Ивановский государственный энергетический университет
Центр по проектированию и повышению надёжности электрооборудования

Программный комплекс «Диагностика+» версия 7.6

Руководство администратора

Иваново, 2024

Статус документа

Программный комплекс «Диагностика+». Веб-версия 7.6. Руководство администратора.

Центр по проектированию и повышению надёжности электрооборудования (ЦППНЭ) федерального государственного бюджетного образовательного учреждения высшего образования «Ивановский государственный энергетический университет имени В.И. Ленина» (ИГЭУ).

Документ содержит: описание архитектуры программного комплекса Диагностик+, инструкции по установке и настройке программного комплекса и программного окружения, инструкции по созданию резервных копий и восстановлению БД, описание управления пользователями и их правами доступа, описание интерфейса.

Оглавление

Термины определения и сокращения 5
Введение 7
Варианты поставки системы Диагностика+ конечному пользователю 8
Архитектура 9
Стандартная версия 9
Корпоративная версия 10
Техническое обеспечение 10
Веб-клиент 10
Клиент Администратора (Клиент GUI) 10
Веб-сервер 11
Сервер БД 11
Системное и базовое программное обеспечение 11
ПО сервера БД (версия стандарт) 12
ПО клиента (версия стандарт) 12
ПО, используемое на серверах (версия корпоративная) 13
ПО, используемое на веб-клиенте 13
ПО, используемое на клиенте Администратора 14
Установка Системы диагностики 15
Настройка ПО 16
Настройка СУБД Firebird 4.0 16
Настройка сетевого экрана на севере 16
Примеры настроек брандмауэра для различных версий Windows 18
Настройка сетевого экрана на клиенте 20
Резервирование базы данных 21
Создание резервных копий 21
Отличия в работе механизма резервного копирования 21
Восстановление из резервной копии 22
Полезные ссылки 22
Управление доступом 23
Узлы репликации 24
Создание и редактирование групп 25
Создание и редактирование пользователей 27
Порядок проверки прав доступа и права по умолчанию 28
Права доступа для объектов 29
Рекомендации по базовым настройкам доступа 30
Внешняя авторизация 31
Страница состояния системы 33
Глобальные настройки 35
[UserSetup] 35
[Decimal] 35

[Options] 35
[DB] 36
[ADServer] 36
[Prompts] 36
[Display] 36
[WebUI] 36
Типичные сообщения об ошибках 38

Термины определения и сокращения

В настоящем документе использованы термины и определения, предусмотренные ГОСТ 20911-89 [1] и ГОСТ 27.002-89 [2]. Кроме того, использован ряд терминов и определений, не предусмотренных указанными ГОСТ:

Термин	Определение
Диагностическая экспертиза	Автоматизированная процедура экспертной системы, анализирующая значения параметров объекта с целью установления его состояния
Единица оборудования	Отдельный объект, техническое обслуживание и ремонт которого выполняются независимо
Информационный объект	Описание некоторой сущности (реального объекта, явления, процесса, события) в виде совокупности логически связанных информационных элементов – реквизитов (свойств)
Класс информационных объектов	Совокупность информационных объектов с одинаковым набором свойств
Класс состояния оборудования	Совокупность объектов оборудования, выделенных по его техническому состоянию
Нормативно-справочная информация	Постоянные и условно-постоянные справочники, классификаторы
Параметр	Паспортная характеристика оборудования либо характеристика, получаемая в ходе диагностики или осмотра оборудования (физическая величина, в единицах измерения, используемых для измерения этой физической величины), влияющая на состояние оборудования либо на состояние ее компонента
Справочник	Логически-независимый элемент НСИ, описывающий совокупность условно-постоянной информации определенного вида (материалы, оборудование, контрагенты и т.п.)
Техническое состояние объекта	Состояние, которое характеризуется в определенный момент времени, при определенных условиях внешней среды значениями параметров, установленных в технической документации на объект. Техническое состояние отражают значения индекса технического состояния и класс состояния оборудования

Ниже приводятся сокращения, использованные в Документе:

Сокращение	Определение
БД	База данных
МЭС	Магистральные или межсистемные электрические сети
НСИ	Нормативно-справочная информация
ПК	Программный комплекс
ПО	Программное обеспечение
РЭС	Район электрических сетей
СУБД	Система управления базами данных
ЭС	Экспертная система
Jasig CAS	(Central Authentication Service) - сервер аутентификации
SSO	(Single Sign-On) – технология единого входа, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации
GUI	(Graphic User Interface) – графический интерфейс пользователя. В случае системы Диагностика+, интерфейс приложения PDP.exe
WebUI	(Web User Interface) – веб-интерфейс. Предусматривает работу с системой через совместимый браузер.

Введение

Программный комплекс (ПК) предназначен для оценки технического состояния электрооборудования энергопредприятий.

ПК состоит из двух подсистем:

- подсистемы Пользователя;
- подсистемы Разработки и администрирования.

Данный документ рассматривает работу подсистемы Разработки и администрирования, как основной инструмент Администратора.

Варианты поставки системы Диагностика+ конечному пользователю

Существует два варианта поставки системы конечному пользователю:

- Диагностика+ стандарт (далее «стандартная версия»);
- Диагностика+ корпоративная (далее «корпоративная версия»).

Стандартная версия предназначена для работы небольшого количества пользователей преимущественно с использованием графического интерфейса пользователя. Веб-интерфейс может использоваться для работы, но отдельного веб-сервера не предусмотрено и в качестве него используется экземпляр приложения PDP.exe.

Корпоративная версия предназначена для крупных предприятий и организаций с использованием исключительно веб-интерфейса. Графический интерфейс используется исключительно администратором в редких случаях для решения проблем, если это невозможно выполнить через веб-интерфейс.

Все различия в настройке и администрировании систем описаны в соответствующих разделах настоящего руководства. Если не указано иное, то подразумевается, что описанная процедура администрирования и настройки аналогична для всех вариантов системы Диагностика+.

Архитектура

Архитектура ПК Диагностика+ зависит от поставляемой версии.

Стандартная версия

Стандартная версия имеет двухуровневую архитектуру насыщенного клиент-серверного приложения. Уровень данных представлен сервером БД, а прикладной уровень – десктопными персональными компьютерами, подключёнными к локальной сети предприятия (рис. 1).

Эти два уровня могут быть дополнены третьим – уровнем веб-клиента. Роль веб-сервера в этом случае будет играть экземпляр толстого клиента (PDP.exe).

Подсистемы Пользователя (Разработчика) и Администратора не выделяются в данной версии. Пользователи, Администраторы и Разработчики могут использовать как Клиент GUI, так и Веб-браузер.

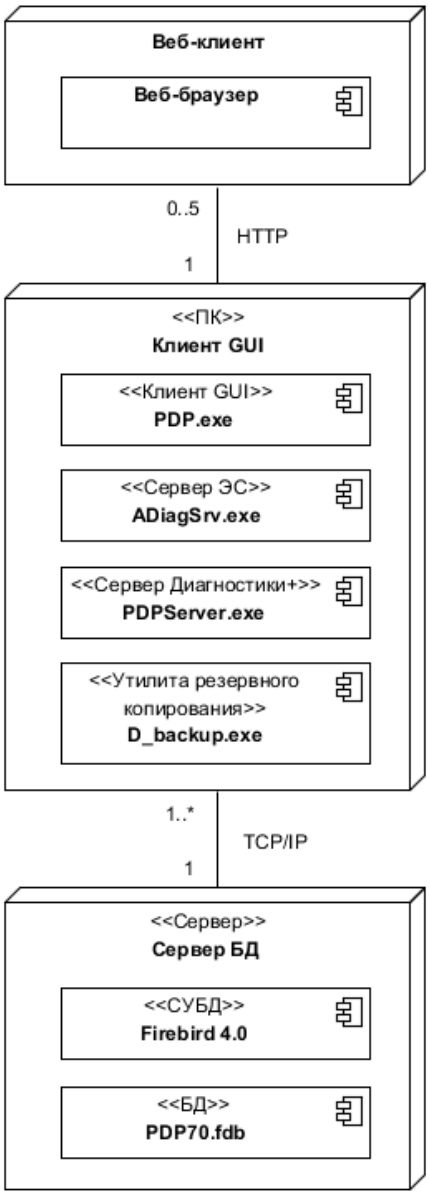


Рис. 1. Диаграмма развертывания для версии «Стандарт»

Корпоративная версия

В корпоративной версии совмещены трёхуровневая архитектура типичного веб-приложения с тонким клиентом и двухуровневая архитектура насыщенного клиент-серверного приложения (рис. 2).

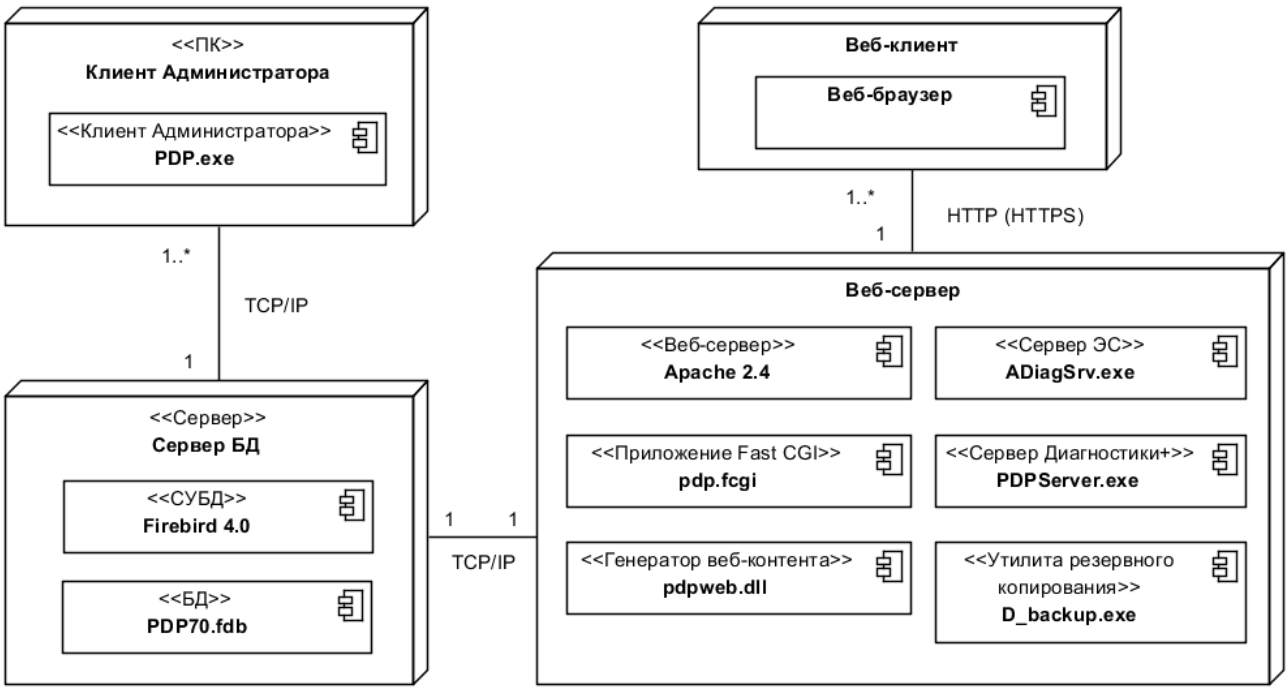


Рис. 2. Диаграмма развертывания для версии «Корпоративная»

