



**Программный комплекс автоматизации пунктов
централизованной охраны «Эгида-3»
Р.АЦДР.00101-01 91 04**

Выпуск 7.1

**Особенности организации сетевого
режима АРМ ПЦО Эгида-3**

Руководство по настройке сетевого режима

КОМПЛЕКС ПУЛЬТОВОЙ ОХРАНЫ


2019


ЭГИДА-3

Оглавление


Термины и определения	3
Глава 1. Общие сведения. Область применения сетевого режима в АРМ ПЦО Эгида-3	5
1.1 Определение сетевого режима, задачи, решаемые с использованием сетевого режима в АРМ ПЦО Эгида-3	5
1.2 Варианты работы сетевого режима в АРМ ПЦО Эгида-3	6
1.2.1 Классический вариант работы сетевого режима	6
1.2.2 Вариант работы сетевого режима для перекрестного мониторинга	7
Глава 2. Настройка ПК, базы данных и ПО АРМ ПЦО Эгида-3 для работы в сетевом режиме	10
2.1 Проверка требования ОС	10
2.1.1 Проверка связи по локальной или виртуальной сети	10
2.2 Настройка службы SQL сервера на машинах сетевого режима	11
2.2.1 Настройка службы SQL, сетевых протоколов и агента	11
2.2.1 Работа с утилитой «Конфигуратор БД». Подключение к службе SQL с удалённой машины	14
2.3 Настройка Эгида-3 в сетевом режиме. Работа с менеджером конфигурации	16
2.3.1 Импорт объектов на удалённые рабочие места (вкладка «Архитектура»)	16
2.3.2 Настройка прав оператора удалённых мест (вкладка «Персонал»)	23
2.3.3 Создание и настройка рабочих мест операторов (вкладка «Рабочие места»)	25
2.3.4 Проверка работы Эгида-3 в сетевом режиме	27
Глава 3 Особенности работы в сетевом режиме	29
3.1 Особенности работы при разрыве связи с удалённым ПК	29
3.2 Особенности работы графических модулей рабочего места в сетевом режиме.	29
3.3 Работа с ГБР в сетевом режиме	31
3.4 Удаленное управление реле, зонами и разделами в сетевом режиме	34
3.5 Работа с видеоподсистемой в сетевом режиме	34

Термины и определения

Охраняемый объект (ОО или просто Объект)  – полная совокупность охраняемых логических зон, разделов, зон состояния, определенная в договоре на охрану с юридическим или физическим лицом. В Эгида-3 под объектом охраны может пониматься объект или часть территории любой сложности.


Отдел  – Это условное подразделение ПЦО, в которое входят сотрудники ПЦО имеющие набор определённых прав на конфигурирование БД объектов и оборудования, и работы с рабочим местом оператора. По умолчанию, в Эгида-3 создаётся только один отдел - Администраторы, где сотрудник имеет полные права.


Графический модуль – отдельный компонент окна рабочего места оператора, который в составе других графических модулей решает задачи отображения состояния объекта охраны и его компонентов. Модули могут размещаться на рабочем месте согласно разметке в ручном или автоматическом режимах. На данный момент окно рабочего места может состоять из семи графических модулей: окно тревожных извещений, список тревог, список или сетка объектов, протокол событий, модуль поиска объектов, панель оператора, план объекта.


Сотрудник ПЦО  - сотрудник ПЦО – администратор, оператор или другое лицо, имеющее набор определённых прав на мониторинг, управление объектами и редактирование БД объектов. По умолчанию, в системе создаётся только один сотрудник – Иванов Иван Иванович, который имеет полные права на мониторинг и конфигурирование системы.

Пароль – пароль оператора или администратора для запуска оболочки, конфигуратора БД или менеджера конфигурации. По умолчанию администратор (Иванов Иван Иванович) имеет пароль 123456.

Права доступа – полномочия операторов и администраторов системы на работу с той или иной вкладкой менеджера конфигурации, запуском и выгрузкой оболочки и модуля отчётов.

Рабочее место  – рабочее место оператора ПЦО, состоящее из набора графических модулей для отображения состояния извещателей, приборов, объектов охраны, обработки тревожных извещений и управления выходами.

Абонент (хозорган)  – пользователь услугами централизованной охраны, который в соответствии с назначенным ему уровнем доступа осуществляет локальное или удалённое управление охраняемых объектов (зон и разделов). В качестве абонентов могут выступать как физические лица (владельцы квартир, или квартиросъёмщики, например), так и юридические лица (управляющий персонал, сотрудники частных охранных агентств и т.д.)

Уровень доступа  – это набор временных ограничений и полномочий, определяющих права абонентов на управление привязанных к ним (абонентам) охраняемых объектов. Один и тот же уровень доступа может назначаться нескольким абонентам, но у каждого объекта охраны свой уровень доступа.

АРМ – автоматизированное рабочее место

ПК – персональный компьютер

ОО – охраняемый объект

ПО – программное обеспечение

ПОО – прибор объектовый оконечный

ППО – прибор пультовой оконечный

ПЦО – пункт централизованной охраны

Глава 1. Общие сведения. Область применения сетевого режима в АРМ ПЦО Эгида-3

1.1 Определение сетевого режима, задачи, решаемые с использованием сетевого режима в АРМ ПЦО Эгида-3

Сетевой режим АРМ ПЦО Эгида-3 – это режим совместной работы нескольких ПК с установленным программным комплексом АРМ ПЦО «Эгида-3», объединенных в единую локальную сеть для решения задач администрирования и мониторинга.

Сетевой режим предназначен для удаленного конфигурирования распределенных мест диспетчеров, операторов, администраторов, совместной работы нескольких мест мониторинга, объединённых локальной сетью или интернет соединением.

Сетевой режим решает следующие задачи:

- позволяет конфигурировать БД, добавлять новые объекты охраны, редактировать уже имеющиеся в режиме реального времени, не прерывая работу операторов удалённых рабочих мест;
- обеспечивает объединение нескольких ПК в локальную сеть с общей базой данных объектов охраны и подключенного пультового и объектового оборудования;
- распределяет зоны ответственности операторов по объектам охраны, мобильным бригадам между несколькими ПК, объединёнными в сеть (раздельный мониторинг);
- позволяет использовать перекрёстный мониторинг объектов охраны для обеспечения надёжности мониторинга;
- позволяет разнести ПК с Эгида-3 и БД на разные машины для обеспечения надёжности хранения и резервирования БД.

Первоначально сетевой режим в АРМ ПЦО Эгида-3 создавался для предоставления пользователям возможности удаленного конфигурирования распределенных мест мониторинга в локальной сети, без необходимости перезапуска оболочки Эгида-3. При этом работа оператора на рабочем месте - не прерывается. В более поздних версиях Эгида-3 была добавлена возможность совместной работы и распределения объектов охраны по рабочим местам.

При использовании интернет соединения общее количество ПК в сетевом режиме зависит от сложности системы: количества ОО, информативности протоколов, количества передаваемых сообщений в сутки, числа камер, количества операторов, и от скорости работы локальной сети

Следует помнить, что избыточное усложнение системы приведет к увеличению нагрузки на канал передачи данных. Следовательно, возможно возникновение задержек в работе, которые влияют на качество наблюдения за объектами охраны.

Сетевой режим рассчитан на работу в рамках локальной сети со скоростью передач данных до 100 Мбит, соответственно при использовании интернет-подключения ПК друг к другу, необходимо обеспечить достаточную скорость передачи данных при высокой надёжности соединения.

1.2 Варианты работы сетевого режима в АРМ ПЦО Эгида-3

Существует несколько условных вариантов объединения ПК с АРМ ПЦО Эгида-3 в единую сеть, для решения различных задач администрирования и мониторинга.

1.2.1 Классический вариант работы сетевого режима

Так называемый «классический» вариант сетевого режима – когда используется один ПК с БД, и подключенным пультным оборудованием, открытыми портами на приём и подключенными интернет-каналами (рабочее место администратора - условный сервер) и один, или несколько удалённых ПК, за которыми предполагается работа операторов с рабочими местами (удалённые рабочие места мониторинга – УРМы). Соответственно на этих ПК не созданы каналы связи и не подключены приборы приёма.

