работы подсистемы
..\server\ClientUpdater.sms	Библиотека, реализующая логику работы подсистемы
..\server\DbErrorLocalizeSupport.sms	Библиотека, реализующая логику работы подсистемы
..\server\DbProvider.sms	Библиотека, реализующая логику работы подсистемы
..\server\DBSessionManager.sms	Библиотека, реализующая логику работы подсистемы

..\server\DocLockManager.sms	Библиотека, реализующая логику работы подсистемы
..\server\EnumService.sms	Библиотека, реализующая логику работы подсистемы
..\server\EventAggregator.sms	Библиотека, реализующая логику работы подсистемы
..\server\EventHandler.sms	Библиотека, реализующая логику работы подсистемы
..\server\HistoryLogger.sms	Библиотека, реализующая логику работы подсистемы
..\server\Integration.sms	Библиотека, реализующая логику работы подсистемы
..\server\kernel.sms	Библиотека, реализующая логику работы подсистемы
..\server\libeay32.dll	Библиотека, реализующая работу с SSL
..\server\Listener.sms	Библиотека, реализующая логику работы подсистемы
..\server\MessageDispatcher.sms	Библиотека, реализующая логику работы подсистемы
..\server\MsSqlSupport.sms	Библиотека, реализующая логику работы подсистемы
..\server\PermanentStorage.sms	Библиотека, реализующая логику работы подсистемы
..\server\Permissions.sms	Библиотека, реализующая логику работы подсистемы
..\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 подсистемы
..\server\Roles.sms	Библиотека, реализующая логику работы подсистемы
..\server\RP.sms	Библиотека, реализующая логику работы подсистемы «Ремонты»

..\server\Rp2Ias.sms	Библиотека, реализующая интеграцию с АС ОБМ (наличие обязательно)
..\server\RPIntegration.sms	Библиотека, реализующая логику работы подсистемы
..\server\Scheduler.sms	Библиотека, реализующая логику работы подсистемы
..\server\SessionContext.sms	Библиотека, реализующая логику работы подсистемы
..\server\SettingsStorage.sms	Библиотека, реализующая логику работы подсистемы
..\server\ssleay32.dll	Библиотека, реализующая работу с SSL
..\server\StandbyStub.sms	Библиотека, реализующая логику работы подсистемы
..\server\TaskManager.sms	Библиотека, реализующая логику работы подсистемы
..\server\TimeService.sms	Библиотека, реализующая логику работы подсистемы
..\server\Users.sms	Библиотека, реализующая логику работы подсистемы
..\server\WorkTime.sms	Библиотека, реализующая логику работы подсистемы
..\server\ZVKLogic.sms	Библиотека, реализующая логику работы подсистемы
..\auth\web.config	Файл конфигурации веб-сервера IIS (требуется только для IIS 7 и выше)
..\ZRP.NET\web.config	
..\ZRP.NET\Autofac.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Autofac.Extensions.DependencyInjection.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Dapper.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\DnsClient.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\dotnet-etcd.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\FastReport.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.Compat.Skia.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.DataVisualization.Skia.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.SkiaDrawing.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FluentValidation.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Google.Protobuf.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Grpc.Core.Api.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Grpc.Net.Client.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Grpc.Net.Common.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Hangfire.AspNetCore.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Hangfire.Core.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Hangfire.InMemory.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\HarfBuzzSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Humanizer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\libHarfBuzzSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\libSkiaSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\MediatR.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\MediatR.Contracts.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Microsoft.AspNetCore.Authentication.JwtBearer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.CodeAnalysis.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.CodeAnalysis.CSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Data.SqlClient.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Data.SqlClient.SNI.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.Relational.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.SqlServer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Extensions.Caching.Memory.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Extensions.DependencyModel.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Identity.Client.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.JsonWebTokens.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Logging.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Protocols.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Protocols.OpenIdConnect.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Tokens.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.OpenApi.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Microsoft.Win32.SystemEvents.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Newtonsoft.Json.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Npgsql.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Npgsql.EntityFrameworkCore.PostgreSQL.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.AspNetCore.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Enrichers.CorrelationId.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Expressions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Extensions.Hosting.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Extensions.Logging.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Formatting.Compact.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Settings.Configuration.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Sinks.Console.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Sinks.Debug.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Sinks.File.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\SkiaSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Sms.ZRP.Domain.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Etcd.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.CommonSqlLogic.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.PostgreSQL.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.SqlServer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\SqlKata.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\SqlKata.Execution.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Swashbuckle.AspNetCore.Swagger.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Swashbuckle.AspNetCore.SwaggerGen.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Swashbuckle.AspNetCore.SwaggerUI.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\System.Configuration.ConfigurationManager.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Drawing.Common.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.IdentityModel.Tokens.Jwt.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Private.ServiceModel.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Runtime.Caching.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Security.Cryptography.ProtectedData.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Security.Permissions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Duplex.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Http.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.NetTcp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Primitives.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Security.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Windows.Extensions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.exe	Приложение, реализующее работу подсистемы ЗРП.Net
..\ZRP.NET\serilogsettings.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.deps.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.runtimeconfig.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.settings.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.settings.Development.json	Конфигурационный файл подсистемы ЗРП.Net

