

**АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА ПО  
ИСКУССТВЕННЫМ СООРУЖЕНИЯМ НА АВТОМОБИЛЬНЫХ ДОРОГАХ  
(АИС ИССО-Н+)**

Руководство администратора

## **АННОТАЦИЯ**

Настоящий документ содержит инструкцию пользователя по работе с Автоматизированной информационно-аналитической системой по искусственным сооружениям на автомобильных дорогах.

Следует учитывать, что система постоянно совершенствуется, и некоторые положения настоящей инструкции могут отличаться от более нового варианта используемой версии программного комплекса.

## ОГЛАВЛЕНИЕ

1	НАЗНАЧЕНИЕ СИСТЕМЫ .....	4
2	СРЕДСТВА И МОДУЛИ АДМИНИСТРИРОВАНИЯ.....	5
2.1	Общие положения .....	5
2.2	Общие принципы администрирования системы.....	5
2.3	Управление безопасностью системы .....	5
2.3.1	Создание и настройка роли пользователей .....	5
2.3.2	Использование административных шаблонов .....	7
2.3.3	Добавление пользователя или группы пользователей .....	7
2.4	Подключенные пользователи .....	8
3	УСТАНОВКА И ПОДГОТОВКА СИСТЕМЫ К РАБОТЕ .....	9
3.1	Общие сведения .....	9
3.2	Установка электронного ключа .....	9
3.3	Инсталляция сервера приложений .....	9
3.4	Конфигурирование серверного приложения.....	11
3.5	Установка клиентского приложения.....	11
4	ПЕРВЫЙ АДМИНИСТРАТИВНЫЙ ЗАПУСК .....	13
5	ПОДСИСТЕМА ЦЕНТРАЛИЗОВАННОГО ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АС НА ОБЪЕКТАХ АВТОМАТИЗАЦИИ.....	14
5.1	Общие сведения .....	14
5.2	Использование ключей SenseLock .....	14
5.3	Клиент обновлений серверного программного обеспечения .....	14

## **1 НАЗНАЧЕНИЕ СИСТЕМЫ**

Автоматизированная Система (АС или система) предназначена для информационного обеспечения процесса управления содержанием искусственных сооружений (ИССО) на автомобильных дорогах на основе автоматизации решения следующих основных задач:

- Учет и оперативный доступ к информации по конструктивному описанию искусственных сооружений и их состоянию по дефектности.
- Оценка и прогнозирование технического состояния сооружений.
- Определение возможности и условий пропуска нагрузки по сооружениям (по условию грузоподъемности).
- Разработка опорных планов программ по реконструкции, капитальному ремонту, ремонту, ППР, ПИР, обследованию.
- Анализ состояния парка ИССО по произвольным параметрам для перспективного планирования и разработки технической политики в отношении ИССО, научно-исследовательских целей, совершенствования нормативно-методической базы и т.д.
- Формирование и печать стандартных форм отчетных документов.

## 2 СРЕДСТВА И МОДУЛИ АДМИНИСТРИРОВАНИЯ

### 2.1 Общие положения

Система представляет собой трехзвенное приложение, включающее следующие компоненты:

- Сервер баз данных;
- Сервер приложения;
- Клиентское приложение.

Все компоненты системы могут размещаться физически на одном или нескольких компьютерах (серверах). Между компьютерами, с компонентами системы, должна обеспечиваться связь по локальной вычислительной сети на скорости 100Мб/с. Между клиентским и серверным приложениями должна обеспечиваться связь по протоколу TCP/IP. Порт, по которому выполняется коммуникация, настраивается при установке системы.

Серверное приложение представляет собой WCF службу Windows, которая регистрируется в системе при установке приложения. В системе может быть зарегистрировано один или несколько «Наборов данных». «Набор данных» представляет собой структуру, позволяющую логически объединить искусственные сооружения в группы. Пользователям могут быть настроены различные права доступа к различным наборам данных.