В корпоративной версии можно выделить подсистему Пользователя и подсистему Разработчика и Администратора, так как Пользователи работают только через веб-браузер, а Администраторы могут пользоваться и толстым клиентом Администратора (PDP.exe), и веб-интерфейсом.

Техническое обеспечение

Веб-клиент

К клиентскому компьютеру предъявляются следующие требования: может использоваться любая конфигурация, поддерживающая работу рекомендованных браузеров и просмотр документов в формате pdf, odt, xslx и docx (см п. «ПО веб-клиента»).

Клиент Администратора (Клиент GUI)

Минимальные требования:

Процессор: x86-совместимый процессор;

ОЗУ: 2 ГБ;

ПЗУ: 6 ГБ свободного места;

Скорость передачи по локальной сети: 100 Мбит/с.

Веб-сервер

Расчитывается индивидуально и зависит от нагрузки (количества одновременно работающих пользователей и количества одновременно выполняемых HTTP-запросов).

Минимальные требования (20 условных одновременно работающих пользователей):

Процессор: x86, 4 ядра, от 1,5 ГГц;

ОЗУ: 4 ГБ;

ПЗУ: 50 ГБ свободного места;

Скорость передачи по локальной сети: 100 Мбит/с.

Сервер БД

Минимальные требования:

Процессор: 2 x 2 ГГц;

ОЗУ: 2 ГБ;

ПЗУ: 5 ГБ (для размещения БД и СУБД, без учета размещения файлов с термограммами, схемами и фотографиями).

Системное и базовое программное обеспечение

В этом разделе описаны требования к системному и базовому программному обеспечению (ПО).

Состав компонентов ПО и связи между ними показаны на диаграммах компонентов (рис. 3 – 4).

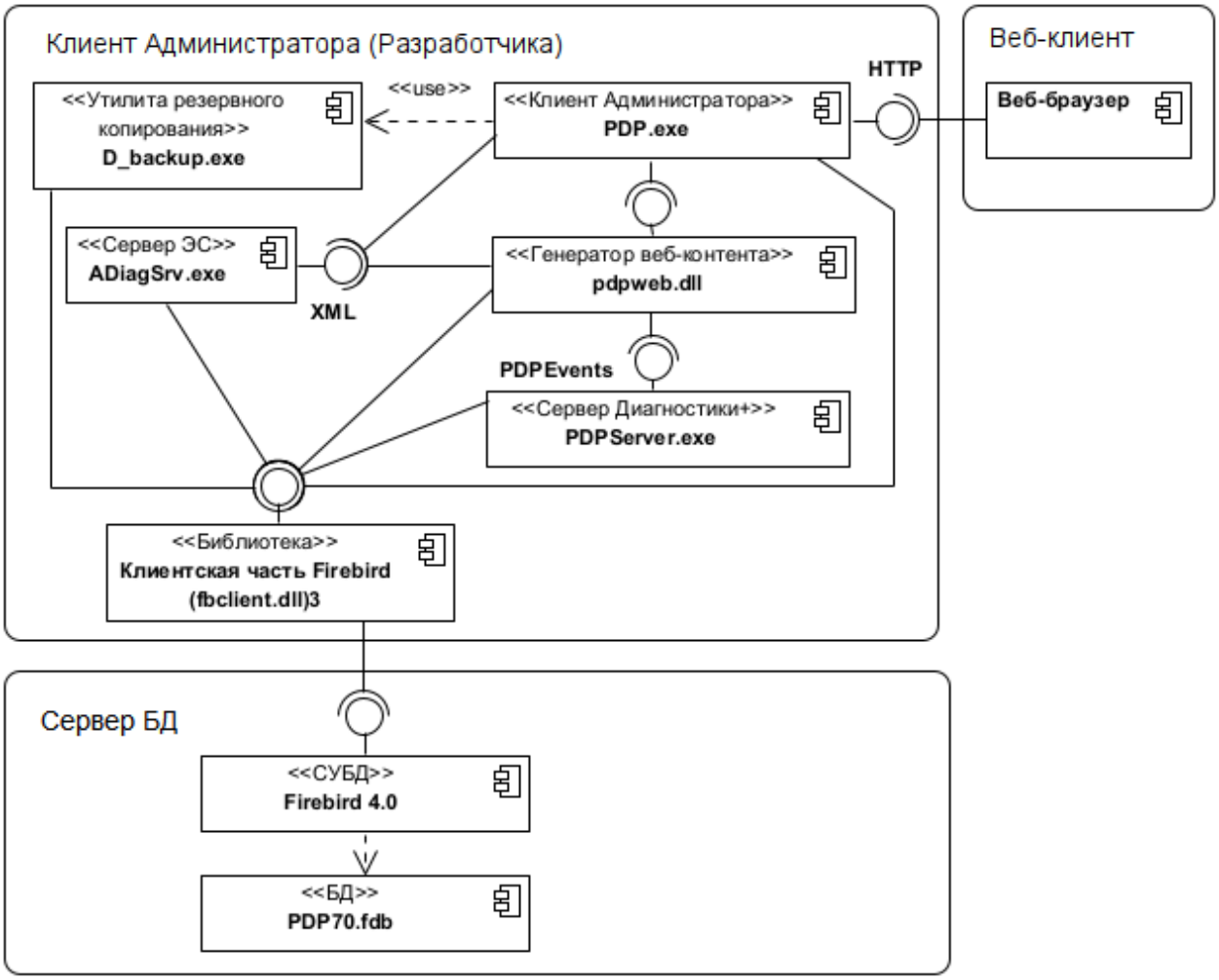


Рис. 3. Диаграмма компонентов для версии «Стандарт»

ПО сервера БД (версия стандарт)

1. В качестве операционной системы на Сервере БД используется Microsoft Windows Server 2012 R2 или новее (32bit или 64bit) либо Microsoft Windows 7.0 или новее.

2. В качестве СУБД используется FireBird версии 4.0.

ПО клиента (версия стандарт)

На клиентском компьютере должны быть установлены:

1. Операционная система Microsoft Windows 7 или новее.

2. Подсистема Администратора и Разработчика (предоставляется программа установки подсистемы).

3. Microsoft Word 2010 (и более новый), Microsoft Exel 2010 (и более новый).

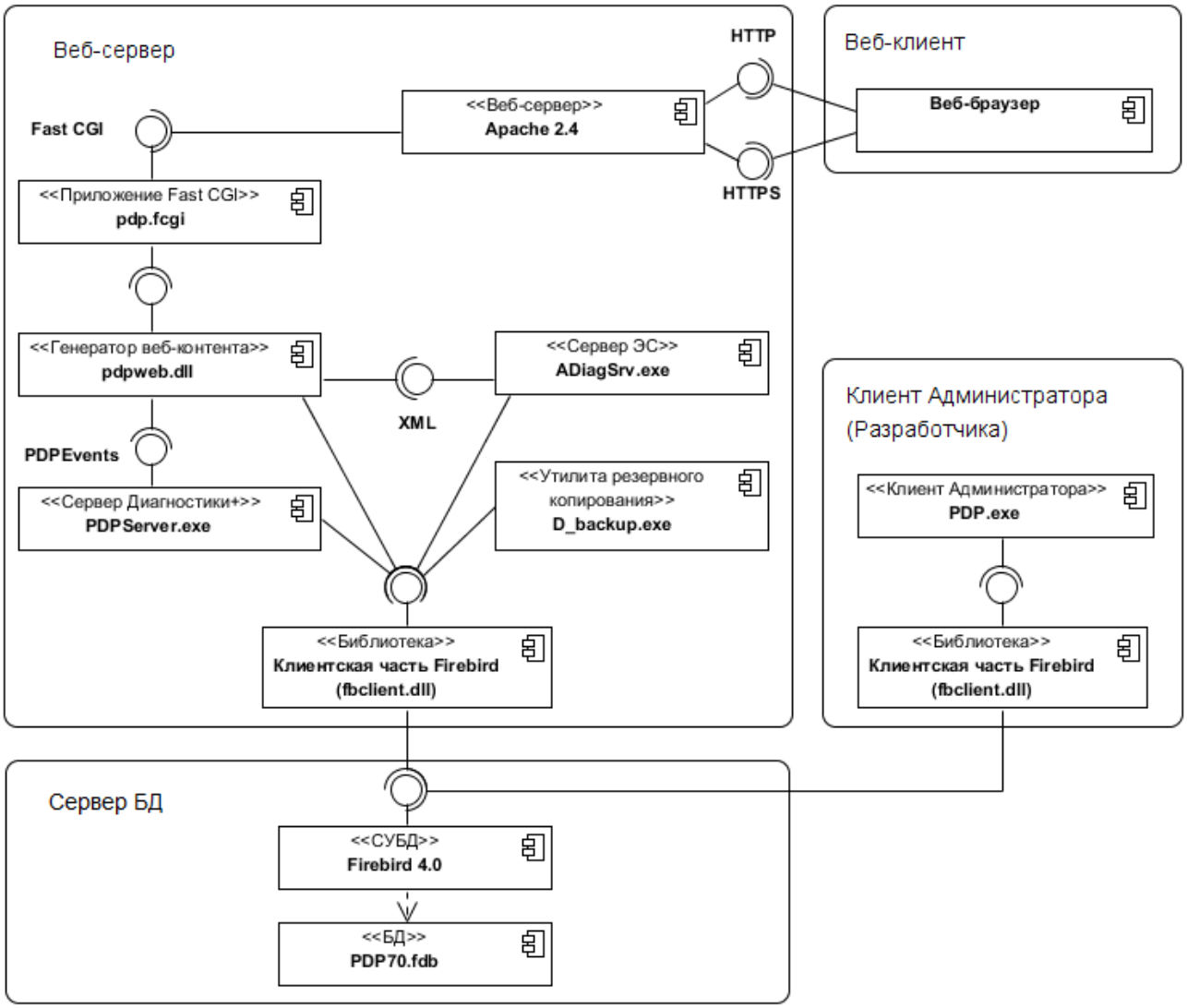


Рисунок 4 - Диаграмма компонентов для версии «Корпоративная»

ПО, используемое на серверах (версия корпоративная)

1. В качестве операционной системы на всех серверах используется Microsoft Windows Server 2012 R2 или новее 32bit или 64bit.