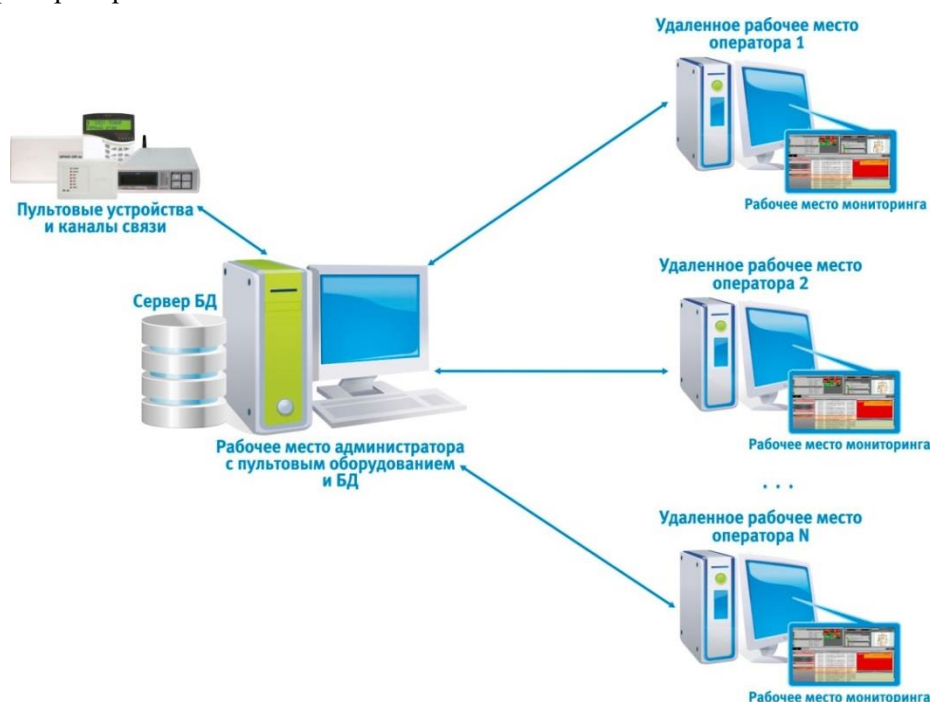


Рис. 1 «классический» вариант сетевого режима

Данная конфигурация сетевого режима, позволяет распределить объекты охраны по отдельным удалённым рабочим местам. Плюсами данного решения являются:

- сокращение нагрузки на операторов, путём перераспределения объектов между ними;
- возможность распределения объектов по сферам ответственности или регламенту. Каждый оператор будет отвечать только за свои объекты, например, можно настроить место, где будут только особо-охраняемые объекты для старших операторов (офицеров);
- распределение объектов по местам с учётом опыта и навыков операторов;
- сокращение времени реагирования на ситуации по объектам и времени вызова мобильных групп;
- улучшение общих показателей реагирования, снижение количества необработанных и ложных вызовов.

1.2.2 Вариант работы сетевого режима для перекрестного мониторинга

Второй вариант работы сетевого режима – это использование нескольких ПК с Эгида-3 подключенным пультовым оборудованием, своими объектами охраны, каналами связи с УОО и модемами для управления, подключенных к одной базе данных.



Рис. 2 Вариант работы с сервером на одном из рабочих мест

В данном случае, может осуществляться как перекрестный мониторинг объектов, так и вариант с распределением объектов по рабочим местам. Например, удалённое рабочее место мониторинга № 2, как на рисунке выше, может осуществлять мониторинг только своих объектов охраны, выведенных на каналы связи и пультовые устройства, подключенные к нему, а рабочее место № 1 может осуществлять перекрёстный мониторинг, как объектов места администратора, так и объектов рабочего места № 2. Комбинированная схема позволяет повысить качественные показатели мониторинга.

Плюсами данного решения являются:

- Улучшение качественных показателей обработки тревог за счёт одновременного реагирования;
- Повышение надёжности системы за счёт использования дублирующих каналов связи на уровне объектового оборудования (при потере связи с местом администратора, останутся объекты рабочего места №2);
- Сокращение времени реагирования мобильных групп счёт более оперативной отправки вызовов;
- За счёт перекрёстного мониторинга можно увеличить нормативное количество объектов охраны на одного оператора;
- Возможность сократить количество рабочих мест при увеличении количества объектов.

Минусами данного варианта работы сетевого режима являются:

- Отсутствие зон ответственности операторов;
- Возможные сложности в распределении нагрузки между удалёнными рабочими местами;
- Требуется более квалифицированный и обученный персонал.

БД SQL, в данном случае, может быть расположена на рабочем месте администратора, или располагаться на отдельной машине, подключенной к общей сети, на которой не требуется установка дистрибутива Эгиды.

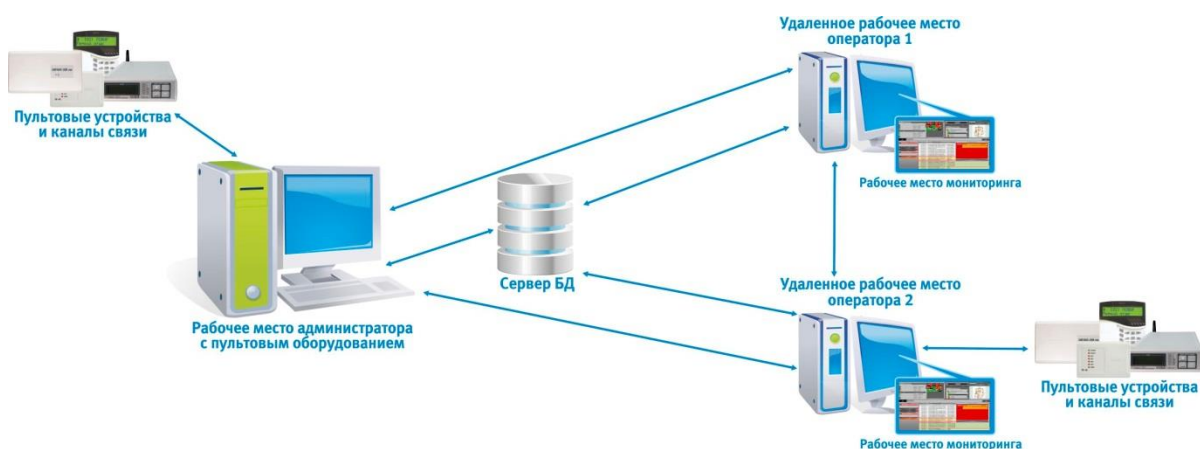


Рис. 3 Вариант работы с сервером на удаленном ПК

Возможны и другие комбинированные схемы работы сетевого режима Эгида-3. Например, на рисунке 3 представлен вариант, когда БД находится на другой машине, а количество рабочих мест с подключенным оборудованием может быть любым, в пределах возможности локальной сети.

Так как идеология Эгиды не делает различий между рабочими местами (ПК, работающими в сетевом режиме), на всех машинах запускаются все модули, подгружаемые с запуском оболочки. Каждое рабочее место в сети может являться сервером оборудования и местом мониторинга, разграничение функций приёма, обработки сообщений с объектов, их отображения в графических модулях рабочего места осуществляется на уровне *импортирования типов* менеджера конфигурации во вкладке «архитектура».

Для всех лицензий эгиды работает общая лицензионная политика – одна лицензия – один ключ, таким образом, на каждую из машин, где установлена Эгида-3, требуется приобретение лицензионного ключа. На рабочие места операторов (там, где требуется только запуск рабочего места без подключения оборудования и проброса каналов связи с объектовыми устройствами) приобретается обычная лицензия на 100 приборов, а на компьютер, к которому подключены пультовые устройства, проброшены каналы связи с ПОО, требуются отдельные варианты лицензий:

- При использовании ПОО (УО-4С, С2000-PGE, С2000-ИТ, Орион радио, приборов «Альтоники» и т.д.), приобретается обычная лицензия Эгиды с индексом 100. Этот же вариант предусматривает подключение к одному ПК не более 100 приборов ИСО Орион по протоколам «Орион» или «Орион ПРО»;
- Если к ПК напрямую подключено более 100 приборов ИСО «Орион», приобретается лицензия на 500\1000\2000 приборов в зависимости от общего количества адресов подключаемых устройств;
- Для периодического удаленного администрирования (без проброса каналов связи и подключения приёмного или передающего оборудования) достаточно демо-версии АРМ ПЦО Эгида-3.

Как правило, распределение прав, объектов охраны, мобильных групп, рабочих мест между ПК осуществляется через таблицу импортирования типов в сетевой архитектуре, настройка прав операторов и фильтров объектов охраны - в настройках самого рабочего места. Подробнее о настройке ПК и АРМ ПЦО Эгида-3, для работы в сетевом режиме изложено в Главе 2.

Глава 2. Настройка ПК, базы данных и ПО АРМ ПЦО Эгида-3 для работы в сетевом режиме

2.1 Проверка требования ОС

В пакет установки АРМ ПЦО «Эгида-3» входит дистрибутив Эгида-3, службы резервного копирования и резервирования, набор пререквизитов¹ и дистрибутив MS SQL Server Express 2008 R2. Установочный файл программы (напр. «bin_release_r6_update3.exe»), представлен в виде самораспаковывающегося архива, который скачивается с сайта компании по ссылке: «<https://bolid.ru/production/center/egida03>».