### 2.2 Общие принципы администрирования системы

Все функции администрирования сосредоточены на клиентской части системы. Аутентификация пользователей реализована на базе пользователей Windows (или домена Windows). Авторизация реализована на базе «ролей», которые создаются в системе в разделе «Управление доступом». Роль представляет собой набор прав доступа к различным объектам системы. При конфигурировании ролей могут быть установлены следующие права доступа:

- «Не заданы» (пользователь не имеет прав доступа к объекту, если иное не указано другой ролью);
- «Отсутствуют» (права доступа отсутствуют в независимости от значений, указанных в других ролях);
- «Чтение» (пользователь имеет право чтения информации или работы с модулем в режиме чтения, если это не запрещено другой ролью);
- «Запись» (пользователь имеет полный доступ к объекту, если иное не указано другой ролью).

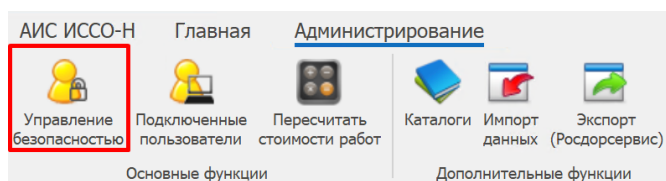
Одна или несколько ролей могут быть назначены доменному пользователю или доменной группе пользователей для каждого набора данных. Права, назначенные пользователю, перекрывают права, назначенные группе пользователей, в которую этот пользователь входит.

Администрирование системы может быть выполнено пользователем, который имеет права «Администратор домена» или права локального администратора на компьютере (сервере), где установлено серверное приложение. При подключении такого пользователя в правом нижнем углу окна входа в систему, в выпадающем списке «Набор данных» присутствует значение «Административный вход». При выборе этого значения клиентское программное обеспечение переходит в режим управления безопасностью системы. Управлять безопасностью системы могут также пользователи, в роли которых имеется право доступа «Изменение» на модуль «Администрирование».

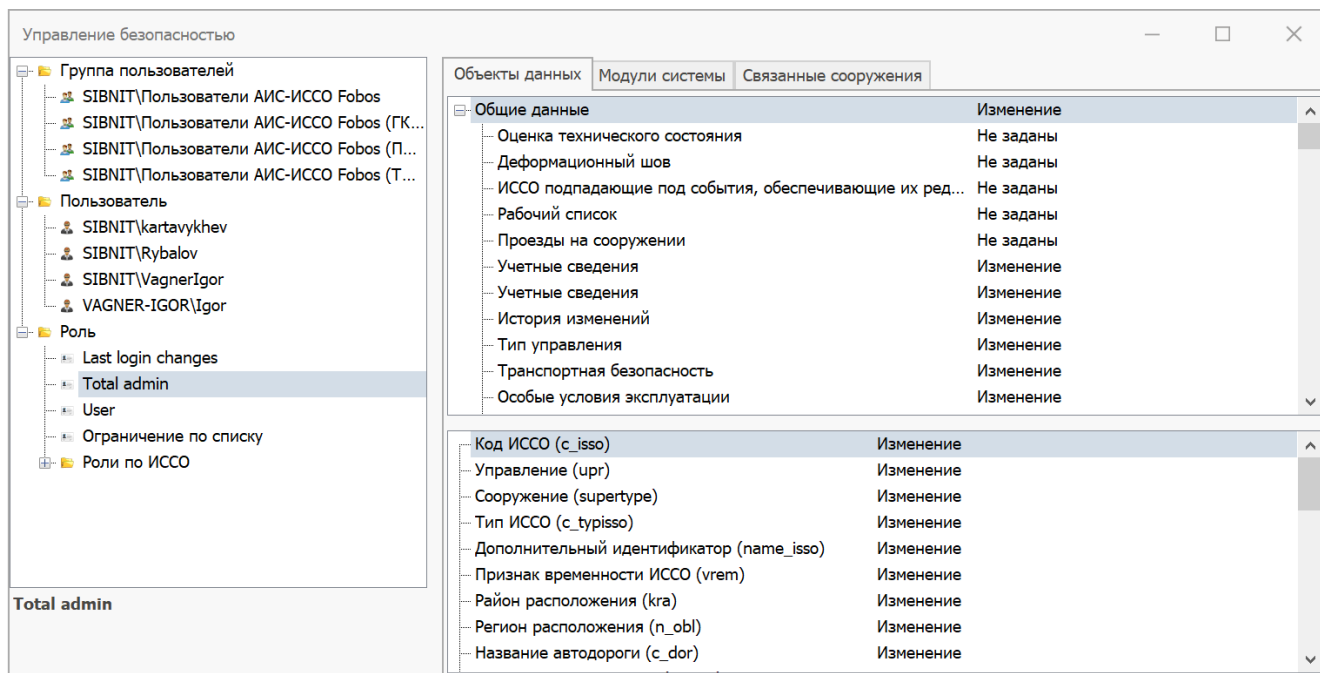
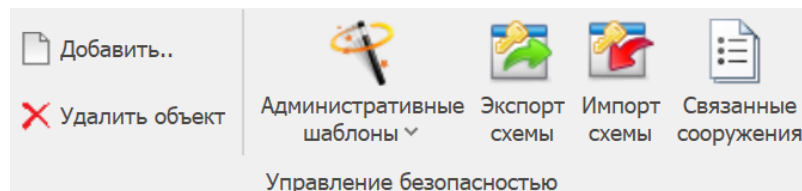
### 2.3 Управление безопасностью системы