2. В качестве веб-сервера используется Apache версии 2.4.

3. В качестве СУБД используется FireBird версии 4.0.

4. Серверная часть Системы диагностики (предоставляется программа установки Системы).

ПО, используемое на веб-клиенте

На клиентском компьютере должны быть установлены:

1. Веб-браузеры:

- FireFox версии 63 и выше,

- Opera версии 41 и выше,
- Google Chrome версии 54 и выше,
- Safari версии 12 и выше,
- Microsoft Edge версии 79 и выше,
- Yandex версии 23 и выше.

2. Средства просмотра отчётов один набор из списка:
   - LibreOffice Community версии 7.5 и выше (распространяется бесплатно, https://ru.libreoffice.org/),
   - Microsoft Word 2010 (и более новый) и Microsoft Excel 2010 (и более новый).

ПО, используемое на клиенте Администратора

На клиентском компьютере Администратора должны быть установлены:

1. Операционная система Microsoft Windows 7 или новее.

2. Подсистема Администратора и Разработчика (предоставляется программа установки подсистемы).

Установка Системы диагностики

Система поставляется в виде единого инсталлятора, позволяющего установить все компоненты системы вместе или в отдельности (см. Руководство по установке ПК «Диагностика+»). Инсталлятор обеспечивает следующие функции:

- установка сервера Firebird 4.0;
- автоматическая конфигурация сервера Firebird 4.0;
- автоматическая конфигурация брандмауэра Windows (открытие портов необходимых для работы сервера и клиента);
- установка серверной части Диагностики+;
- установка web-сервера Apache 2.4 (для версии корпоративная);
- автоматическая настройка сервера Apache 2.4 для работы с web-модулем Диагностики+ (для версии корпоративная);
- установка клиентского графического интерфейса.

Настройка ПО

Настройка СУБД Firebird 4.0

Системой диагностики используется СУБД Firebird версии 4.0. Наличие запущенного и работоспособного сервера необходимо для работы программы. Сервер Firebird устанавливается автоматически инсталлятором системы, однако в некоторых случаях требуется ручная установка. В случае использования брандмауэров (фаерволов) необходима их правильная настройка. В зависимости от вариантов установки системы сервер Firebird может находиться либо на одной машине с веб-сервером, либо на сервере, специально выделенном для базы данных. По умолчанию SQL-сервер Firebird устанавливается в качестве службы и запускается автоматически вместе с операционной системой.

Настройка сетевого экрана на севере

На сервер БД необходима настройка сетевого экрана (брандмауэра, фаервола).

Сервер Firebird использует для работы протокол TCP/IP. По умолчанию используются следующие порты:

3050 – порт сервера, этот порт должен быть открыт для службы сервера на машине, где установлен сервер.

3060 – порт обработки событий, этот порт должен быть открыт на машине клиента (только для версии «стандарт»).

Если используются другие номера портов – настройки должны быть изменены соответствующим образом.

Для версии «стандарт», чтобы сервер Firebird мог свободно слушать порт 3050 и принимать входящие подключения от клиентов, серверный брандмауэр должен быть настроен следующим образом:

- локальный порт 3050
- направление входящие
- протокол TCP
- приложение fbserver.exe

Для версии «корпоративная», чтобы пользователи могли иметь доступ к серверу через веб-интерфейс по используемому по умолчанию порту 80 (незащищенное соединение), либо порту 443 (защищенное соединение) серверный брандмауэр должен быть настроен следующим образом:

- локальный порт 80 либо 443;
- направление входящие;
- протокол TCP.

Также для клиента GUI системы Диагностика+ в версии «стандарт» необходима настройка брандмауэра на клиенте. Клиентский брандмауэр должен быть настроен следующим образом:

- локальный порт 3060;
- направление входящие;
- протокол TCP;
- приложения pdp.exe и PDPServer.exe.

В случае если сервер баз данных расположен на отдельном сервере (для версии «корпоративная»), то на компьютере, где установлена серверная часть Диагностики+ брандмауэр должен быть настроен следующим образом:

- локальный порт 3060
- направление входящие
- протокол TCP
- приложения pdp.exe и PDPServer.exe

В зависимости от используемого брандмауэра способ задания настроек будет отличаться. Дополнительные параметры - такие как IP адрес сервера и клиента, удалённый порт и т.д. настраиваются администратором в зависимости от структуры сети предприятия и требований к безопасности. Рекомендуемые настройки для пакетного брандмауэра следующие:

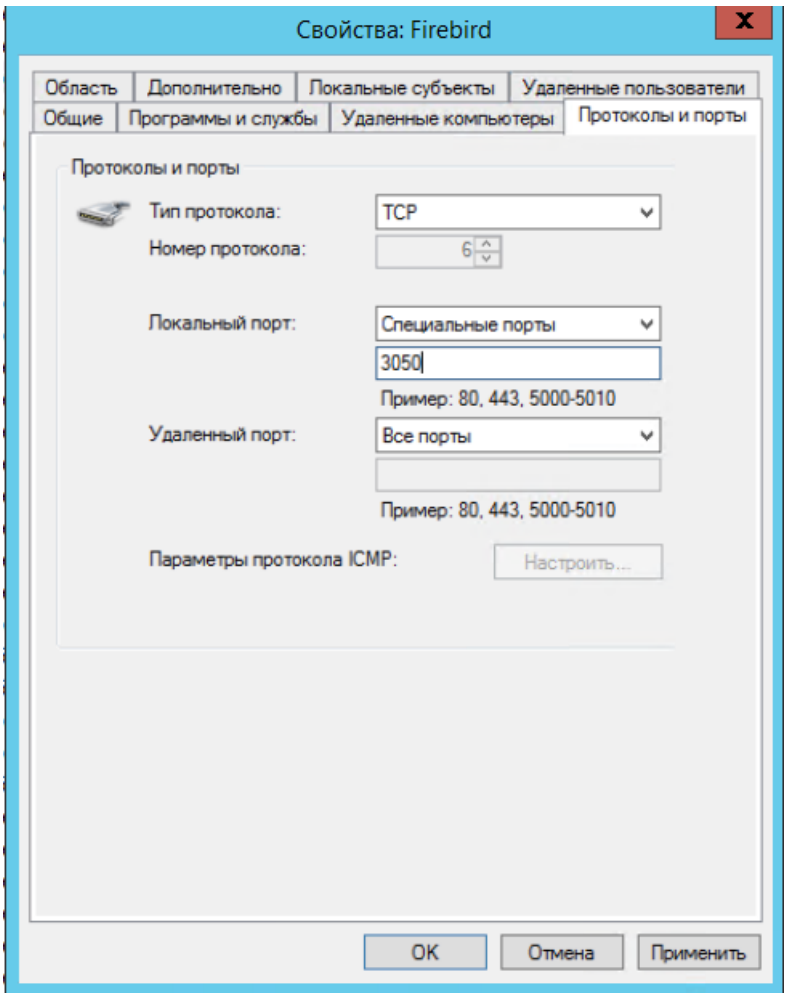
- локальный IP адрес любой
- удалённый IP адрес любой
- удалённый порт любой

Подробности настроек брандмауэра смотрите в документации Вашей операционной системы.

Если у Вас между сервером и клиентом расположено сетевое оборудование, включающее в себя функции брандмауэра, Вам так же необходимо на нём разрешить трафик по портам 3050 и 3060. Для этого смотрите документацию к Вашему сетевому оборудованию.