..\ZRP.NET\Sms.ZRP.Application.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Etcd.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.CommonSqlLogic.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.PostgreSQL.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.SqlServer.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Sms.ZRP.WebApi.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\web.config	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Autofac.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Autofac.Extensions.DependencyInjection.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Dapper.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\DnsClient.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\dotnet-etcd.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.Compat.Skia.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.DataVisualization.Skia.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.SkiaDrawing.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FluentValidation.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Google.Protobuf.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Grpc.Core.Api.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Grpc.Net.Client.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Grpc.Net.Common.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Hangfire.AspNetCore.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Hangfire.Core.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Hangfire.InMemory.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\HarfBuzzSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Humanizer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\libHarfBuzzSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\libSkiaSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\MediatR.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\MediatR.Contracts.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.AspNetCore.Authentication.JwtBearer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.CodeAnalysis.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.CodeAnalysis.CSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Data.SqlClient.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Data.SqlClient.SNI.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.Relational.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.EntityFrameworkCore.SqlServer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Extensions.Caching.Memory.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Microsoft.Extensions.DependencyModel.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Identity.Client.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.JsonWebTokens.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Logging.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Protocols.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Protocols.OpenIdConnect.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.IdentityModel.Tokens.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.OpenApi.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Microsoft.Win32.SystemEvents.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Newtonsoft.Json.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Npgsql.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Npgsql.EntityFrameworkCore.PostgreSQL.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.AspNetCore.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Enrichers.CorrelationId.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Expressions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Extensions.Hosting.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Extensions.Logging.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Serilog.Formatting.Compact.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Settings.Configuration.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Sinks.Console.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Sinks.Debug.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Serilog.Sinks.File.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\SkiaSharp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Etcd.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.CommonSqlLogic.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.PostgreSQL.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.SqlServer.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Sms.ZRP.WebApi.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\SqlKata.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\SqlKata.Execution.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Swashbuckle.AspNetCore.Swagger.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Swashbuckle.AspNetCore.SwaggerGen.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Swashbuckle.AspNetCore.SwaggerUI.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Configuration.ConfigurationManager.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Drawing.Common.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.IdentityModel.Tokens.Jwt.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Private.ServiceModel.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Runtime.Caching.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Security.Cryptography.ProtectedData.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Security.Permissions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Duplex.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Http.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\System.ServiceModel.NetTcp.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Primitives.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.ServiceModel.Security.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\System.Windows.Extensions.dll	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.exe	Приложение, реализующее работу ЗРП.Net
..\ZRP.NET\serilogsettings.json	Конфигурационный файл с настройками логирования
..\ZRP.NET\Sms.ZRP.WebApi.deps.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.runtimeconfig.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.settings.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.settings.Development.json	Конфигурационный файл подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Domain.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Cache.Etcd.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.CommonSqlLogic.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.PostgreSQL.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.Data.SqlServer.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.settings.json	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.settings.Development.json	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net

..\ZRP.NET\FastReport.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Infrastructure.IoC.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.pdb	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\FastReport.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.Application.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.Abstractions.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\ZRP.NET\Sms.ZRP.WebApi.ZVK.xml	Библиотека, реализующая логику работы подсистемы ЗРП.Net
..\IdentityServer\web.config	Конфигурационный файл сайта авторизации ЗРП.Net
..\IdentityServer\AuthServer.dll	Библиотека, реализующая логику работы сервера авторизации ЗРП.Net