#### 2.3.1 Создание и настройка роли пользователей

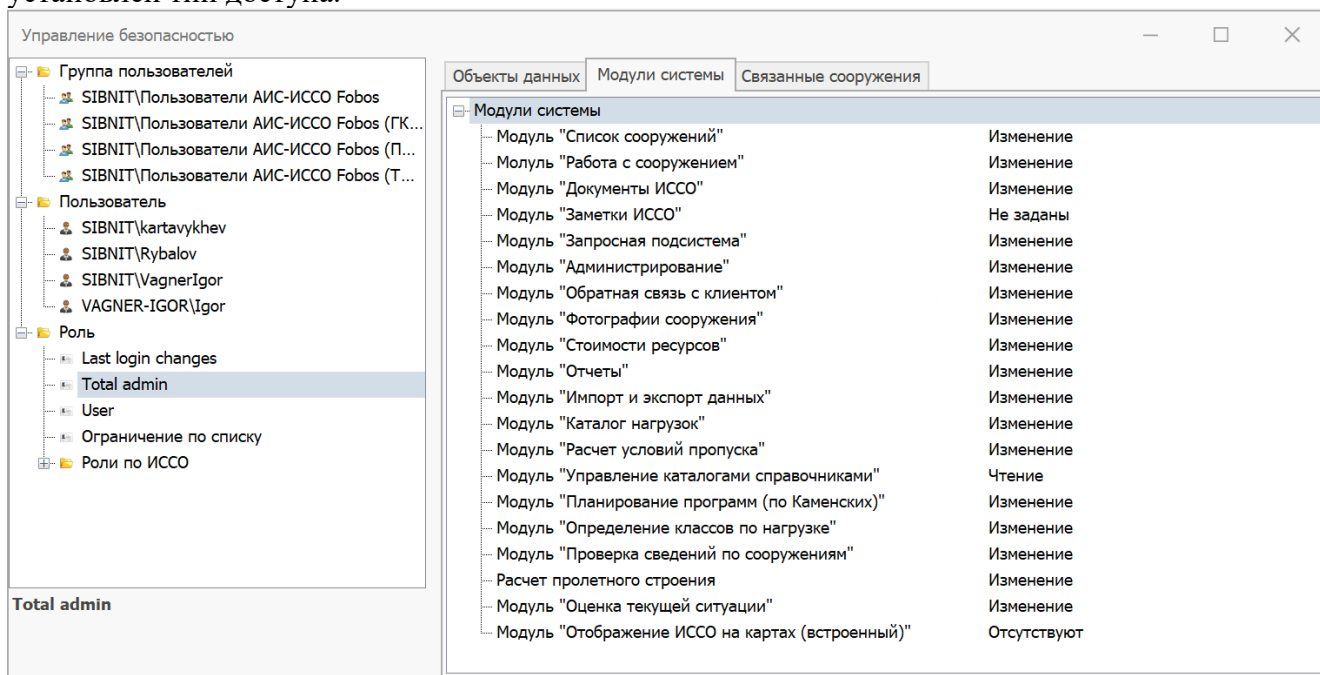
Перейти на закладку «Администрирование» и нажать кнопку «Управление безопасностью».