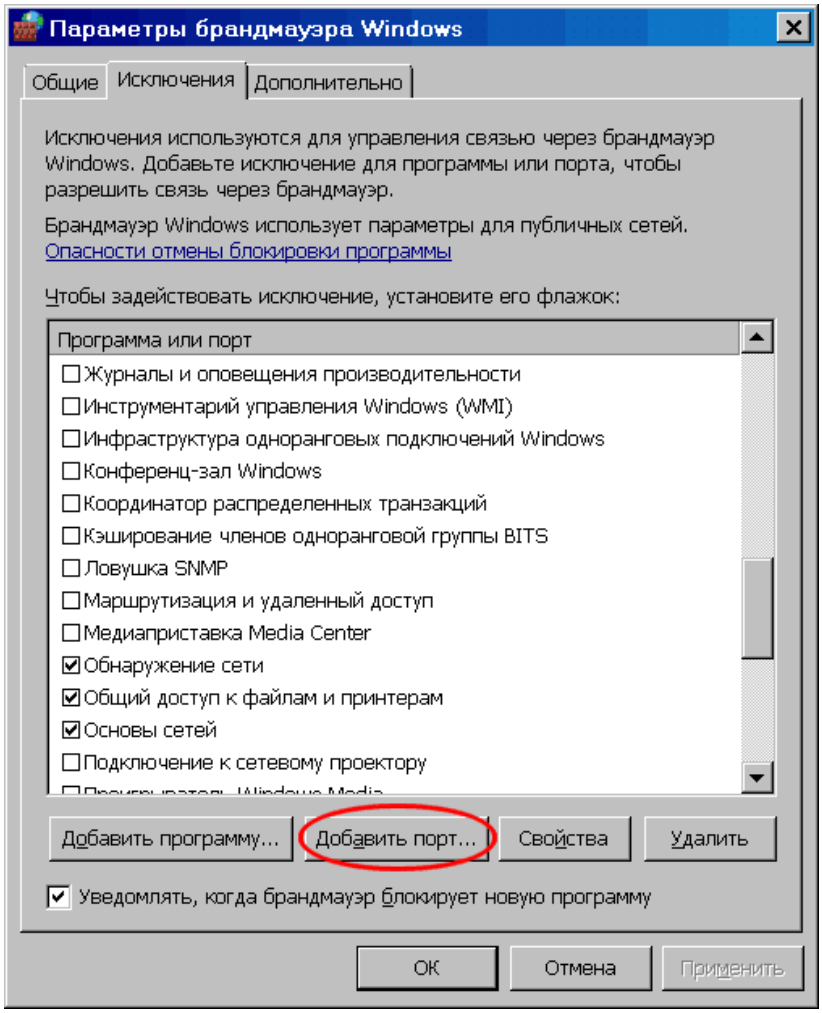
Примеры настроек брандмауэра для различных версий Windows

Windows 2012 Server правило для Firebird (версия «стандарт»)

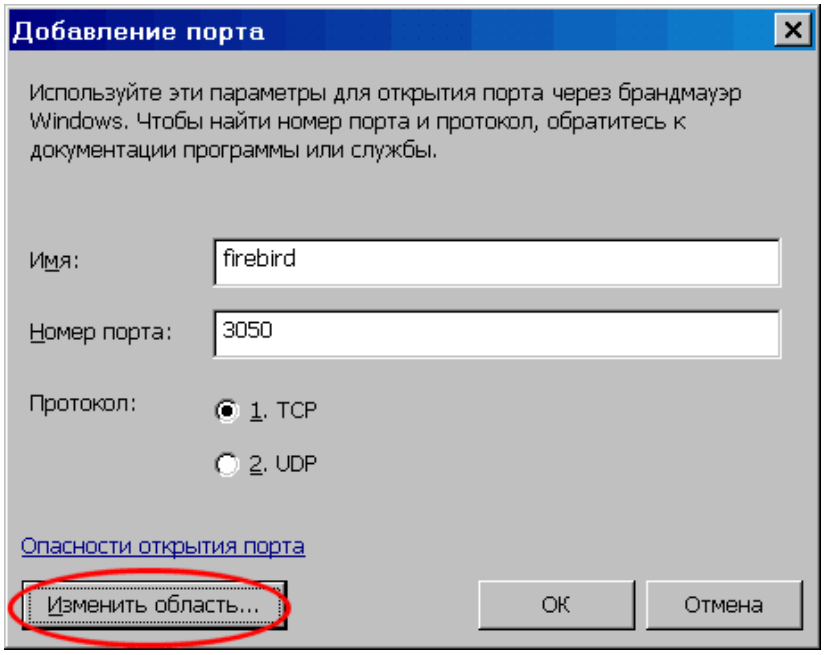


Windows 7

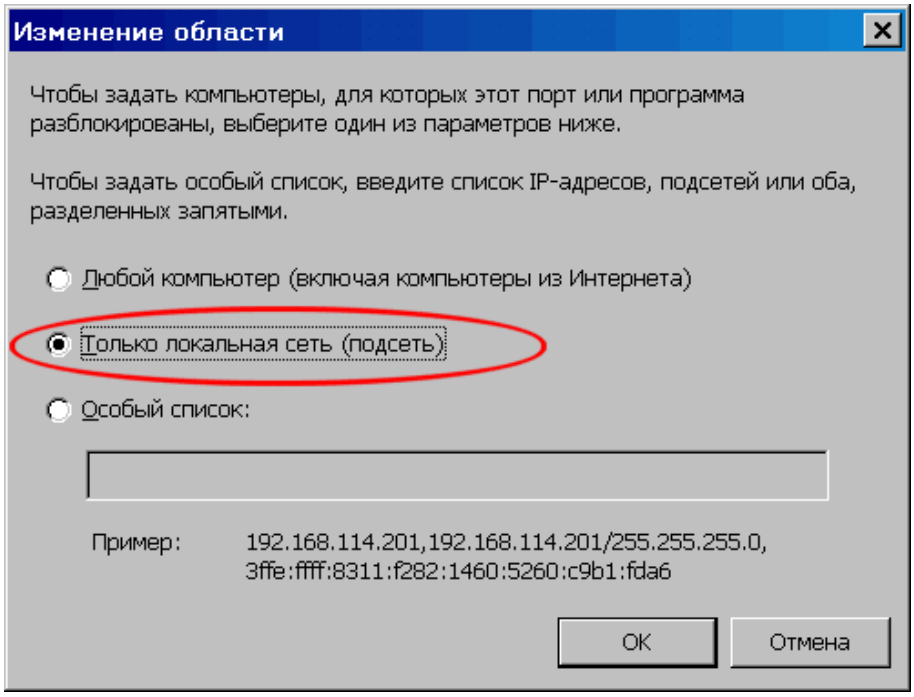
Откройте брандмауэр Windows. Нажмите кнопку "Добавить порт".



Введите имя исключения firebird, номер порта 3050 и протокол TCP.



Нажмите кнопку "Изменить область".



Выберите "Локальная сеть", чтобы разрешить доступ к серверу из локальной сети или "Особый список" и укажите IP-адреса которые будут использоваться для клиентов системы Диагностика+

Настройка сетевого экрана на клиенте

Как правило, брандмауэр на клиентских машинах не препятствует установке исходящих соединений в локальной сети. Однако, если Ваш брандмауэр блокирует на клиенте исходящие соединения на порт 3050 удалённого сервера – Вам необходимо настроить его следующим образом:

- удалённый порт 3050
- локальный порт любой
- направление исходящие
- протокол TCP

В зависимости от используемого брандмауэра способ задания настроек будет отличаться.

Резервирование базы данных

Создание резервных копий

Диагностика+ имеет встроенный механизм создания резервных копий. В зависимости от варианта поставки механизм резервирования отличается.

Резервируется база данных системы (по умолчанию pdp70.fdb). Резервная копия базы имеет префикс "pdp_".

Резервные копии имеют 4 уровня и затираются "по кругу":

- ежедневные - создаются каждый день - хранятся неделю (файлы именуются pdp_D1.fbk - pdp_D7.fbk, где цифра - день недели, первый день - понедельник);
- еженедельные - создаются каждую неделю - хранятся месяц (файлы именуются pdp_W1.fbk - pdp_W5.fbk, где цифра - номер недели в месяце);
- ежемесячные - создаются каждый месяц - хранятся год (файлы именуются pdp_M1.fbk - pdp_M12.fbk, где цифра - номер месяца);
- ежегодные - создаются каждый год - не удаляются (файлы именуются pdp_Y20xx.fbk).

Механизм автоматического резервирования позволяет настроить каталоги для хранения резервных копий БД. Это осуществляется через GUI при помощи диалогового окна "Системные настройки" Настройка|Системные настройки, группа полей "Резервные копии".

Внимание! Пути - локальные пути сервера БД.

"Общий каталог" - указывает путь для всех уровней резервных копий. Все копии сохраняются в него, если для каждого уровня не указан отдельный каталог. Если поле "Общий каталог" не заполнено, то резервные копии сохраняются в каталог по умолчанию BACKUPS, который расположен в каталоге, где находится сама база данных. Различные каталоги для резервных копий каждого уровня можно задать индивидуально в соответствующих полях.

Рекомендуем периодически проводить архивирование резервных копий средствами операционной системы или вручную.

Если система резервного копирования начинает работать с ошибками, то выдаётся соответствующее предупреждение и работа Диагностики+ приостанавливается.

Отличия в работе механизма резервного копирования

Для версии «стандарт» механизм кооперативный, т.е. резервирование базы данных выполняет первый клиент, обнаруживший необходимость создания резервной копии.

Для версии «корпоративная» резервирование базы данных осуществляется по расписанию с использованием планировщика заданий Windows Server. Задание создается автоматически инсталлятором системы. Резервирование производится в 4:00 каждого дня. В случае, если необходимо установить другое время резервирования, то следует отредактировать соответствующее задание в планировщике заданий.

Восстановление из резервной копии

Необходимость восстановления базы данных из резервной копии возникает, как правило, в двух случаях:

1) ошибочные изменения, сделанные пользователем;

2) повреждение базы данных.

В первом случае возможно восстановить базу из резервной копии, чтобы вернуться к её предыдущему состоянию. При этом может быть потеряна часть данных, которые были внесены позже.

Внимание! Советуем пользоваться этой функцией крайне аккуратно, только когда восстановление данных вручную невозможно!

Для выполнения восстановления из резервной копии Вы можете воспользоваться утилитой restorer.exe, входящей в комплект поставки. Подробно читайте файл справки restorer.chm

Случаи повреждения базы данных вызываются, обычно, аппаратными причинами. В этом случае в первую очередь нужно установить причину повреждения базы данных, устранить её и только после этого восстанавливать резервную копию БД. Восстановление должно проводится при помощи штатных средств сервера Firebird 4.0. Подробно читайте документацию сервера.

Внимание! В случае повреждения базы данных немедленно обратитесь к разработчикам системы Диагностика+!

Полезные ссылки

- Документация Firebird http://www.firebirdsql.org/index.php?op=doc
- Утилита резервного копирования (англ) http://www.firebirdsql.org/manual/gbak.html#gbak-intro
- Утилита резервного копирования (рус) http://www.ibase.ru/devinfo/gbak.htm

Управление доступом

Администратор может ограничивать доступ отдельных Пользователей и групп Пользователей к данным. Управление доступом осуществляется как по видам объектов, так и по дереву доступа, отражающему территориальное размещение объектов.