..IdentityServer\IdentityModel.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\IdentityServer4.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\IdentityServer4.Storage.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Kerberos.NET.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.AspNetCore.Authentication.Negotiate.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.AspNetCore.Authentication.OpenIdConnect.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.AspNetCore.Connections.Abstractions.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.Data.SqlClient.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.Data.SqlClient.SNI.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.EntityFrameworkCore.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.EntityFrameworkCore.Abstractions.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.EntityFrameworkCore.Relational.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.EntityFrameworkCore.SqlServer.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.Extensions.Caching.Memory.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.Extensions.DependencyInjection.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.Extensions.Features.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.Identity.Client.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..IdentityServer\Microsoft.IdentityModel.JsonWebTokens.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net

..\IdentityServer\Microsoft.IdentityModel.Logging.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Microsoft.IdentityModel.Protocols.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Microsoft.IdentityModel.Protocols.OpenIdConnect.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Microsoft.IdentityModel.Tokens.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Microsoft.Win32.SystemEvents.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Newtonsoft.Json.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Newtonsoft.Json.Bson.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Npgsql.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Npgsql.EntityFrameworkCore.PostgreSQL.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.AspNetCore.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Enrichers.CorrelationId.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Expressions.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Extensions.Hosting.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Extensions.Logging.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Formatting.Compact.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Settings.Configuration.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net
..\IdentityServer\Serilog.Sinks.Console.dll	Библиотека, реализующая логику работы сервера авторизации ZPII.Net

..IdentityServer\Serilog.Sinks.Debug.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\Serilog.Sinks.File.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Configuration.ConfigurationManager.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.DirectoryServices.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.DirectoryServices.Protocols.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Drawing.Common.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.IdentityModel.Tokens.Jwt.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.IO.Pipelines.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Net.Http.Formatting.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Runtime.Caching.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Security.Cryptography.ProtectedData.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Security.Permissions.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Web.Http.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\System.Windows.Extensions.dll	Библиотека, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\AuthServer.exe	Приложение, реализующая логику работы сервера авторизации ЗПИ.Net
..IdentityServer\AuthServer.deps.json	Конфигурационный файл сайта авторизации ЗПИ.Net
..IdentityServer\AuthServer.runtimeconfig.json	Конфигурационный файл сайта авторизации ЗПИ.Net
..IdentityServer\AuthServer.settings.json	Конфигурационный файл сайта авторизации ЗПИ.Net

---

..\IdentityServer\AuthServer.settings.Development.json	Конфигурационный файл сайта атворизации ЗРП.Net
..\IdentityServer\serilogsettings.json	Конфигурационный файл сайта атворизации ЗРП.Net
..\IdentityServer\AuthServer.pdb	Библиотека, реализующая логику работы сервера авторизации ЗРП.Net

---

## Приложение 2. Скрипт для штатного останова серверов приложений Системы

Ниже приведён скрипт для остановки сервера приложений, а также сервера приложений веб-версии Системы. В тексте скрипта необходимо заменить переменные, помеченные зелёным, на собственные значения.

`server_directory` – расположение серверной директории. По умолчанию `/opt/asureo`

`ASUREO_name` – наименование контейнера сервера приложений. 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;
```









---

## Приложение 3. Скрипт для мониторинга размера каталога docker

```
#!/bin/bash
set -euo pipefail

OVERLAY_DIR="/var/lib/docker/overlay2"
LOGFILE="/tmp/overlay_cleanup_$(date +%Y%m%d_%H%M%S).log"

echo "=== Очистка overlay2 начата $(date) ===" | tee "$LOGFILE"
echo "Log: $LOGFILE"
echo

echo "[1/9] Сбор используемых директорий overlay2 из контейнеров и образов..." | tee -a "$LOGFILE"

USED_IDS_FILE=$(mktemp)

collect_overlay_ids() {
 while read -r json; do
 echo "$json" | jq -r '. | .LowerDir?, .UpperDir?, .WorkDir?, .MergedDir?' \
 | grep -E "^/" | tr ':' '\n' | while read -r path; do
 if [["$path" == $OVERLAY_DIR/*]]; then
 id=$(basename "$(dirname "$path")")
 echo "$id"
 fi
 done
 done
}

if docker ps -aq | grep -q .; then
 docker inspect $(docker ps -aq) --format '{{json .GraphDriver.Data}}' 2>/dev/null | collect_overlay_ids >>
"$USED_IDS_FILE"
fi

if docker images -q | grep -q .; then
 docker inspect $(docker images -q) --format '{{json .GraphDriver.Data}}' 2>/dev/null | collect_overlay_ids >>
"$USED_IDS_FILE"
fi