Откроется следующая экранная форма с собственной группой управляющих кнопок на ленте вкладок:



В левой части формы отображено дерево объектов безопасности: пользователи, группы пользователей, роли. В правой части окна для ролей отображается две закладки: «Объекты данных» и «Модули системы». Правая часть формы для ролей имеет два режима отображения, определяемые закладками: «Объекты данных» и «Модули системы». Закладка «Объекты данных» отображает окно, разделенное горизонтальной границей на две области. В верхней области представлено полное дерево объектов (таблиц) базы данных, в нижней области – атрибуты (поля) выбранного объекта. Закладка «Модули системы» отображает перечень зарегистрированных модулей системы. Для каждого объекта в этой форме может быть установлен тип доступа.



Для создания новой роли необходимо выполнить следующие действия:

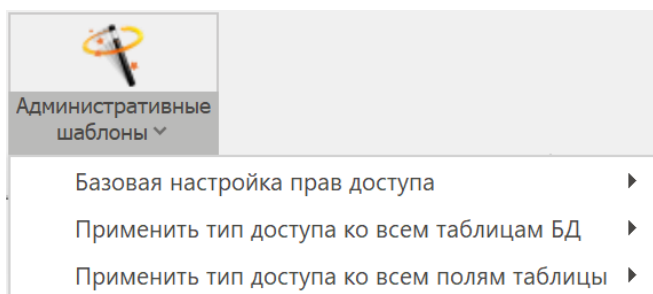
- 1) Выделить в дереве элемент «папку», в которую следует поместить создаваемую роль;
- 2) Нажать кнопку «Добавить» из состава группы «Управление безопасностью»;
- 3) Из выпадающего списка выбрать пункт «Добавить роль»;
- 4) В появившемся диалоговом окне ввести имя добавляемой роли и нажать кнопку «Создать».

Новая роль отобразится в дереве в левой части формы.

Для настройки роли необходимо выделить ее в дереве, и в правой части окна напротив соответствующего объекта установить требуемый уровень прав доступа. По умолчанию все объекты для вновь созданной роли имеют тип доступа «Не заданы».

### 2.3.2 Использование административных шаблонов

Кнопка «Административные шаблоны» в группе «Управление безопасностью» закладки «Администрирование» на ленте позволяет применить определенные права доступа для выбранной роли.



- «Базовая настройка прав доступа» - устанавливает выбранный тип доступа ко всем объектам безопасности за исключением некоторых (системных).
- «Применить тип доступа ко всем таблицам БД» - устанавливает выбранный тип доступа ко всем таблицам и их полям.
- «Применить тип доступа ко всем полям таблицы» - устанавливает выбранный тип доступа ко всем полям выбранной таблицы.