В Системе существуют 4 уровня прав доступа:

1. запрещено - пользователь не видит этих данных;
2. чтение - пользователь видит данные, но не может их изменять;
3. чтение/изменение (редактирование) - пользователь видит данные и может изменять значения полей объектов и испытаний, но не может создавать новые или удалять объекты или испытания;
4. полный доступ - пользователь видит данные и может изменять значения полей объектов и испытаний, может создавать новые объекты или испытания и удалять их.

Пользователи должны быть включены в группы доступа. Права доступа назначаются для групп доступа, а не для отдельных пользователей. Все пользователи группы имеют одинаковые права доступа. Редактировать пользователей и группы можно только через веб-интерфейс на странице «Группы». Редактировать, добавлять и удалять учетную запись пользователя могут члены групп «администраторы» (любого пользователя системы) и «администраторы узла» (только на своём узле).

Пользователя может сам редактировать свою учетную запись (ограниченно). Подробнее см. «Руководство пользователя».

Пользователь может принадлежать к нескольким группам. В этом случае для определения прав доступа пользователя выбирается максимальный уровень прав из всех групп, в которые он включён.

Учетная запись пользователя может находится в двух состояниях «активный» и «заблокированный». Заблокированный пользователь не может войти в систему, но вся информация учетной записи, включая все настройки и историю, сохраняется.

В систему встроено 5 групп доступа, с определённым набором прав, которые менять нельзя:

1. **Администраторы**. Имеют полный доступ ко всем объектам и таблицам, могут менять любые настройки (за исключением запретов на уровне узла см. ниже).
2. **Редактирование**. Имеют полный доступ к объектам и таблицам, не могут менять настройки, не могут редактировать словари.
3. **Чтение**. Могут видеть все таблицы и объекты, но не могут их изменять.
4. **Администраторы узла**. Пользователям этой группы предоставляется ограниченный административный доступ к определённому узлу администрирования. Принадлежность пользователя к узлу задаётся в учётной записи конкретного пользователя.
5. **Редактирование словарей**. Только пользователи этой группы и «Администраторы» могут редактировать словари.

Права доступа в Диагностике+ устанавливаются на 3 вида сущностей:

1) узлы репликации;
2) объекты;
3) таблицы.

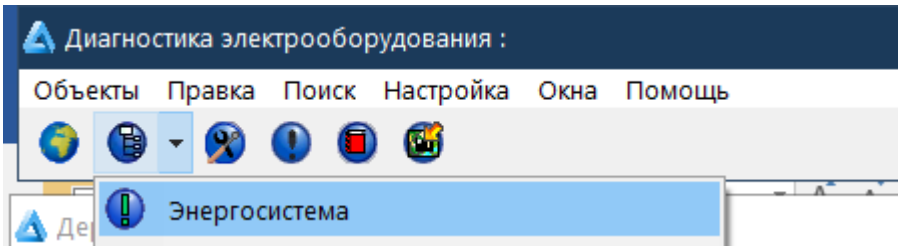
Создание пользователей и групп доступа возможно только через веб-интерфейс.

Узлы репликации

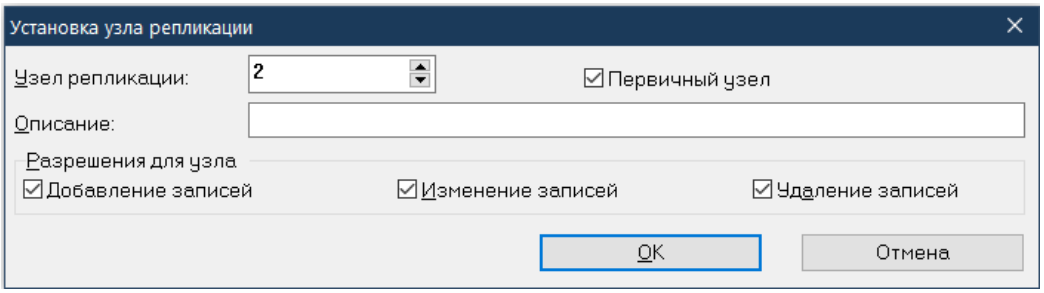
В текущей версии системы узлы репликации не используются непосредственно для репликации данных между распределёнными базами данных. Вместо этого узлы репликации предназначены для делегирования части административных прав от глобальных администраторов – администраторам узла. Это применяется в случае, если организация, эксплуатирующая систему, имеет сложную организационную структуру. Термин «узел репликации» используется для обратной совместимости и по историческим причинам. В системе всегда задан, как минимум, один узел репликации. Узел с номером 1 ВСЕГДА связан с корневым узлом главного дерева и является синонимом всей организации, эксплуатирующей систему Диагностика+.

Назначение и удаление улов репликации выполняется глобальным администратором через интерфейс GUI.

Для назначения узла откройте главное дерево – оно помечено восклицательным знаком.



В дереве объектов выделите необходимый узел и в контекстном меню выберите пункт «Назначить узел репликации». В диалоговом окне укажите параметры узла и нажмите «ОК».



Узел репликации имеет следующие параметры:

- узел репликации – номер узла в диапазоне 2-99;
- описание – текстовое описание узла, например «Филиал №2».

Остальные параметры не используются. Все флаги должны быть включены.

Узлы дерева, связанные с узлами репликации, будут иметь пометку [UID=(x)], где x -номер этого узла.

Создание и редактирование групп

Для этого перейдите на страницу Группы ().На этой странице Вы можете видеть список групп. Группы могут быть **глобальными**, либо принадлежать какому-либо узлу репликации, включая корневой узел № 1. Используя выпадающий список в заголовке таблицы можно отфильтровать необходимые группы с разных узлов.

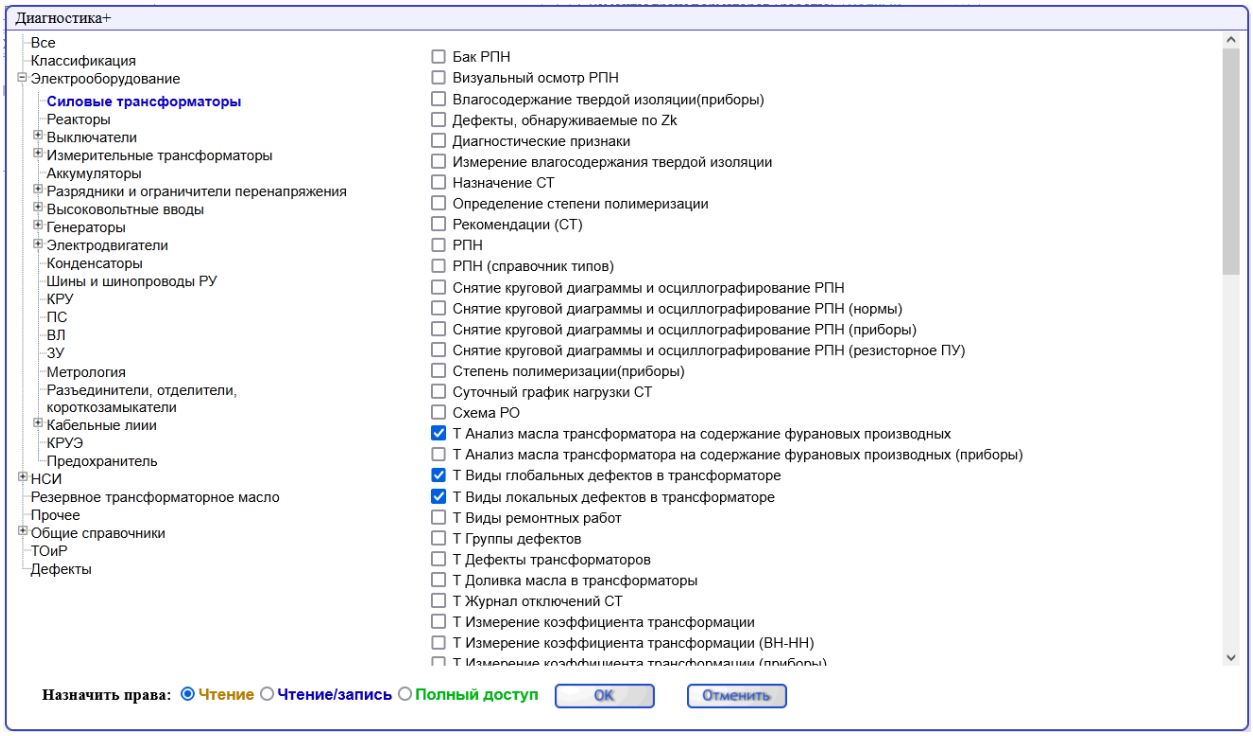
Встроенные группы нельзя редактировать, можно только просмотреть пользователей этой группы. Для этого используйте кнопку  .

Для добавления группы нажмите  , для редактирования  в строке выбранной группы. Добавление и редактирование не отличаются. Необходимо заполнить следующие параметры для группы:

- узел – узел репликации, где расположена группа;
- название – наименование группы;
- разрешения для таблиц

Внимание! Настройка разрешений для таблиц на уровне групп не рекомендуется, так как это не позволяет осуществить гибкое управление доступом. Данная настройка считается **устаревшей** и вскоре будет удалена! Рекомендуется пользоваться управлением доступом на уровне объектов.

Для редактирования разрешения для таблиц нажмите кнопку  в колонке “разрешения для таблиц”. В всплывающем окне отметьте выберите группу таблиц в дереве, для которых Вы хотите произвести настройку. Отметьте те таблицы, доступ к которым Вы хотите настроить. В нижней части окна выберите уровнь доступа для выбранных таблиц и нажмите “ОК”.



Выбранные таблицы будут добавлены в список «разрешения для таблиц».

Для того чтобы удалить таблицу из списка отметьте её (или несколько) и нажмите  .

Чтобы изменить уровень доступа для таблицы, которая уже присутствует в списке выберите соответсвующее значение из выпадающего списка. Если Вы хотите изменить разрешения сразу для нескольких таблиц – отметьте несколько из них и при помощи выпадающего списка на одной из выбранных таблиц установите разрешения сразу для всех из них.