На компьютерах, предназначенных для эксплуатации системы, не желательна установка сторонних программных продуктов, не имеющих прямого отношения к функционированию комплекса кроме предустановленных вариантов MS SQL Express 2008 и MS SQL Server 2008 (полноценная версия).

- 1. Имя компьютера должно иметь только латинские буквы, название компьютера на кириллице не допускается.*
- 2. Всю установку системы в Windows 7, Windows 8(8.1, 10) проводить под правами администратора (включая установку MS SQL 2008 Express\MS SQL 2012 Express), ярлыки всех приложений АРМ ПЦО «Эгида-3» запускать только от имени администратора компьютера.*
- 3. Если на ОС Windows 10 при установке Эгиды появляется ошибка установки MS SQL 2008 Express, то в ОС установлены обновления, в которых включена проверка версионности SQL. Для решения данной проблемы необходимо самостоятельно скачать с сайта Microsoft дистрибутив MS SQL 2012, выполнить установку со смешанной авторизацией² и провести процедуру создания и подключения БД вручную. Подробности описаны в документе «03-Руководство администратора».*
- 4. При возникновении проблем совместимости со службой UAC в Windows рекомендуется запускать приложения через контекстное меню от имени администратора или изменить уровень контроля учётных записей.*
- 5. Версии дистрибутивов Эгида-3 на всех устройствах, работающих в сетевом режиме должны быть одинаковы.*



2.1.1 Проверка связи по локальной или виртуальной сети

После установки Эгида-3 на машины, работающие в сетевом режиме, необходимо проверить связь между ними по сети. Для этого необходимо, чтобы у каждого ПК был свой уникальный IP адрес, при этом IP адреса сетевых машин должны лежать в одном диапазоне (в одной подсети). При объединении удалённых ПК, находящихся в разных подсетях и имеющими,

¹ Набор системных утилит для корректной работы программного обеспечения

² Смешанный режим авторизации позволяет выбрать тип учетной записи, под которой будет выполняться вход на сервер.

например, подключение к сети Internet необходимо использовать маршрутизацию на уровне сторонних сервисов и аппаратных средств (VPN тоннели или другие способы организации локальной сети в рамках интернет - соединения).

Настройку сетевого подключения ПК, настройку VPN тоннелей, или других способов организации виртуальной сети в рамках Internet подключения должен осуществлять квалифицированный персонал.



- *Не допускается разрыв соединения между местом администратора (условным сервером с подключенным оборудованием) и ПК операторов;*
- *Не допускается (даже кратковременный) разрыв соединения с БД на всех ПК, объединённых в локальную сеть;*
- *При использовании виртуальных подключений в рамках Internet соединений необходимо использовать только надёжные высокоскоростные подключения к сети (рекомендуется - выделенные линии, оптико-волоконные подключения и т.д.).*
- *При использовании мобильного интернета (3G, 4G), необходимо проверять реальную скорость интернет - соединения при обмене данными, уточнить у провайдера мобильной связи возможность использовать передачи данных по каналам UDP.*

Перед подключением необходимо убедиться, что брандмауэр ОС Windows отключен, UDP и TCP порты (сокеты), с которыми работает Эгида-3, не заняты другим программным обеспечением. По умолчанию ядро Эгида-3 работает с портом «11112», БД SQL с портами «1433», «1434». Проверить состояние портов можно с помощью специализированных программ (например «portmon.exe») или монитора системных ресурсов ОС Windows.

Перед организацией сетевого режима необходимо полностью сконфигурировать Эгида-3, пультовое и объектовое оборудование. Предполагается, что система является исправной и полностью работоспособной: настроено подключение к БД, подключено оборудование, проверены каналы связи с оконечными устройствами, проброшены порты, проверены настройки сетей и сетевых соединений между ПК, локальное рабочее место функционирует в требуемом объёме.

2.2 Настройка службы SQL сервера на машинах сетевого режима

2.2.1 Настройка службы SQL, сетевых протоколов и агента

АРМ ПЦО Эгида при подключении к БД MS SQL Server 2008 Express использует смешанный режим авторизации (логин - «sa» пароль – «sysdba»), однако запуск службы SQL Server, по умолчанию, может быть осуществлён от имени локальной машины.

Перед началом работы в сетевом режиме, необходимо произвести настройку MS SQL Express 2008 R2 (Далее SQL). Для этого, в настройках диспетчера конфигурации MS SQL Server 2008 Express (далее - диспетчер), необходимо проверить конфигурацию сетевых служб.



Данные настройки необходимы только на ПК с сервером БД SQL. На удаленных рабочих местах установка и настройка служб и протоколов MS SQL не требуется.

Диспетчер находится в приложении «Управление компьютером», его можно запустить несколькими способами:

- на рабочем столе: в свойствах ярлыка «Этот компьютер» подпункт «управление»;
- в проводнике Windows: на панели быстрого доступа, в контекстном меню «Этот компьютер», подпункт «управление»;
- в строке поиска: начать вводить словосочетание «Управление компьютером». Выбрать его из появившегося списка.

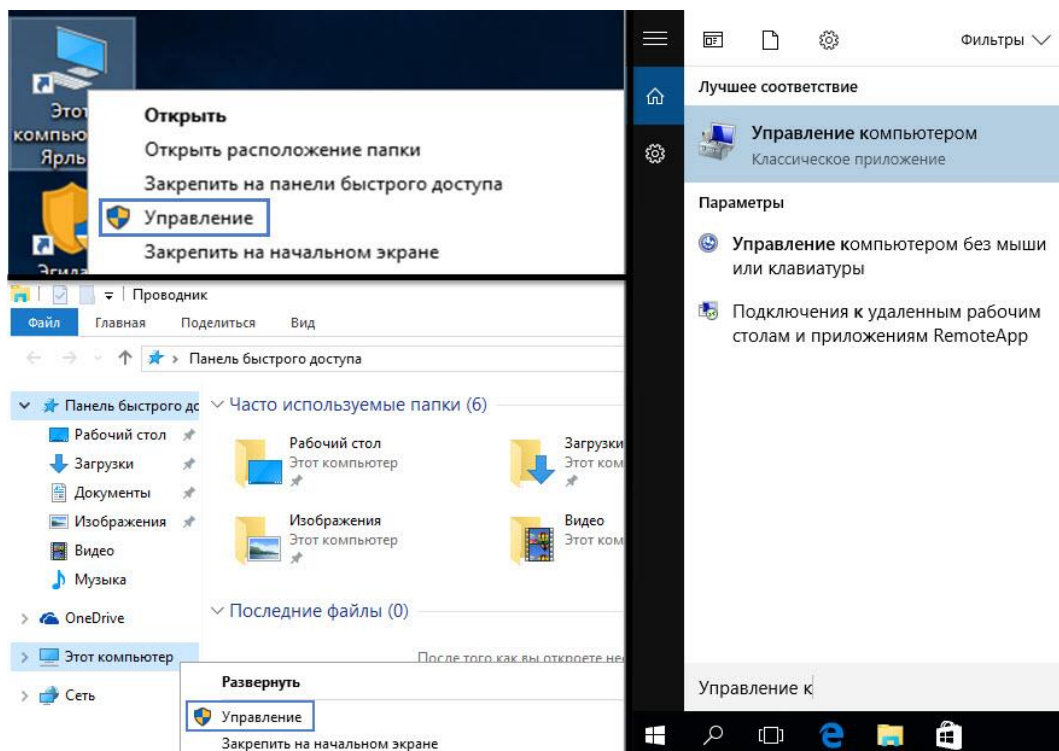


Рис. 4 Запуск диспетчера конфигурации SQL сервера

В окне приложения «Управление компьютером», в дереве объектов выбрать пункт «Службы и приложения» \ «Диспетчер конфигурации SQL Server» \ «Службы SQL Server».

В колонке состояния служб должны быть указаны следующие параметры работы:

- «SQL Server» - работает;
- «Агент SQL Server» – остановлена;
- «Браузер SQL Server» - работает.

Управление компьютером (л)			
Службы и приложения			
Службы			
Диспетчер конфигурации SQL Server			
Имя	Состояние	Режим запуска	
SQL Server (SQLE...	Работает	Авто	
Агент SQL Server...	Остановлена	Другое (Загрузочн...	
Браузер SQL Ser...	Работает	Авто	

Рис. 5 Службы SQL сервер

По умолчанию, служба «*Браузер SQL Server*» может не запуститься, после установки пакета MS SQL Express. Для того чтобы ее запустить нужно:

1. Открыть свойства «Браузер SQL Server»;
2. В поле «Использовать для входа» поставить флажок на «Встроенную учетную запись», в открывшемся списке, выбрать «Сетевая служба»;
3. В появившемся окне, с сообщением о перезапуске службы нажать на клавишу «Да».