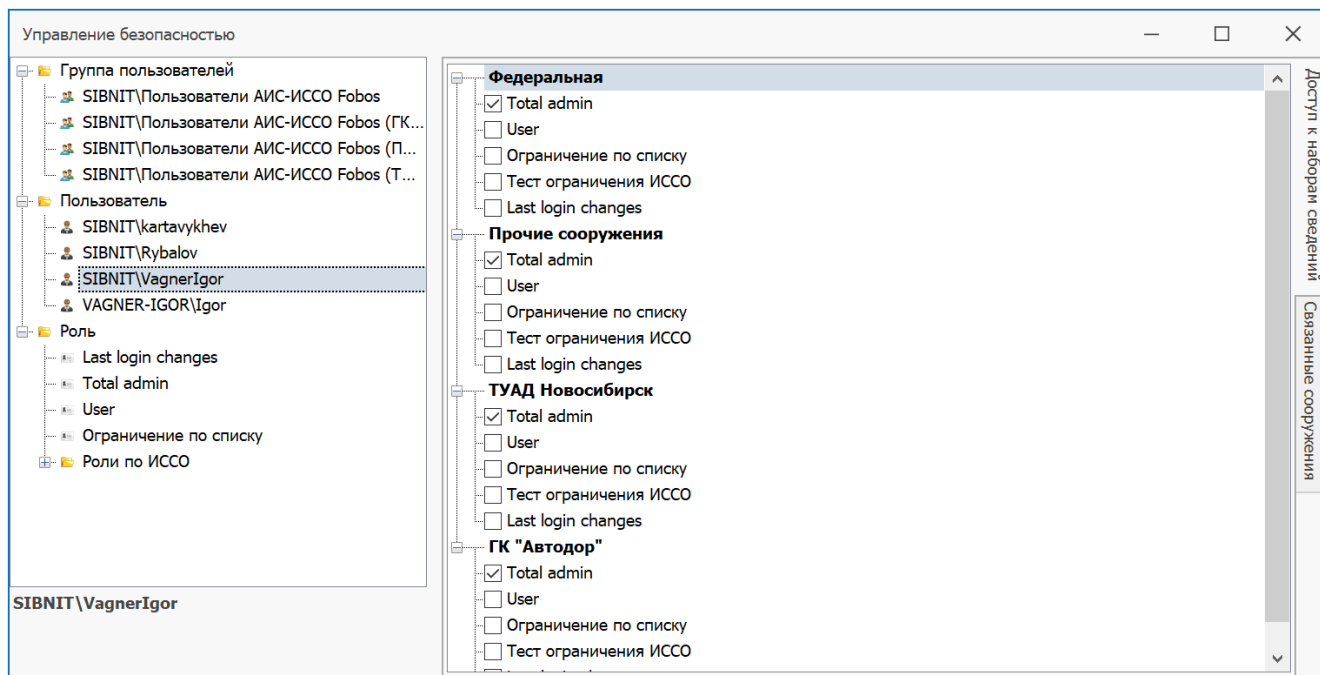
### 2.3.3 Добавление пользователя или группы пользователей

Для добавления пользователя или группы пользователей необходимо:

- выделить в дереве, расположенном в левой части окна, элемент «папку», в которую следует поместить создаваемого пользователя;
- выбрать соответствующий пункт меню кнопки «Добавить» в группе «Управление безопасностью».

В появившемся диалоговом окне ввести имя пользователя или группы в поле «Имя» и нажать кнопку «Проверить». При положительном результате проверки кнопка «Создать» станет доступной. Нажать кнопку «Создать».

Для настройки параметров доступа для конкретного пользователя или группы необходимо выбрать соответствующий объект (пользователя или группу пользователей) и в правой части формы в группе соответствующего набора сведений выбрать постановкой «флажков» необходимые роли.



## 2.4 Подключенные пользователи

Просмотр списка работающих в системе пользователей доступен при нажатии кнопки «Подключенные пользователи». В окне отображается перечень, работающих в данный момент пользователей.

Пользователь	Адрес	Подключен
SIBNIT\PopovAleksey	10.242.52.157	13.11.2025 4:53:46
SIBNIT\VagnerIgor	10.242.52.182	13.11.2025 11:26:41
SIBNIT\kartavykhev	::1	13.11.2025 11:53:05

Модуль системы позволяет выполнять следующие операции над одним или несколькими (выделенными в списке) пользователями:

- Завершить сеанс. Данное действие отображает на мониторе пользователя диалоговое окно о завершении сеанса работы. Пользователь может нажать кнопку «отмена» и продолжить работать в клиентском приложении. В этом случае система предупредит о том, что следует завершить работу в ближайшее время. Если в течение 30 секунд пользователь не нажмет ни на одну из кнопок диалогового окна, система завершит работу автоматически.
- Завершить сеанс аварийно. Завершает работу клиента без отображения предупреждений пользователю.
- Отправить сообщение. Позволяет отправить пользователю произвольное текстовое сообщение.



### 3 УСТАНОВКА И ПОДГОТОВКА СИСТЕМЫ К РАБОТЕ

#### 3.1 Общие сведения

Установка программного обеспечения АС включает следующие этапы:

- установка электронного ключа;
- инсталляция базы данных (процедура описана в отдельном документе);
- инсталляция сервера приложений;
- инсталляция клиентской части (пользовательского приложения);
- настройка системы (см. раздел «Первый административный запуск»).