Чтобы выбрать сразу все таблицы – используйте флажок в заголовке колонки. С его помощью можно выбрать или снять выбор сразу для всех таблиц.

Нажмите «сохранить» чтобы сохранить изменения или «сбросить» чтобы вернуться к последнему сохраненному состоянию.

Так-же на странице редактирования группы Вы можете посмотреть список всех пользователей группы и перейти к редактированию любого из них через гиперссылку. По

умолчанию члены группы скрыты. Чтобы отобразить список пользователей используйте кнопку  .

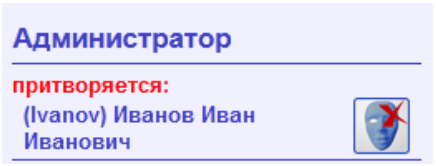
Создание и редактирование пользователей

Для этого перейдите на страницу Пользователи ().На этой странице Вы можете видеть список пользователей.

Используйте кнопки для добавления редактирования и удаления соответствующих элементов.

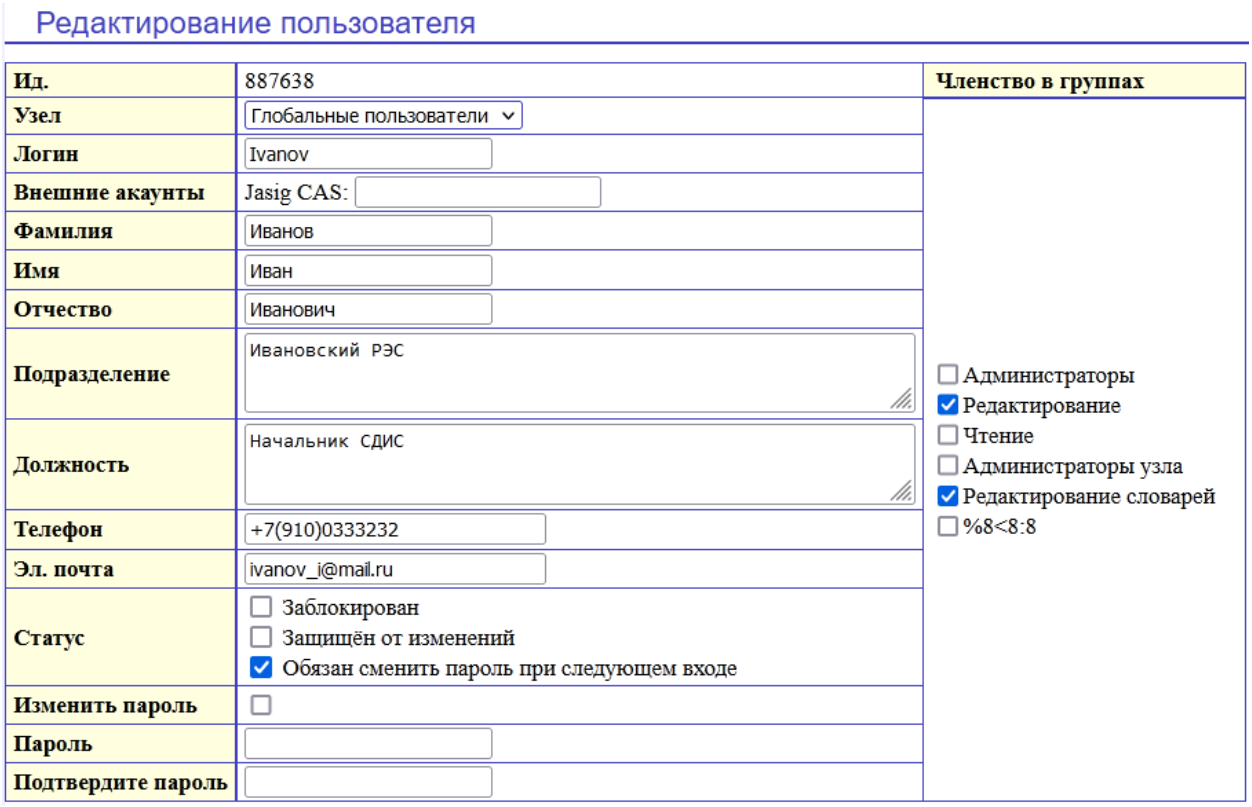
Внимание! Встроенных пользователей и группы нельзя изменять. Для них кнопки редактирования недоступны!

Используйте кнопку  для того чтобы притвориться выбранным пользователем. Этот режим удобен для тестирования прав доступа выбранного пользователя. В этом режиме интерфейс меняется с администраторского на пользовательский и все права доступа и настройки используются от выбранного пользователя. При этом история изменнеий, если таковые будут сделаны, будет сохранена для администратора, а не для того, кем он притворяется. В данном режиме в заголовке будет отображаться информация о режиме приворства. Например:



Для того чтобы выйти из режима притворства нажмите кнопку  .

На странице редактирования пользователя Вы можете задать значения для параметров пользователя, таких как: имя аккаунта, ФИО и задать для пользователя пароль и членство в группах безопасности.



Редактирование параметра «узел» доступно только глобальным администраторам. «Администраторы узла» могут редактировать только пользователей своего узла.

Для включения/исключения пользователя из групп безопасности установите галочки возле соответствующих значений.

Для задания пароля установите галочку "Изменить пароль" и введите в два поля значения нового пароля пользователя.

Чтобы изменить только учётные данные пользователя и не трогать пароль - отключите галочку "Изменить пароль". В этом случае пароль пользователя останется неизменным.

Чтобы заблокировать или разблокировать пользователя используйте галочку «заблокировать».

Чтобы запретить пользователю менять настройки своего профиля используйте галочку «защищён от изменений».

При помощи галочки «обязан сменить пароль при следующем входе» можно заставить пользователя обязательно сменить пароль.

Порядок проверки прав доступа и права по умолчанию

Права доступа к каждому конкретному объекту системы вычисляются в следующем порядке:

Проверяются разрешения для узла репликации. Если на уровне узла установлены права доступа для какой-либо таблицы, то все другие разрешения не могут их расширить.

Т.е. если на уровне узла репликации для таблицы CT1 (Хроматографический анализ) установлен уровень прав чтение, то все пользователи данного узла не смогут изменять эту таблицу, даже если на уровне объектов или таблиц они имеют более высокие права.

Проверяются разрешения на уровне таблиц. Из всех групп, в которые входит пользователь, выбирается наибольший уровень прав для конкретной таблицы. Если ни в одной из групп уровень доступа к таблице не указан явным образом, выбирается уровень доступа запрещено.

Проверяются разрешения на уровне объекта. Если для конкретного объекта права доступа установлены ЯВНО хотя бы для одной из групп, в которые входит пользователь (включая наследование от родительских узлов) то выбирается этот уровень разрешений, иначе используются разрешения на уровне таблиц (п. 2).

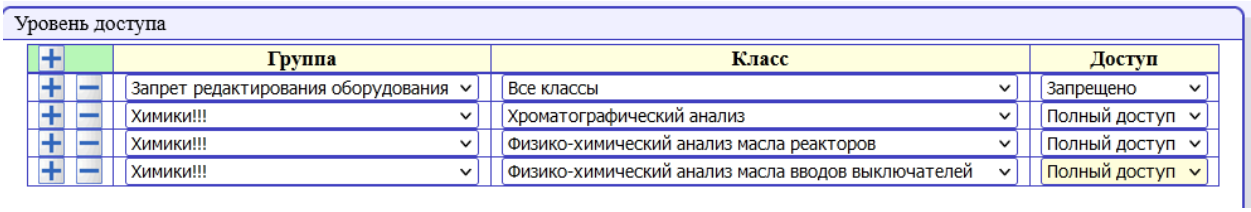
Ниже подробно описано как работать с различными видами прав доступа.

Права доступа для объектов

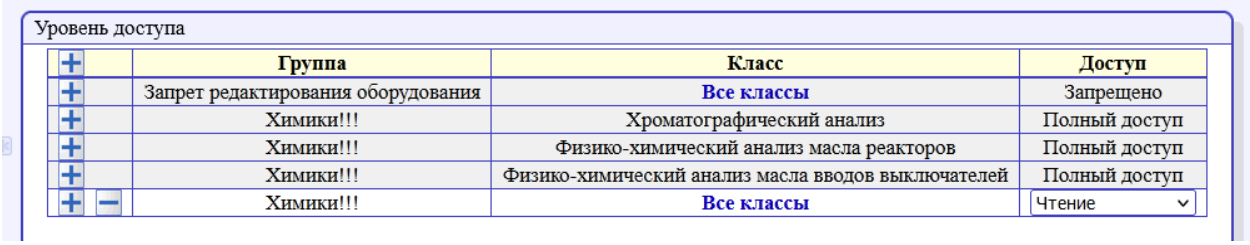
Администратор системы или администратор узла может назначить права доступа на определённые объекты системы. Права доступа наследуются по главному дереву. Объекты, расположенные под объектом, которому назначены права доступа получают те же самые разрешения. Наследуемые права доступа можно перекрывать, назначая расположенным ниже по иерархии объектам другие права. Права доступа могут быть назначены только из главного дерева.

Назначение прав доступа осуществляется через веб-интерфейс. Для этого откройте главное дерево из списка деревьев. Главное дерево помечено в списке значком  .

Выберите объект, для которого Вы хотите установить права доступа. Из меню пункт «Права». Откроется диалоговое окно, в котором Вы сможете назначить разрешения для групп доступа к этому объекту.



В этом окне перечислены группы и их права доступа к этому объекту. Серым цветом выделены наследуемые от родителей права доступа.



Чтобы изменить разрешение для группы: выберите необходимый уровень прав из выпадающего списка. Если в списке нет нужной группы - нажмите кнопку «Добавить» и выберите группу из списка доступных групп пользователей. Группа будет добавлена, и ей будут назначены полные права доступа. В колонке «класс» выберите класс объектов, которому Вы назначаете права. Таким образом все объекты, относящиеся к указанному классу, и находящиеся ниже по дереву относительно выбранного объекта получат эти права. Если Вы выберете «все классы» из списка, то права будут заданы для объекта любого класса, расположенного ниже по дереву.