USED_IDS=$(sort -u "$USED_IDS_FILE")
rm -f "$USED_IDS_FILE"

USED_COUNT=$(echo "$USED_IDS" | grep -c . || true)
echo "Найдено используемых overlay-директорий: $USED_COUNT" | tee -a "$LOGFILE"
```

---

```
echo "[2/9] Поиск всех директорий overlay2..." | tee -a "$LOGFILE"
ALL_IDS=$(find "$OVERLAY_DIR" -mindepth 1 -maxdepth 1 -type d -not -name "l" -printf '%f\n' | sort)
TOTAL_COUNT=$(echo "$ALL_IDS" | grep -c . || true)
echo "Всего директорий: $TOTAL_COUNT" | tee -a "$LOGFILE"

echo "[3/9] Определение неиспользуемых директорий..." | tee -a "$LOGFILE"

ORPHAN_IDS=$(comm -23 <(echo "$ALL_IDS") <(echo "$USED_IDS"))
ORPHAN_COUNT=$(echo "$ORPHAN_IDS" | grep -c . || true)
echo "Неиспользуемых директорий: $ORPHAN_COUNT" | tee -a "$LOGFILE"

if [[$ORPHAN_COUNT -eq 0]]; then
 echo "Нет неиспользуемых директорий. Завершение." | tee -a "$LOGFILE"
 exit 0
fi

echo
echo "Следующие директории будут удалены:" | tee -a "$LOGFILE"
echo "$ORPHAN_IDS" | sed 's/^/ - /' | tee -a "$LOGFILE"
echo

read -p "Удалить эти overlay-директории после остановки Docker? (y/N): " confirm
if [["$confirm" != [yY]]]; then
 echo "Отменено пользователем." | tee -a "$LOGFILE"
 exit 0
fi

echo "[4/9] Убиваем процессы внутри контейнеров..." | tee -a "$LOGFILE"

kill -9 $(ps aux | grep 'JsonEditor.dll' | grep -v 'grep' | awk '{print $2}') > /dev/null 2>&1 && \
 echo "Убиты процессы JsonEditor.dll" | tee -a "$LOGFILE"

kill -9 $(ps aux | grep 'Sms.ZRP.WebApi.dll' | grep -v 'grep' | awk '{print $2}') > /dev/null 2>&1 && \
 echo "Убиты процессы Sms.ZRP.WebApi.dll" | tee -a "$LOGFILE"

kill -9 $(ps aux | grep 'AuthServer.dll' | grep -v 'grep' | awk '{print $2}') > /dev/null 2>&1 && \
 echo "Убиты процессы AuthServer.dll" | tee -a "$LOGFILE"

docker exec zrp wine cmd /k net stop Zvk_zvk > /dev/null 2>&1 && \
 echo "Служба Zvk_zvk внутри контейнера zrp остановлена" | tee -a "$LOGFILE"

echo "[5/9] Остановка Docker..." | tee -a "$LOGFILE"
systemctl stop docker || true
sleep 3
```

---

---

```
echo "[6/9] Проверка dockerd..." | tee -a "$LOGFILE"
for i in {1..20}; do
 if ! pgrep dockerd >/dev/null; then
 echo "Docker успешно остановлен." | tee -a "$LOGFILE"
 break
 fi
 sleep 1
done
pgrep dockerd >/dev/null && { echo "dockerd всё ещё активен, убиваю..."; pkill -9 dockerd || true; sleep 2; }

echo "[7/9] Удаление неиспользуемых директорий..." | tee -a "$LOGFILE"
for id in $ORPHAN_IDS; do
 DIR="$OVERLAY_DIR/$id"
 echo "Удаляю $DIR" | tee -a "$LOGFILE"
 rm -rf "$DIR" || echo "Не удалось удалить $DIR" | tee -a "$LOGFILE"
done

echo "[8/9] Очистка пустых каталогов..." | tee -a "$LOGFILE"
find "$OVERLAY_DIR" -mindepth 1 -maxdepth 1 -type d -empty -print -delete || true

echo "[9/9] Перезапуск Docker..." | tee -a "$LOGFILE"
systemctl start docker || true
sleep 3

echo
echo "=== Очистка overlay2 завершена успешно ===" | tee -a "$LOGFILE"
echo "Подробности: $LOGFILE"
```