#### 3.2 Установка электронного ключа

Система поставляется вместе с электронным ключом SenseLock, который используется для идентификации организации, представители которой производят редактирование сведений в системе.

При отсутствии электронного ключа система работает в режиме просмотра сведений – пользователи имеют возможность просматривать информацию по ИССО и имеют доступ к определенному набору аналитических функций. Редактирование данных невозможно. Наличие электронного ключа снимает блокировку на редактирование.

Каждый электронный ключ имеет уникальный идентификатор, который используется АС в работе подсистемы автоматического обновления и ряде других подсистем.

Электронный ключ SenseLock устанавливается на компьютере, где работает серверное приложение АС. Клиенты АС получают доступ к электронному ключу автоматически.

Для обеспечения функционирования электронного ключа необходимо выполнить установку его драйвера. Дистрибутив драйвера электронного ключа имеется в комплекте поставки системы. Для установки драйвера необходимо выполнить следующие операции:

- 1) Распаковать файл драйвера.
- 2) Запустить файл InstWiz3.exe.
- 3) В мастере установки нажимать кнопки «Next» до тех пор, пока драйвер не будет установлен полностью.

По окончании установки драйверов вставить электронный ключ в свободный USB порт компьютера. Электронный ключ должен быть подключен к компьютеру на протяжении всего времени работы серверного приложения АС.

#### 3.3 Инсталляция сервера приложений

Убедиться, что на сервере установлен Microsoft .NET Framework 4.6.2 (дистрибутив доступен по ссылке: [Автономный платформа .NET Framework 4.6.2 для Windows \(microsoft.com\)](https://www.microsoft.com/ru-ru/details/4699462)).

Запустить файл aisIssoServer\_pg.msi из состава установочного пакета. Если на компьютере уже была установлена предыдущая версия системы, первый запуск файла aisIssoServer\_pg.msi сообщит об этом и предложит удалить приложение самостоятельно стандартными средствами операционной системы. После удаления приложения следует заново выполнить установку.

В процессе установки отображаются диалоговые окна в следующем порядке: приглашение; выбор директории установки; выбор дополнительных параметров; подтверждение; отображения хода выполнения; завершение установки. Все диалоги, за исключением выбора дополнительных параметров, стандартные и не требуют дополнительного разъяснения. Диалоговое окно «Дополнительные параметры» имеет следующий вид:

- Порт сервера. Вводится параметр, указывающий целочисленное значение порта, по которому обеспечивается клиент–серверное взаимодействие. Значение порта может быть изменено, но не рекомендуется использовать значение меньше 1024. По умолчанию значение равно 9991.
- Имя экземпляра сервера баз данных. Вводится адрес сервера в виде IP адреса или DNS имени. По умолчанию значение равно localhost.
- Порт сервера базы данных. Вводится значение порта сервера PostgreSQL. По умолчанию значение равно 5432.
- Имя базы данных. Вводится имя присоединенной БД.
- Пользователь БД. Вводится имя пользователя для подключения к базе данных. По умолчанию равно postgres.
- Пароль пользователя. Вводится соответствующий пароль пользователя.

Указанные параметры являются обязательными при установке серверного приложения и впоследствии могут быть изменены администратором системы.

В процессе установки программа выполняет следующие операции:

- Копирование файлов системы.
- Создание исключения в брандмауэр Windows для сервиса системы.
- Установка и запуск сервиса системы.

После установки серверного приложения в главном меню Windows в разделе «Программы» будет создана группа «АИС ИССО-Н v8.0», содержащая следующие ярлыки:

- Запустить сервер АИС ИССО-Н v8.0 – запуск сервиса «Сервер АИС ИССО-Н»;
- Конфигурация АИС ИССО-Н v8.0 сервер – открыть файл конфигурации сервера АС, в котором можно отредактировать параметры сервера, вводимые на этапе его установки. Для применения изменений, внесенных в конфигурационный файл, необходимо остановить и запустить сервер АС;
- Остановить сервер АИС ИССО-Н v8.0 – остановка сервиса «Сервер АС»;
- Удалить АИС ИССО-Н v8.0 сервер – удаления из системы сервера АС;
- Лог АИС ИССО-Н v8.0 сервер – просмотр лог файла сервера АС.