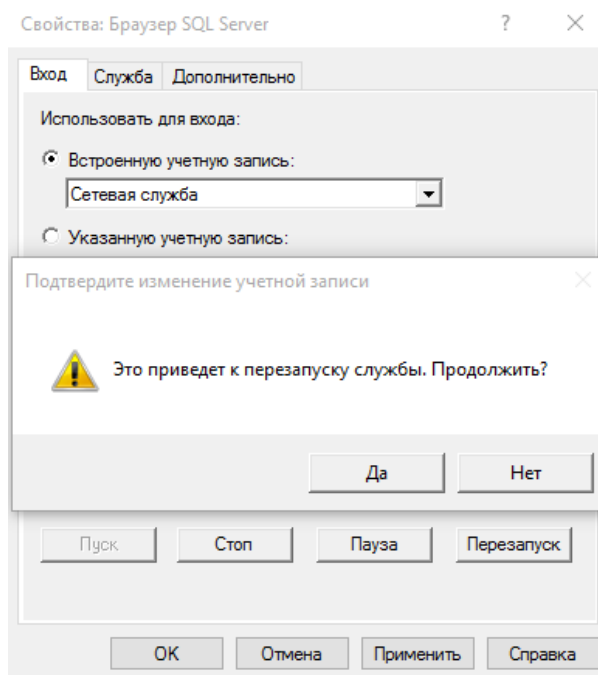


Рис. 6 Запуск службы «Браузер SQL Server»

Если, после этого служба «*Браузер SQL Server*» не запустилась, то необходимо выполнить запуск службы вручную.

В дереве объектов выбрать пункт «*Службы и приложения*» \ «*Службы*». В открывшемся списке найти службу «*Браузер SQL Server*», в ее свойствах указать тип запуска – «*автоматически*», нажать «*Запустить*».

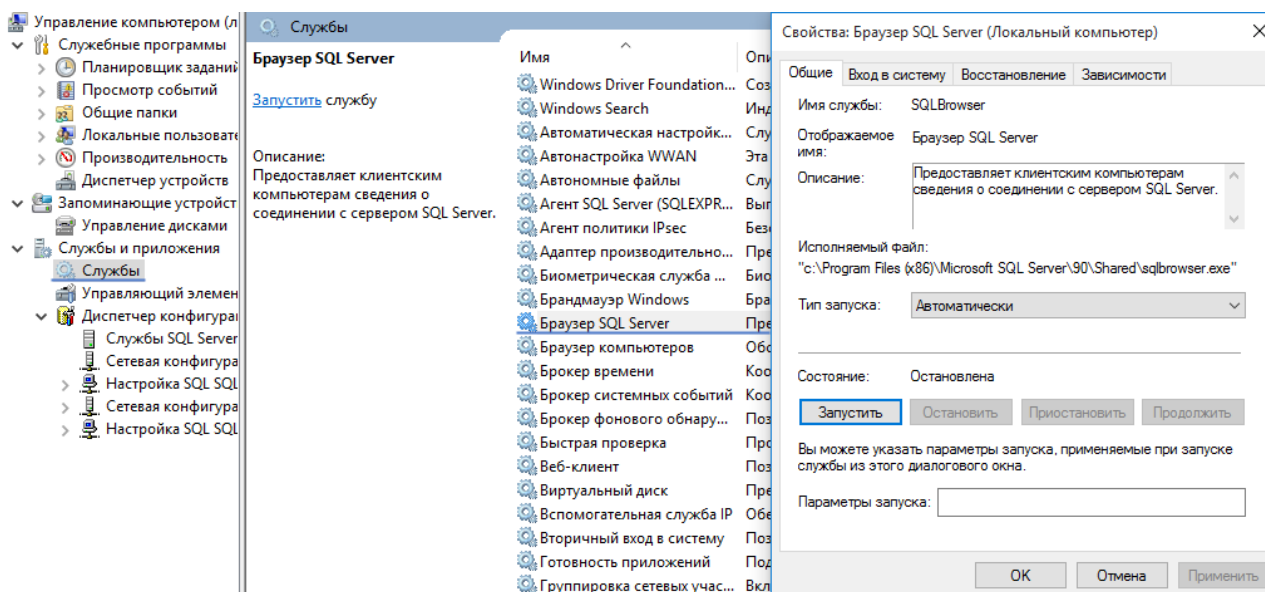


Рис. 7 Ручной запуск службы «Браузер SQL Server»

После ручного запуска службы в диспетчере служб, необходимо проверить состояние службы браузера SQL после запуска в: «Диспетчер конфигурации SQL»\ «Службы SQL Server».

Следующим этапом настройки является включение протоколов «SQLEXPRESS» в сетевой конфигурации SQL Server. В данном пункте меню необходимо включить протоколы: «Общая память», «Именованные каналы», «TCP/IP».

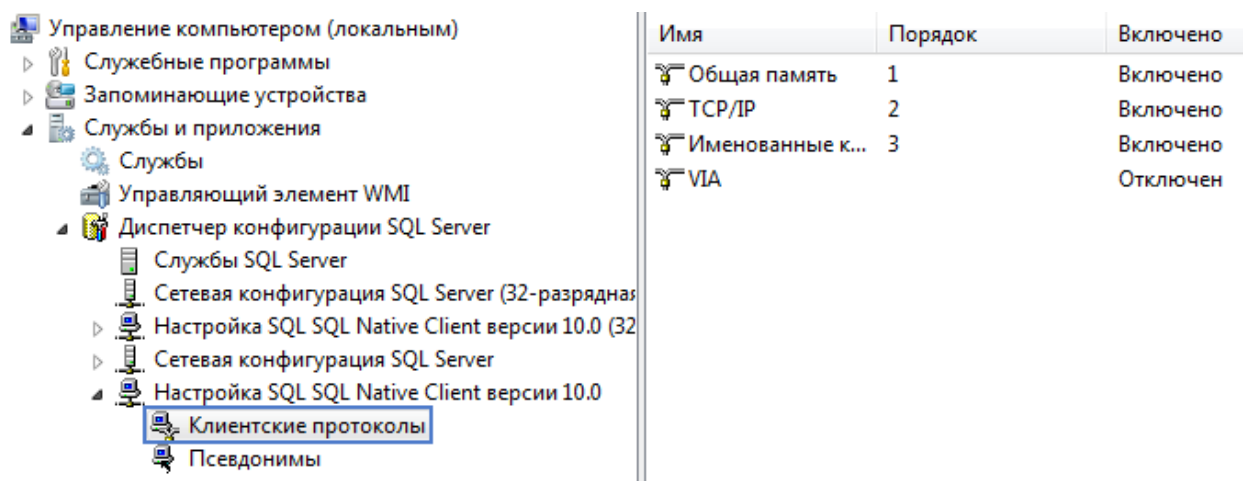



Рис. 8 Настройка «SQL Native client»

После настройки служб и протоколов диспетчера конфигурации SQL Server, необходимо с удаленного рабочего места подключиться к серверу БД и настроить Эгиду-3.

2.2.1 Работа с утилитой «Конфигуратор БД». Подключение к службе SQL с удалённой машины

Подключение удаленной машины к БД Эгиды осуществляется через приложение «Конфигуратор БД». Путь к данной программе через меню пуск: «Пуск» - «Все приложения»\«Эгида-3»\ «Конфигуратор БД»  Конфигуратор БД.

Так же ее можно запустить из корневого каталога с установленной АРМ ПЦО Эгида-3. Каталог по умолчанию «C:\Program Files (x86)\Эгида-3\Tools\ConfigDB.exe».

«Конфигуратор базы данных системы Эгида 3» предназначен для создания, удаления, обновления БД. Кроме того, в данной программе задаются настройки резервирования БД, создается БД истории.