После завершения редактирования нажмите кнопку «ОК» - доступ к этому и всем подчинённым ему объектам будет ограничен в соответствии с установленными разрешениями.

Рекомендации по базовым настройкам доступа

Мы рекомендуем для начала создать простую схему доступа как компромисс между простотой и безопасностью. В дальнейшем схему можно развить.

Предлагаем создать две группы (в каждом филиале):

1. Пользователи филиала. (например: "Пользователи Фил1")
2. Запрет изменения структуры. (например: "Запрет структуры Фил1")

Внимание! Дина имени группы 32 символа.

Первая группа нужна, чтобы дать пользователям доступ для редактирования, добавления и т.д. Вторая группа нужна, чтобы запретить пользователям менять структуру (удалять подстанции, РЭС, группа ПС и т.д.).

Для того чтобы организовать доступ администратор соответствующего узла или глобальный администратор должны сделать следующее:

1. Создать группы, указанные выше.
2. Включить в эти 2 группы всех пользователе филиала (кроме себя).
3. Зайти в дерево.
4. Открыть меню на узле своего МЭС и выбрать пункт "права".
5. В окне "Уровень доступа нажать кнопку "+".
6. Выбрать группу "Пользователи Фил1" класс "Все" доступ "полный доступ".
7. Снова нажмите кнопку "+" и выберите следующие классы (см на скриншоте). Для них выберите "чтение".

Таким образом будет предотвращена случайная порча орг. структуры пользователями. Администраторы филиалов будут по-прежнему иметь право полного доступа.

Внешняя авторизация

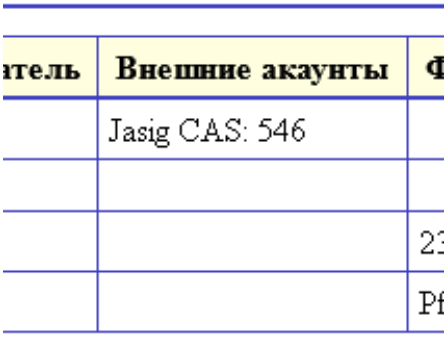
В Диагностике+ реализована система внешней авторизации, которая позволяет использовать для авторизации пользователей внешние источники. Внешняя авторизация реализуется при помощи модулей внешней авторизации и доступна только для пользователей веб-интерфейса. Модули внешней авторизации должны располагаться в каталоге cas корневого каталога программы. Каждый модуль представляет собой 1 или несколько подключаемых библиотек (зависит от реализации) и файл настроек, которой должен располагаться в том же каталоге, что и сам модуль. Администратор системы может выбрать способы авторизации на странице **Авторизация** (доступно из главного меню веб-интерфейса). Администратор может включать и выключать каждый из доступных способов авторизации.

Каждый модуль внешней авторизации настраивается через файл конфигурации. Убедитесь, что Вы правильно настроили выбранный модуль, перед тем как его включить! В противном случае вход в систему пользователей может стать невозможным. Конфигурация каждого отдельного модуля зависит от реализации.

Для того чтобы пользователь мог войти в систему с использованием модуля внешней авторизации - внешнее имя пользователя должно быть сопоставлено со встроенным именем пользователя (аккаунтом). Это необходимо для того чтобы назначить права и группы безопасности. Сопоставление происходит по следующему алгоритму:

- используется имя внешнего пользователя, назначенное для конкретного модуля авторизации;
- используется имя встроенного пользователя.

Сопоставить внешние имена можно через интерфейс управления пользователями. В списке пользователей в колонке внешние аккаунты отображаются доступные внешние модули авторизации и, если назначено, сопоставленное ему внешнее имя пользователя.



Изменять эти значения можно через интерфейс редактирования.

Внимание! Для того чтобы можно было сопоставлять внешнее имя пользователя - соответствующий модуль внешней авторизации должен быть установлен.

Решение проблем внешней авторизации

Возможно при использовании внешней авторизации вход систему станет невозможным по следующим причинам:

- недоступен сервис авторизации;
- неправильно настроен модуль авторизации.

В этом случае необходимо переключиться на встроенную авторизацию вручную. Для чего необходимо в файле конфигурации **setup.ini** расположенном в корневом каталоге программы в разделе **[**Options**]** установить значение **Authorization=**builtin Изменение вступит в силу немедленно. Изменение возможно вносить при работающем сервере.

Так же члены группы Администраторы могут заходить в систему, используя встроенную авторизацию даже при включённой внешней авторизации. Для этого необходимо в строке браузера указать следующий адрес страницы /login?b Например: http://site.ru/pdp7/login?b

Настройка уровня сложности пароля

Администратор может задать минимальную длину и сложность пароля пользователей. Пользователь или администратор не смогут задать пароль не соответствующий требованиям. Настройки не повлияют на уже существующие пароли, а только на задание новых. Настройки сложности и длины пароля осуществляются через редактирования файла **setup.ini** расположенного в корневом каталоге программы в разделе **[**Options**]** Для задания минимальной длины пароля необходимо установить параметр **MinPass** (по умолчанию 1). Для задания минимальной сложности пароля параметр: **PassDiff** Возможные значения для этого параметра:

- no – пароль может быть любым (значение по умолчанию)
- low – пароль должен содержать буквы и цифры или буквы и специальные символы или цифры и специальные символы
- med – пароль должен содержать буквы в разном регистре и цифры или буквы в одном регистре, цифры и специальные символы или буквы в разных регистрах и специальные символы
- high – пароль должен содержать буквы в разном регистре, цифры и специальные символы

Внимание! При любой сложности пароля концевые пробелы не допускаются!

Страница состояния системы

Администратор может наблюдать состояние системы на странице «Система». Страница доступна из главного меню по кнопке «Системная информация». На этой странице доступна следующая информация:

- время запуска сервера и продолжительность его непрерывной работы;
- количество запуска рабочего процесса;
- пользователь, от имени которого запущен процесс сервера;
- максимальное количество соединений;
- сжатие браузером;
- таймаут сессий;
- серверы экспертиз;
- количество сессий;
- память;
- состояние сервера PDP;
- состояние базы данных;
- общие переменные;
- активные пользователи.

Время запуска сервера и продолжительность его непрерывной работы – отображает время, когда был запущен сервер и сколько он проработал без остановки. Для версии «стандарт» сервером является процесс PDP.exe, для версии «корпоративная» - httpd.exe (веб-сервер Apache 2.4).

Количество запуска рабочего процесса – сколько раз запускался рабочий процесс. Для версии «стандарт» рабочий процесс совпадает с процессом сервера, поэтому значение параметра всегда 1. Для версии «корпоративная» показывает количество запусков процесса pdp.fcgi.

Максимальное количество соединений – отображает параметр настройки сервера. Этот параметр обозначает максимальное количество запросов обслуживаемых сервером одновременно. Не может быть меньше 50. Рекомендуемое значение 100.

Сжатие браузером – (вкл/выкл) показывает в каком виде сервер передаёт страницы веб-браузеру. **Вкл** – страницы передаются в сжатом виде, что экономит трафик и ускоряет их загрузку. **Выкл** – страницы передаются в исходном виде без сжатия, что снижает нагрузку на сервер и компьютер пользователя, но увеличивает трафик.

Таймаут сессий – время бездействия пользователя, по истечении которого, будет завершен его сеанс.

Серверы экспертиз – количество процессов, отвечающих за выполнение экспертиз. Например: **3(1) из 5**. Это означает что сейчас выполняется 3 процесса экспертной системы, причем 1 выполняет экспертизу, а соответственно 2 находятся в режиме ожидания. Последняя цифра показывает максимальное возможное количество

одновременно запущенных процессов. В случае если экспертизы не запускались ни разу – отображается **0 из 0.**

Количество сессий – показывает количество веб-сессий на сервере. Сессия – это 1 подключение к серверу браузера. Браузеры для одного сайта могут создавать несколько подключений. Таким образом, количество сессий может не соответствовать количеству браузеров, работающих с сервером.

Память – отображает использование памяти системой Диагностика+. Данная информация предназначена для анализа разработчиками.

Сервер PDP – отображает состояние сервера PDP – память и размер пула рабочих потоков.

База данных – показывает состояние базы данных. OST-OAT – показывает разрыв между Oldest snapshot и Oldest active транзакциями. Значение «отлично» об отличном состоянии транзакций и отсутствии мусора в БД. В случае проблем с базой данных будет отображаться мигающее красным цветом число. При помощи гиперссылки «статистика» можно посмотреть статистику заголовка БД. Как правильно анализировать статистику см. документацию SQL-сервера Firebird 4.0.

Общие переменные – отображает состояние общих пользовательских переменных. Данная информация предназначена для анализа разработчиками.

Активные пользователи – таблица активных пользователей, т.е. тех, которые работают или недавно работали с системой. Вы можете сортировать таблицу, кликнув на соответствующий заголовок. Таблица имеет следующую структуру:

- **Ид –** идентификатор пользователя.
- **Аккаунт –** аккаунт пользователя с помощью которого был произведён вход в систему. Зависит от типа авторизации.
- **Вход через –** способ каким пользователь зашёл в Диагностику+ (встроенная, CAS и т.д.).
- **ФИО –** фамилия, имя, отчество пользователя.
- **Компьютер –** имя компьютера, с которого был произведён вход. Имя не всегда возможно определить на стороне сервера – в этом случае оно не отображается.
- **IP –** адрес компьютера с которого выполнен вход (IP4 или IP6).
- **Браузер –** название и версия браузера.
- **Время входа –** время входа пользователя в систему (по часам сервера).
- **Время работы –** время, прошедшее с момента входа пользователя в систему до текущего момента.
- **Простой –** время, прошедшее с момента последней пользовательской активности. Пользовательская активность регистрируется пока открыт браузер пользователя и в нём открыта страница Диагностики+ и есть связь с сервером. По достижении таймаута (пользователь закрыл браузер, ушёл со страницы Диагностика+, разорвалось соединение с сервером на стороне пользователя) сессия пользователя автоматически завершается.