По завершении процесса установки серверное приложение полностью готово к работе. Контроль работоспособности сервера осуществляется посредством просмотра лог файла (файл aisLog.log), расположенного в директории установки сервера. Для просмотра файла в главном меню Windows, разделе «Программы \ АИС ИССО-Н v8.0» программа установки создает ярлык «Лог АИС ИССО-Н v8.0 сервер». Лог файл состоит из строк следующего формата:

[дата и время события] [статус события] [текст события]

Возможны следующие варианты типов событий:

- **i** – информационное сообщение;
- **w** – предупреждение;
- **e** – ошибка;

- s – операция выполнена успешно.

При запуске серверного приложения и в процессе его работы не должно появляться сообщений со статусом «ошибка». Наличие записей со статусом «ошибка» сигнализирует о неполадках в работе системы. В таком случае рекомендуется отправлять данные лог файла разработчику системы.

### 3.4 Конфигурирование серверного приложения

Конфигурирование серверного приложения в обычном режиме его работы не требуется. Управление параметрами серверного приложения осуществляется посредством редактирования его конфигурационного файла, который расположен в директории установки серверного приложения и имеет название AisServerService.exe.config. В файл включено несколько параметров, значения которых влияют на работу системы. Перечень параметров и их значений по умолчанию представлен в следующей таблице:

Имя параметра	Значение по умолчанию	Описание параметра
<b>Параметры группы DbConnect_Main</b>		
dbHost	[отсутствует]	Имя сервера баз данных (его расположение в сети)
dbName	[отсутствует]	Имя базы данных на сервере баз данных
dbUser	[отсутствует]	Имя пользователя для подключения к серверу БД
dbPass	[отсутствует]	Пароль пользователя для подключения к БД
dbPort	5432	Порт базы данных
<b>Параметры группы appSettings</b>		
port	9991	Порт, на котором сервер приложений принимает подключения клиентов

После редактирования конфигурационного файла необходимо перезапустить службу сервера приложений АС (или перезагрузить сервер).

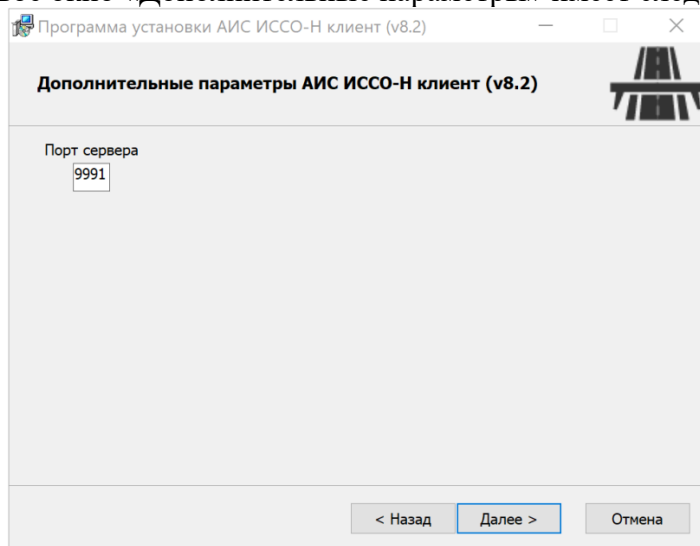
### 3.5 Установка клиентского приложения

Убедиться, что на компьютере установлен Microsoft .NET Framework 4.6.2.

Для установки клиентского приложения запустить файл aisIssoClient\_pg.msi из состава установочного пакета.

Если на компьютере уже была установлена предыдущая версия системы, первый запуск файла aisIssoClient\_pg.msi сообщит об этом и предложит удалить приложение самостоятельно стандартными средствами операционной системы. После удаления приложения заново выполнить установку.