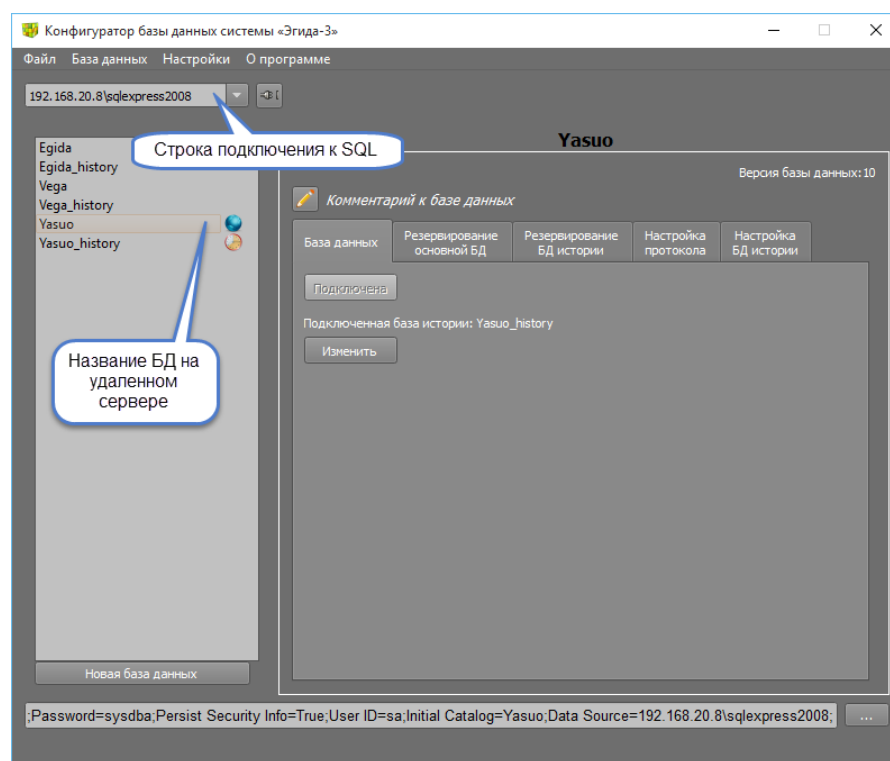


Рис. 8 Окно конфигуратора БД с подключенной БД

Для того чтобы подключить удаленный ПК к БД на сервере необходимо нажать на раскрывающийся список в верхнем левом углу программы, и из появившегося списка выбрать строку подключения к именованному экземпляру SQL Server с названием нужного ПК (например: `PROG-OZ-8\SQLEXPRESS2008`). Откроется окно ввода данных учетной записи SQL. По умолчанию - Пользователь: «sa»; Пароль: «sysdba». Если MS SQL Express был установлен вручную, то указывается пользователь и пароль, заданные в процессе установки.

Если в списке браузера отсутствует имя сервера, то необходимо ввести его вручную, если после ручного ввода имени сервера, логина и пароля подключения не происходит

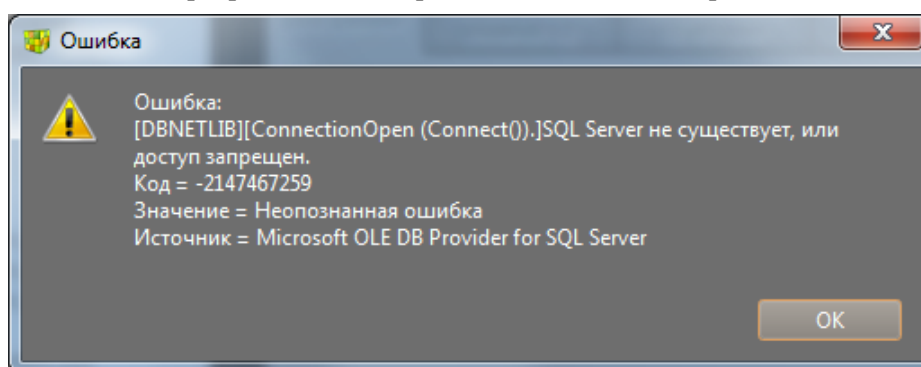


Рис. 9 Ошибка подключения к серверу БД

то, необходимо в строке подключения через «\» ввести IP адрес компьютера с сервером БД и имя установленного экземпляра SQL Server далее нажать на значок подключения рядом со строкой



ввода имени сервера

Данный способ подключения используется, если в ОС ПК используется несколько сетевых подключений.

В случае успешного подключения к удалённому серверу, при выборе БД, если ранее подключение к данной базе с данного ПК не осуществлялось, появляется диалоговое окно, сообщающее о том, что в БД не созданы системные (главные) объекты с именем данного ПК. Диалоговое окно показывает, какие ПК (системные объекты) уже добавлены и предлагает добавить новый объект с именем ПК удаленного рабочего места. Необходимо согласиться и нажать кнопку «Да».

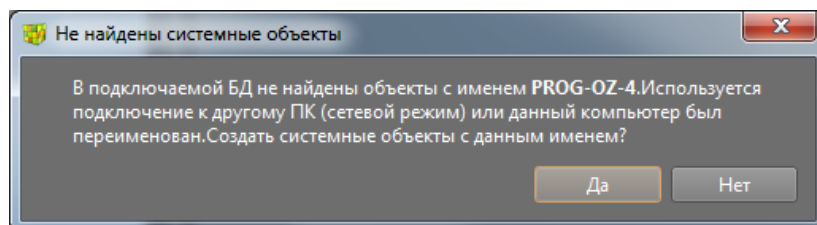


Рис. 10 Окно создания новых системных объектов

После успешного добавления в БД нового системного объекта можно приступать к сетевому конфигурированию Эгиды-3 через «Менеджер конфигурации» компьютера, на котором создано оборудование, объекты охраны и рабочие места.

2.3 Настойка Эгида-3 в сетевом режиме. Работа с менеджером конфигурации

2.3.1 Импорт объектов на удалённые рабочие места (вкладка «Архитектура»)

Настройка сетевого режима в Эгида-3 начинается с конфигурирования вкладки «Архитектура». «Менеджер конфигурации» \ «Архитектура».

Вход в оболочку на компьютере условного сервера должен осуществляться под пользователем с максимальными правами.

Вкладка «Архитектура» предназначена для настройки параметров режима работы компьютеров в сетевом режиме. В данной вкладке настраиваются параметры импорта типов с удаленных мест для удаленного администрирования и мониторинга.

После того, как в БД будут добавлены системные объекты новой сетевой машины, на всех вкладках менеджера конфигурации (Объекты охраны, Оборудование и т.д.) будут отображаться два системных объекта: ПК, на котором сейчас работает администратор (условный сервер) и название ПК удалённой машины.

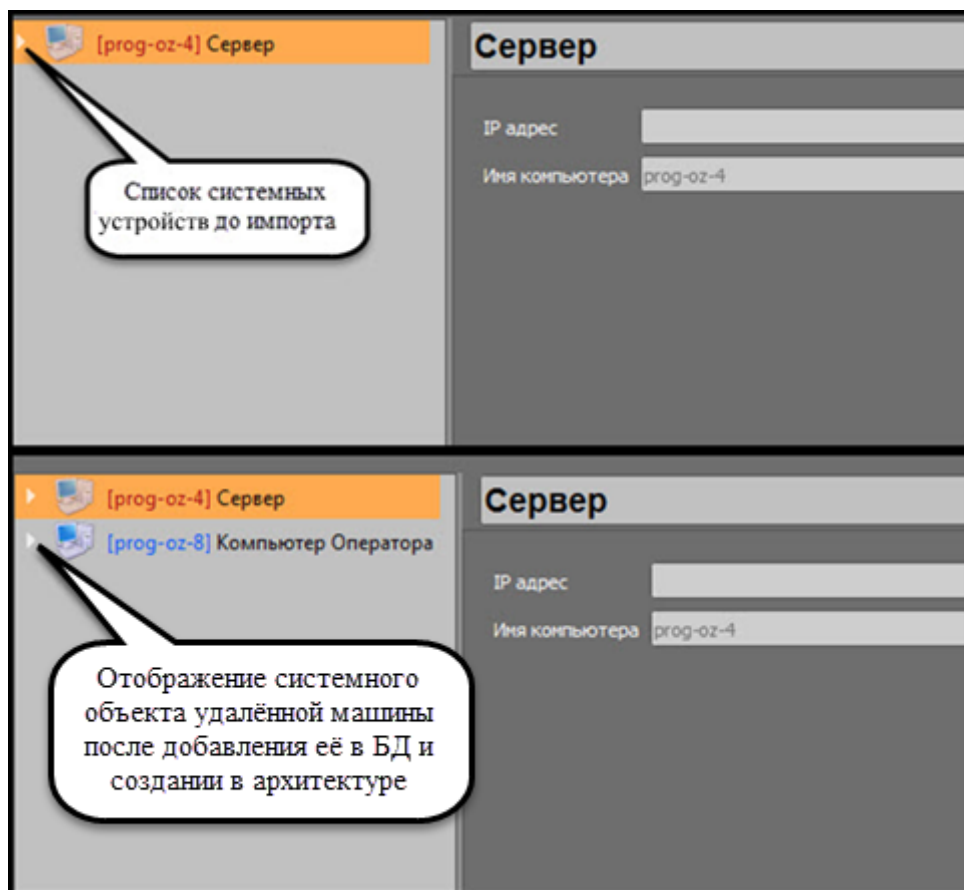


Рис. 11 Список системных устройств

Конфигурация начинается с добавления импортируемого компьютера (системного объекта) во вкладку «Архитектура».