Глобальные настройки

Глобальные настройки действуют на всю систему и всех пользователей. Они применяются для тонкой настройки системы. Глобальные настройки хранятся в файле **SETUP.INI** в основном каталоге ПК Диагностика+. Изменение глобальных настроек требует перезапуска сервера. В случае отсутствия в файле какого-либо параметра используется значение по умолчанию. Файл глобальных настроек разбит на разделы. Далее будет представлен список разделов и настроек с описаниями.

Внимание! Изменяйте файл глобальных настроек осторожно! Всегда сохраняйте резервную копию! Неправильные настройки могут привести к неработоспособности системы!

[UserSetup]

Не менять!

[Decimal]

Настройка отображения чисел с плавающей запятой.

- **Standard** – количество значащих цифр (целое число, по умолчанию 3).
- **High** – количество цифр в числе > 1 при котором оно отображается в экспоненциальной форме, 0 - никогда (целое число, по умолчанию 0).
- **Low** – количество цифр в числе < 1 при котором оно отображается в экспоненциальной форме, 0 - никогда (целое число, по умолчанию 5).

[Options]

Общие настройки.

- **EditableID** – разрешает редактировать идентификаторы объектов (0 – запрещено, 1 – разрешено, по умолчанию 0).
- **TempDir** – временный каталог (путь, по умолчанию пустой, в этом случае используется стандартный каталог Windows).
- **DicAutoDrop** – только для GIU. Разрешает автоматически открывать следующий словарь для вложенных словарей (0 – запрещено, 1 – разрешено, по умолчанию 0).
- **ReleaseState** – разрешает отображения классов, находящихся в состоянии бета-тестирования (строка, по умолчанию Release) возможные значения:
  - *Beta* – классы , находящихся в состоянии бета-тестирования будут отображаться;
  - *Release* – будут отображаться только протестированные классы.
- **Authorization** – доступные методы авторизации (перечисление строк через запятую, по умолчанию builtin). Каждая строка должна быть либо builtin – встроенная авторизация, либо имя модуля авторизации.
- **MinPass** – минимальная длина пароля (целое число, по умолчанию 0).
- **PassDiff** – минимальная сложность пароля (см. раздел “Настройка уровня сложности пароля”).

- **HistorySize** – размер лога изменений (целое число в диапазоне 0 – 10000000, по умолчанию 5000000).

[DB]

Настройки базы данных.

- **SweepInterval** – интервал OST-OAT трактующийся как критическое состояние (целое число, по умолчанию 10000).
- **SweepHour** – расписание выполнения sweep в часах (целое число 0-23, по умолчанию 4). Определяет в каком часу суток будет выполнен свип. Рекомендуется устанавливать время суток, когда пользователи не работают с системой или когда нагрузка минимальна. Свип выполняется сервером Диагностики+, автоматический свип должен быть отключен для базы данных (см. документацию SQL-сервера Firebird 4.0).

[ADServer]

Настройки сервера экспертной системы.

- **Count** – максимальное количество процессов сервера экспертной системы (целое число, по умолчанию 10).

[Prompts]

Запросы пользователю. Только для GUI.

- **Exit** – разрешает запрос пользователю на выход из системы (0 – не спрашивать, 1 – спрашивать, по умолчанию 1).

[Display]

Настройки отображения. Только для GUI.

- **NULLText** – текст для null (строка, по умолчанию пустая строка).

[WebUI]

Настройки веб-интерфейса.

- **MaxConnections** – максимальное количество подключений к серверу (целое число, по умолчанию 0 – не ограничено). Только для встроенного сервера.
- **WaitTimeout** – время ожидания ответа от сервера Диагностики+ в секундах (целое число, по умолчанию 5).
- **EventTimeout** – время одного цикла отправки сообщений веб-браузеру в секундах (целое число, по умолчанию 30). Рекомендуется уменьшить, если сообщения об отложенных операциях, таких как выполнение экспертиз и аналитических отчетов не доходят или доходят не всегда.
- **Inactivetimeout** – таймаут веб-сессий в минутах (целое число, по умолчанию 10).

- **MaxRequests** – максимальное количество запросов на процесс fcgi (целое число, по умолчанию 100000, 0 – не ограничено). После выполнения указанного количества запросов, процесс завершается. Только для версии «корпоративная».
- **Lifetime** – время жизни процесса fcgi в минутах (целое число, по умолчанию 1080, 0 – не ограничено). Через заданное время процесс завершается. Только для версии «корпоративная».
- **MapProviders** – доступные источники карт для ГИС. (строка, возможные значения: Bing MapBox Yandex Google). Возможно указание нескольких или одного поставщика в любом порядке через запятую. Если не указан ни один поставщик или в setup.ini отсутствует параметр MapProviders, то по умолчанию используется MapBox.

Типичные сообщения об ошибках

Если выводятся сообщения об ошибках при сохранении изменений после редактирования данных (рис. 5, 6), то это скорее всего вызвано неправильным вводом данных.

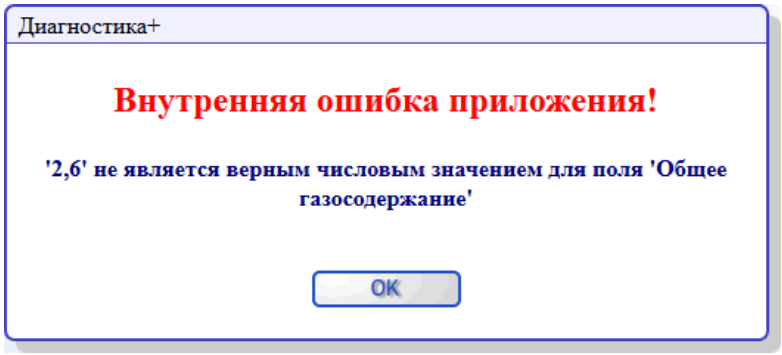


Рис. 5. Ошибка при вводе числа

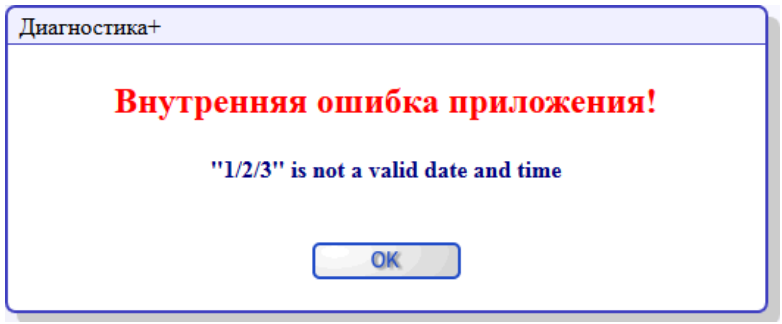


Рис. 6. Ошибка в формате даты

Если на экран появляется сообщение об ошибке (рис. 7 – 9), то, скорее всего, это значит, что сервер разорвал соединение. Часто это бывает в случае, когда в течение нескольких минут не было обращения к серверу.

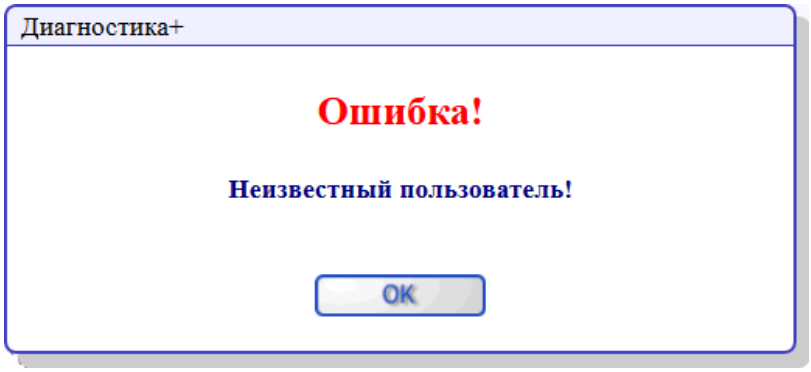


Рис. 7. Неизвестный пользователь

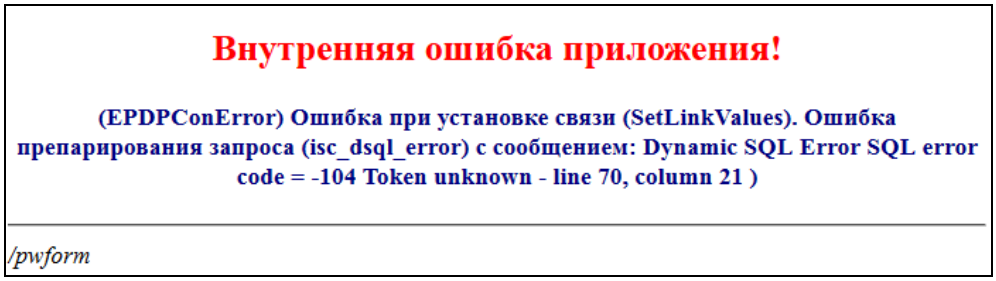


Рис. 8. Ошибка в форме

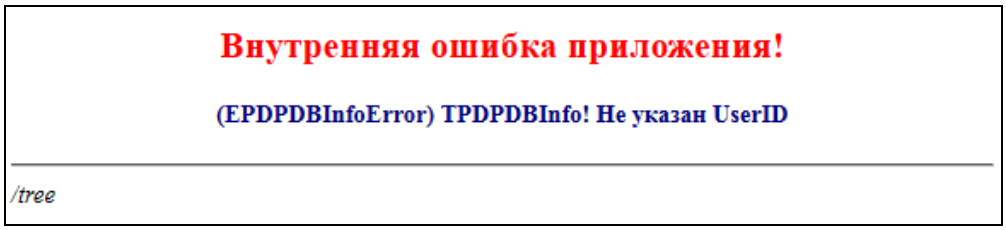


Рис. 9. Ошибка в дереве

В этом случае нужно нажать клавишу F5, и если будет предложено, то снова войти в систему указав имя и пароль. Если F5 не помогает, или не удается войти в систему, то необходимо закрыть браузер и снова открыть его с URL Системы.