В процессе установки пользователю отображаются следующие диалоговые окна: приглашение; выбор директории установки; выбор дополнительных параметров; подтверждение; отображения хода выполнения; завершение установки. Все диалоги, за исключением дополнительных параметров, стандартные и не требуют дополнительного разъяснения. Диалоговое окно «Дополнительные параметры» имеет следующий вид:



В поле «Порт сервера» вводится параметр, указывающий целочисленное значение порта, по которому обеспечивается клиент–серверное взаимодействие. Значение порта должно соответствовать значению порта, используемому при установке серверного приложения.

Запуск клиентского приложения осуществляется с помощью главного меню Windows («Пуск» → «Программы» → «АИС ИССО-Н v8.0» → «АИС ИССО-Н v8.0 клиент»).

#### 4 ПЕРВЫЙ АДМИНИСТРАТИВНЫЙ ЗАПУСК

Перед выполнением первого запуска необходимо убедиться в правильном функционировании серверного приложения, посредством просмотра лог файла на предмет отсутствия в нем событий со статусом «ошибка».

При первом запуске системы необходимо настроить подсистему безопасности. Для этого следует подключиться к серверному приложению с использованием учетной записи, обладающей административными правами (локальный администратор или администратор домена) на компьютере с установленным серверным приложением, выполнив следующие действия:

- 1) Запустить клиентское приложение АС.
- 2) В левом нижнем углу окна входа в поле «Адрес сервера» ввести адрес сервера (IP адрес или его DNS имя). При локальном входе (когда серверное и клиентское приложения расположены на одном компьютере) можно использовать адрес 127.0.0.1 или ключевое слово localhost. Нажать Enter.
- 3) В правом нижнем углу окна входа в выпадающем списке «Набор данных» выбрать значение «Административный вход».
- 4) Нажать кнопку «Вход».

В режиме «Административного входа» в клиентском приложении присутствует только одна закладка «Администрирование», в которой имеется, в том числе, кнопка «Управление безопасностью». В процессе настройки безопасности необходимо выполнить следующие операции:

- 1) Создать роли (предлагаемый список носит рекомендательный характер):
  - «Администратор» – роль, для создания которой используется административный шаблон «Базовая настройка прав доступа \ Запись» и установлено значение типа доступа «Изменение» к модулям «Администрирование» и «Импорт и экспорт данных».
  - «Пользователь» - роль, для создания которой используется административный шаблон «Базовая настройка прав доступа \ Запись» без дополнительных изменений.
- 2) Добавить пользователей или группы (доменные) пользователей.
- 3) Установить роли для добавленных пользователей и групп пользователей на каждый набор данных.

## **5 ПОДСИСТЕМА ЦЕНТРАЛИЗОВАННОГО ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АС НА ОБЪЕКТАХ АВТОМАТИЗАЦИИ**

### **5.1 Общие сведения**

Подсистема обеспечивает обновление программного обеспечения АС для всех групп пользователей системы. В состав обновляемых компонентов входят:

- Программное обеспечение сервера приложения.
- Программное обеспечение рабочего места пользователя (клиентское ПО).
- Структуру и состав базы данных.

### **5.2 Использование ключей SenseLock**

Система обновлений использует электронные ключи SenseLock для идентификации клиентов обновлений серверного ПО и разграничения прав доступа.

При обращении клиента обновления серверного ПО к серверу обновлений, клиент предъявляет идентификатор электронного ключа. На основании этой информации сервер обновлений идентифицирует клиента и определяет возможность установки и состав обновлений, необходимых для конкретного клиента.

### **5.3 Клиент обновлений серверного программного обеспечения**

Клиент обновлений серверного программного обеспечения включен в установочный дистрибутив сервера приложения АС и представляет собой программное обеспечение, в задачи которого входит:

- Сбор информации о версии и составе установленного серверного ПО;
- Подключение к серверу обновлений и загрузка обновлений системы при необходимости.
- Отключение все пользователей, работающих в системе (при их наличии), с отправкой им соответствующего сообщения.
- Установка обновлений и проверка работоспособности нового серверного программного обеспечения. В случае возникновения внештатных ситуаций - выполнение восстановления предыдущей работоспособной версии серверного ПО и отправка сообщения серверу обновлений о внештатной ситуации.
- Протоколирование выполняемых операций локально и в журнале на сервере обновлений.

Конфигурирование клиента обновлений серверного программного обеспечения не требуется.