Импортируемые компьютеры – это объединение сетевых имён подключенных к БД компьютеров для их удалённого конфигурирования и отображения созданных на них объектов.

Импортируемый компьютер – это ПК (системное устройство) созданный в БД Эгиды и подключенный к данному компьютеру по локальной сети. Импортируемый компьютер добавляется в список импортируемых для того, чтобы администратор или оператор мог видеть в менеджере конфигурации и удалённо конфигурировать типы объектов (оборудование, объекты охраны, права, рабочие места и т.д.) созданные на удалённой машине.

Импорт типов также позволяет отображать в локальном рабочем месте объекты охраны, группы быстрого реагирования, планы помещений, созданные на удалённой машине, т.е. позволяет оператору на одном рабочем месте «видеть» и работать с объектами, созданными на других компьютерах.

Импортирование компьютеров необходимо проводить «взаимно», поскольку настройка отображаемых типов для каждой машины проводится индивидуально. Например, если разделить два сетевых ПК на «компьютер условного сервера», с подключенным оборудованием, БД, каналами связи с объектом, GSM модемом для управления, созданной базой объектов охраны и ГБР. И на компьютер, на котором будет вестись наблюдение за объектом охраны – «компьютер оператора», то для того, чтобы на удаленной машине оператора видеть состояние объектов охраны, работать с мобильными группами, управлять объектами, необходимо импортировать часть объектов «условного сервера» на «компьютер оператора».

Это может сделать сам администратор сервера, создав свой компьютер в импортируемых компьютерах удалённого ПК оператора и указав минимально необходимый для работы оператора импорт типов.

Подход на уровне импортирования сетевых компьютеров и отдельных типов позволяет создать очень гибкую настройку видимых элементов на каждой из машин, при этом каждый компьютер может иметь свой набор системных объектов – созданного оборудования, объектов охраны, рабочих мест, мобильных групп, обслуживающего персонала и т.д.

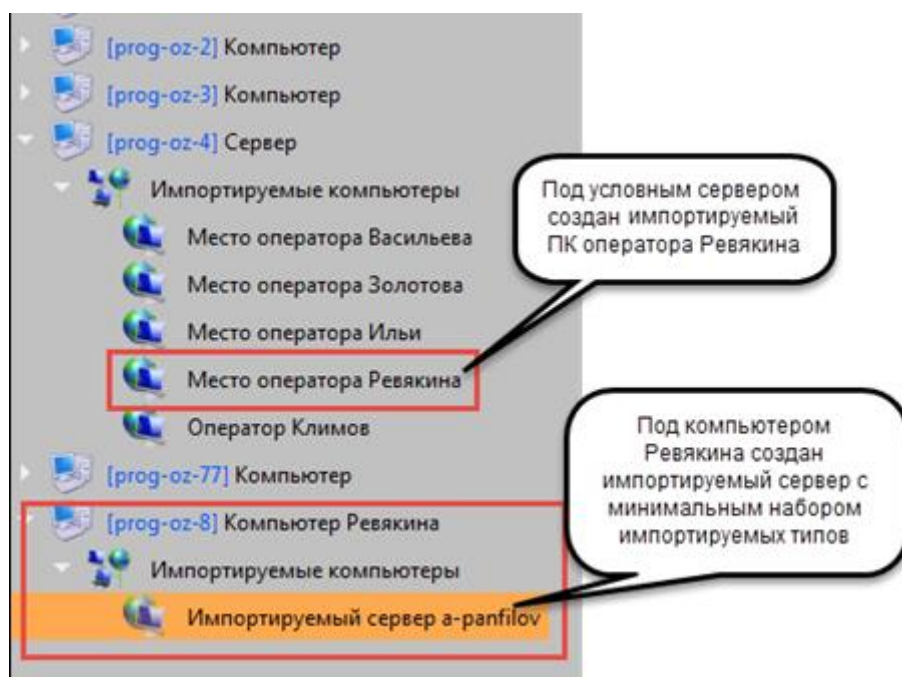


Рис. 12 «Взаимный» импорт сетевых компьютеров во вкладке Архитектура

При добавлении импортируемого компьютера в его свойства указывается сетевое имя компьютера и его статический IP адрес. В таблице импортируемых типов флагами отмечаются только те типы, которые будут импортироваться на данный компьютер (т.е. будут доступны для просмотра, редактирования и мониторинга) с удалённой машины. Под импортируемыми типами следует понимать объединение отдельных элементов менеджера конфигурации (а фактически – базы данных), расположенных в разных вкладках.

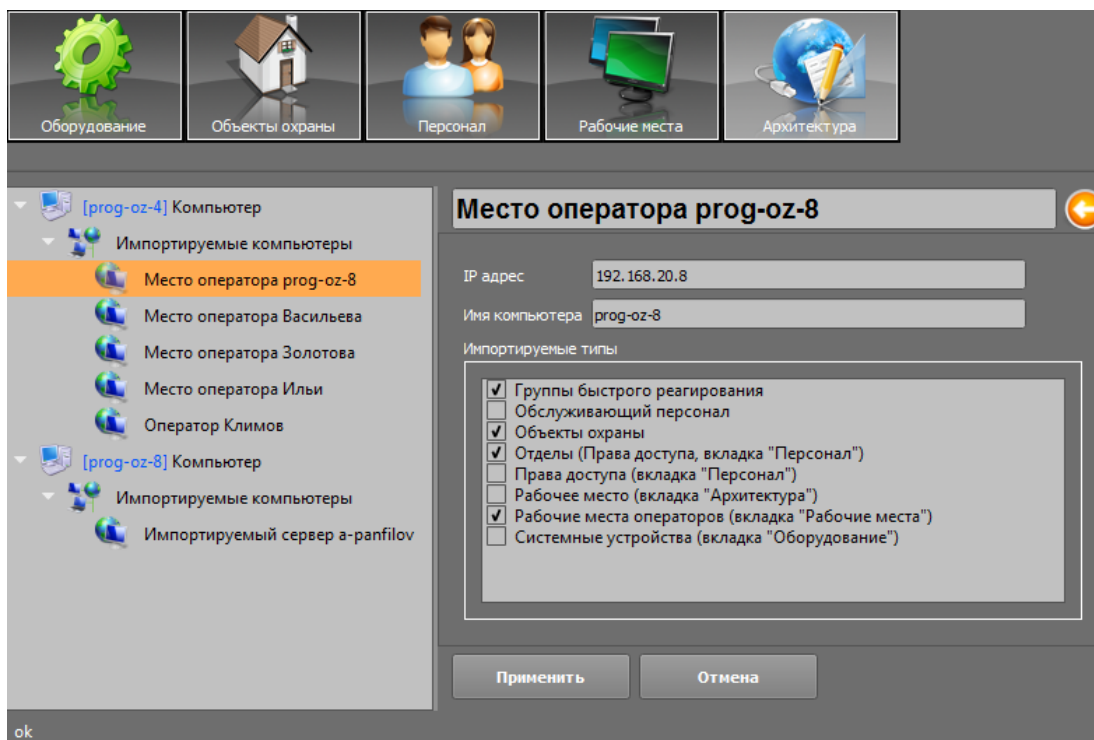


Рис. 13 Свойства подключаемого места оператора

На данный момент в Эгида-3 различают 8 импортируемых типов менеджера конфигурации:

- Группы быстрого реагирования (мобильные бригады)
- Обслуживающий персонал
- Объекты охраны
- Отделы (права доступа, вкладка «Персонал»)
- Права доступа (вкладка «Персонал»)
- Рабочее место (вкладка «Архитектура»)
- Рабочие места операторов (вкладка «Рабочие места»)
- Системные устройства (вкладка «Оборудование»)

«Группы быстрого реагирования» - импорт данного типа позволяет просматривать редактировать параметры мобильных групп «чужой» машины в менеджере конфигурации (вкладка «Персонал»), и работать с этими группами в рабочем месте. Если группы не импортированы, то оператор не будет видеть их в рабочем месте, и не сможет вызывать их на объекты.

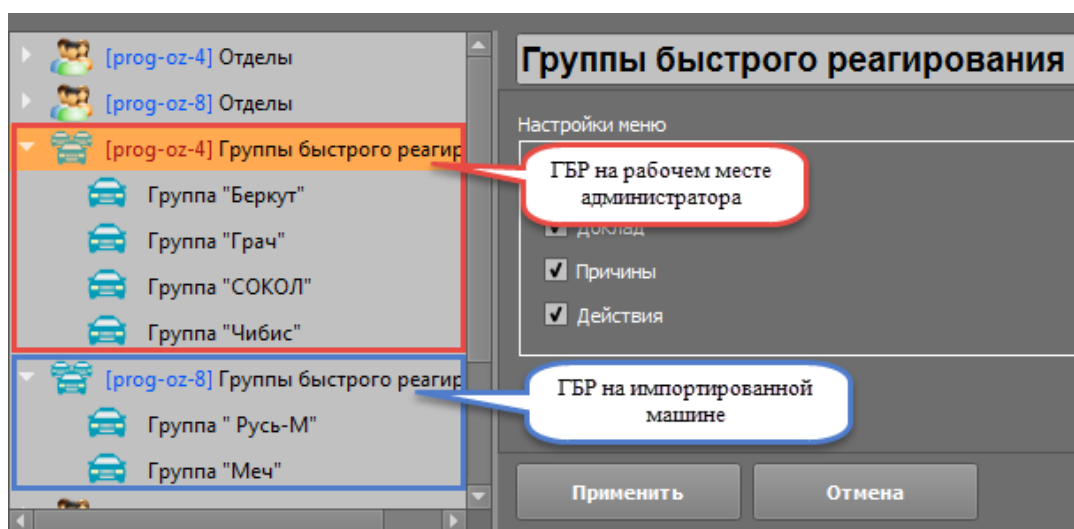


Рис. 14 Вариант отображения импортированных групп в менеджере конфигурации

«**Обслуживающий персонал**» - импорт данного типа разрешает просмотр и редактирование настроек (создание, удаление инженеров и техников, обслуживающих организаций.) обслуживающего персонала (вкладка «Персонал»). Импорт данного типа характерен, как правило, только для компьютеров, где будет дополнительное рабочее место администратора и персонала, у которого есть полномочия на редактирование данных типов в БД;

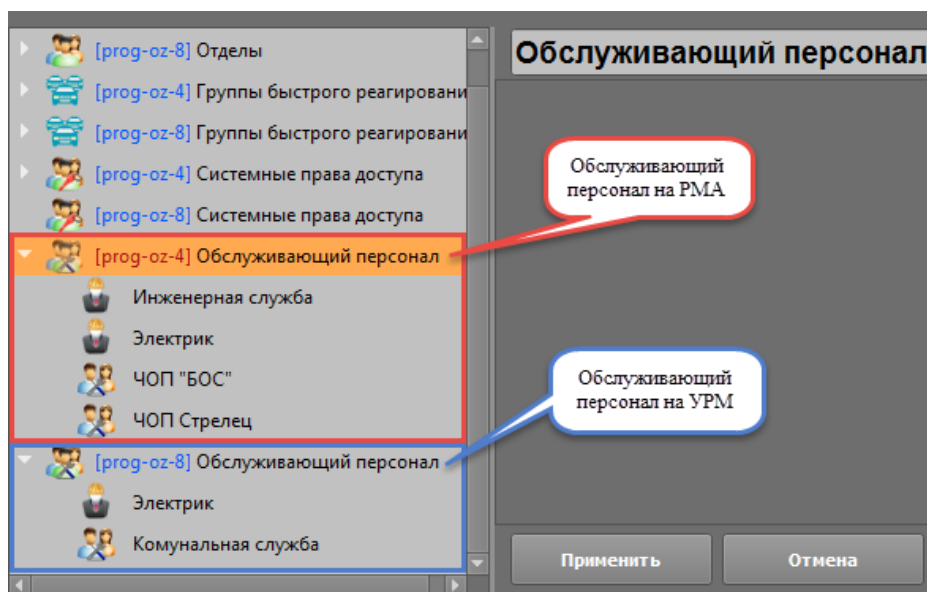


Рис. 15 Вариант отображения импортированных прав персонала в менеджере конфигурации

«**Объекты охраны**»- импорт данного типа дает возможность использовать и редактировать объекты охраны, созданные на импортированном компьютере в менеджере конфигурации (вкладка «Объекты охраны») и осуществлять их мониторинг и управление в рабочем месте оператора. Данный тип является основным и обязательным для работы сетевых ПК;

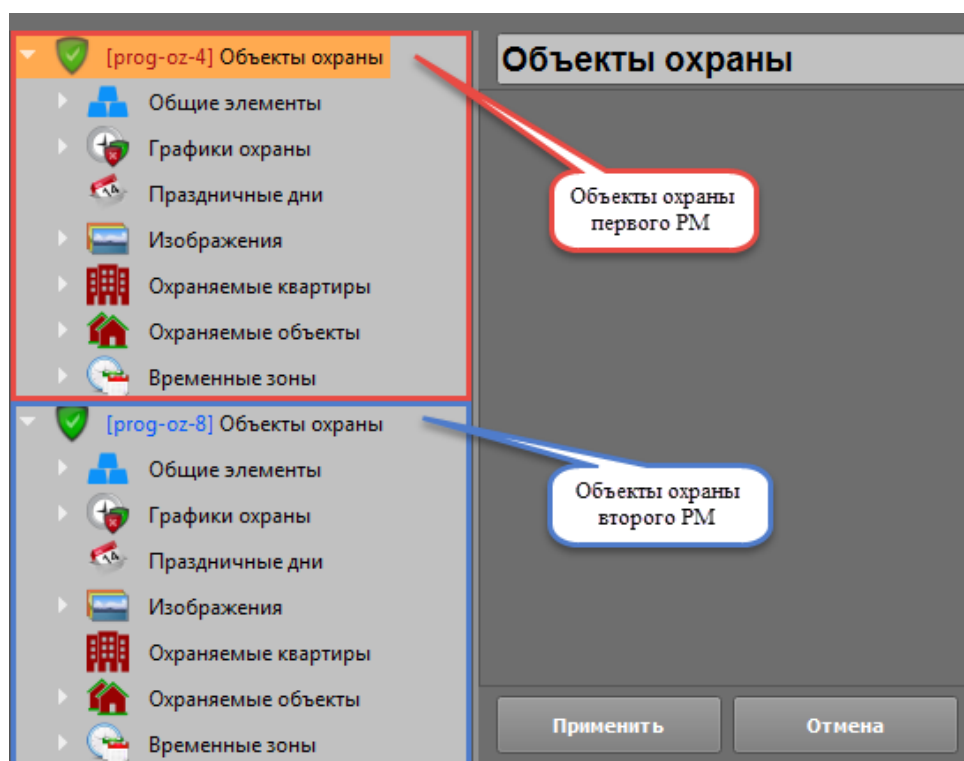


Рис. 16 Вариант отображения импортированных объектов охраны в менеджере конфигурации

«Отделы (Права доступа вкладка «Персонал»)» – импорт данного типа обеспечивает просмотр и редактирование настроек (создание\удаление сотрудников, переназначение прав, редактирование учётных данных и т.д.) обслуживающего персонала (вкладка «Персонал»). Данный тип характерен для ПК, где будет работать администратор. Редактирование и создание прав персонала целесообразно выполнять при импортированном типе «Отделы»;

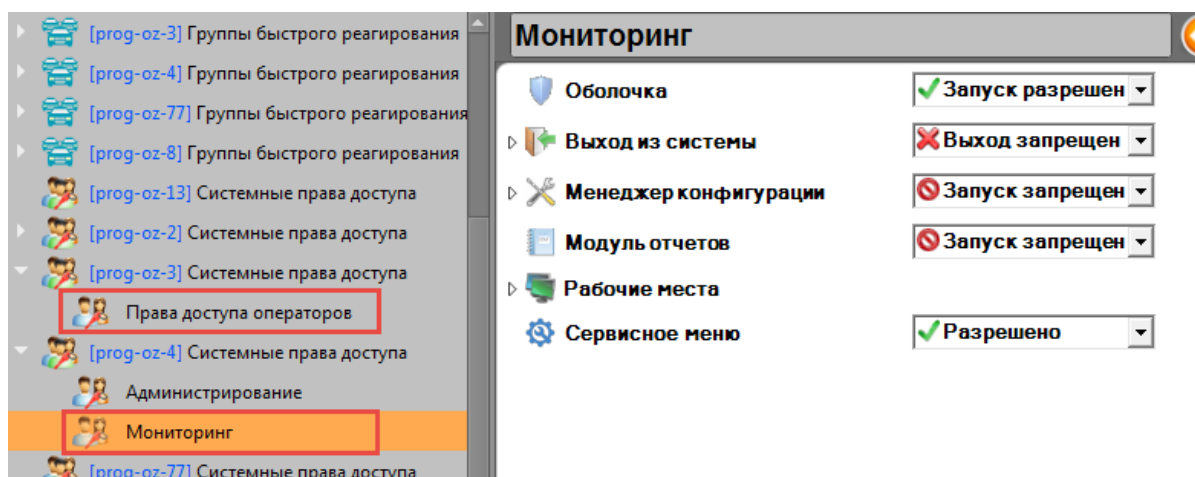


Рис. 17 Импортированные права доступа персонала

«Рабочие места (вкладка «Архитектура»)» - позволяет настраивать вкладку «импортируемые компьютеры» на удаленной машине. Данный тип позволяет администратору удалённо настраивать архитектуру импорта «соседних» машин;

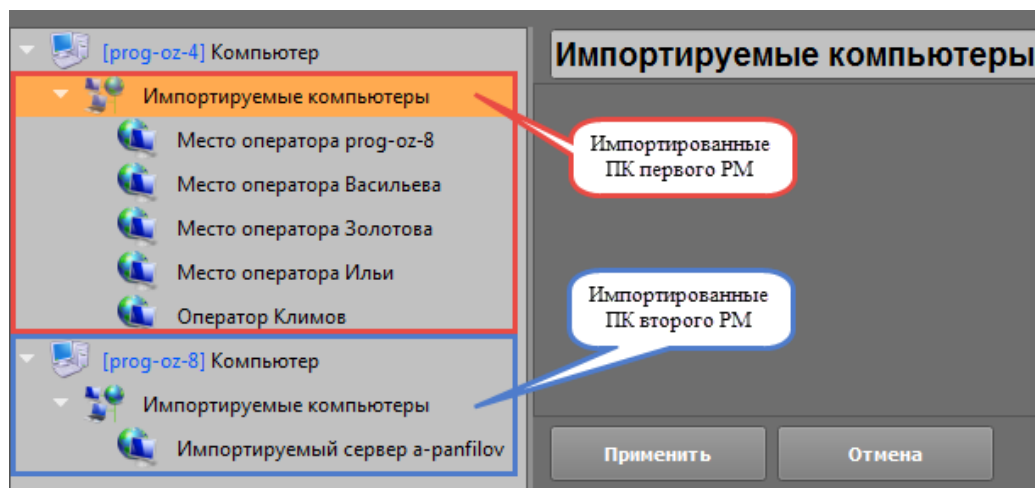


Рис. 18 Импортированные рабочие места «соседних» компьютеров

- **«Рабочие места операторов (вкладка «Рабочие места»)»** - импорт данного типа обеспечивает отображение и настройку рабочих мест на импортированном компьютере. Импорт данного типа не позволяет оператору запускать рабочие места, созданные на соседних машинах, поэтому импорт данного типа предназначен для компьютеров рабочих мест администратора;

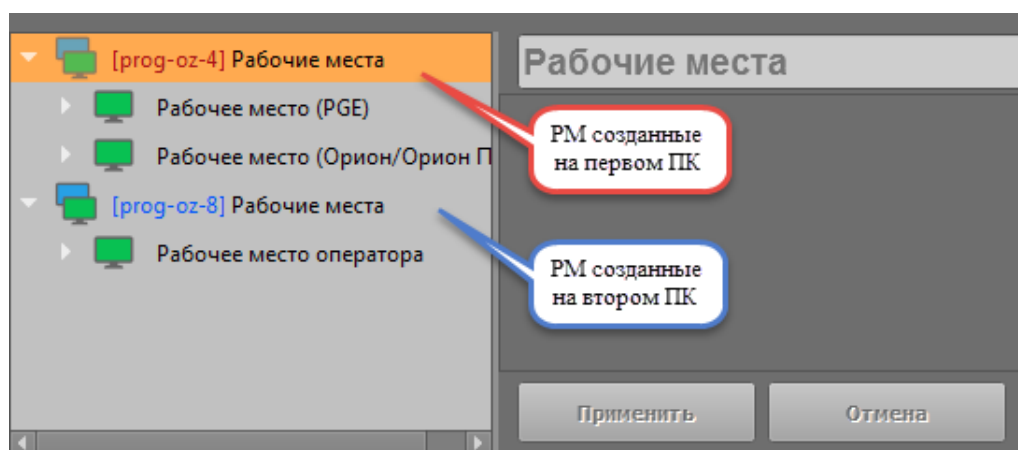


Рис. 19 Импортированные рабочие места «соседних» компьютеров

- **«Системные устройства (вкладка «Оборудование»)»** - импорт данного типа предназначен для просмотра и редактирования приборов, каналов связи, видеоподсистемы, личного кабинета. Для удалённых компьютеров, за которыми работает администратор, импорт системных устройств соседних машин является обязательным.

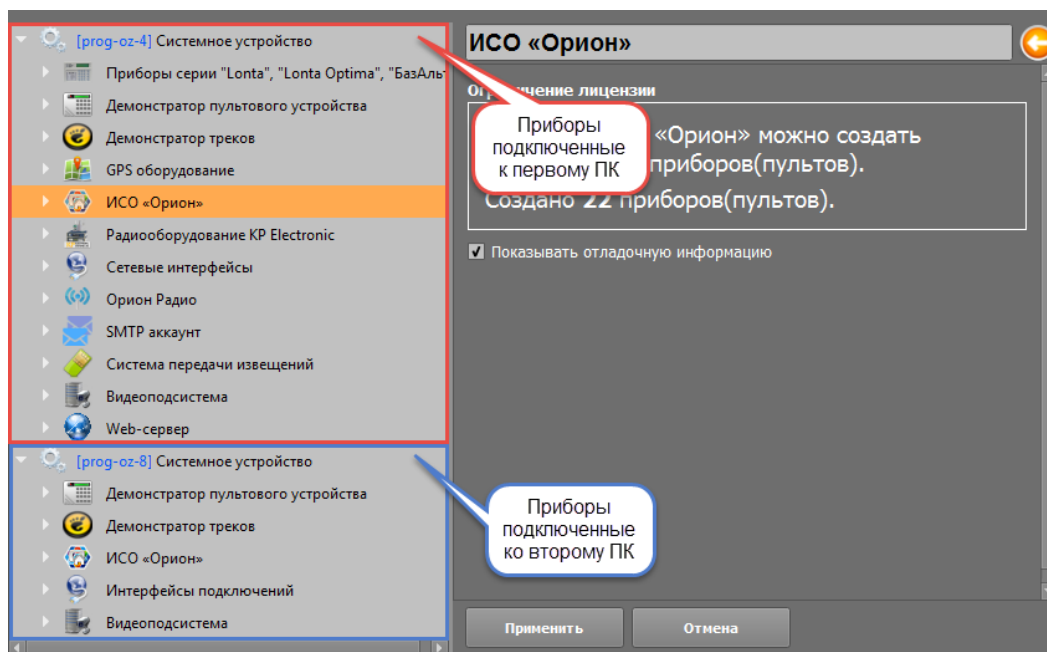


Рис. 20 Импортные рабочие места «соседних» компьютеров

В первую очередь, импорт типов необходим для администрирования удаленных рабочих мест, но часть типов является обязательными или рекомендуемыми для удаленных мест мониторинга (например, «Объекты охраны», «Группы быстрого реагирования», «Обслуживающий персонал»).

Необходимо учесть, что при использовании более сложных (комбинированных) схем сетевого режима, импорт типов может быть иным. Если предполагается, что на удаленной машине, к примеру, персонал будет иметь доступ к редактированию рабочих мест, или редактированию данных обслуживающего персонала, собственных прав доступа и прав других сотрудников персонала ПЦО, то необходимо отметить флагами типы «Отделы (права доступа)», «Обслуживающий персонал» и т.д. При использовании нескольких рабочих мест администратора в одной локальной сети, рекомендуется использовать полный импорт собственных объектов (типов) на обе машины.

После настройки архитектуры и импортирования типов, можно приступить к настройке прав персонала удаленной машины, создания рабочих мест и их настройки.

2.3.2 Настройка прав оператора удаленных мест (вкладка «Персонал»)

Вкладка «Персонал» предназначена для создания операторов и администраторов ПЦО, их полномочий для работы с системой, которые определяют доступ сотрудников к просмотру и редактированию отдельных вкладок менеджера конфигурации и запуску отдельных приложений Эгида-3.

Подробно о настройке прав персонала ПЦО описано в документе «03-Руководство администратора» подпункт «3.4 Вкладка «Персонал». Системные права доступа».

По умолчанию, на удаленной машине уже создан пользователь **Иванов Иван Иванович** с паролем на вход «123456». Он владеет максимальными правами на запуск менеджера конфигурации и всех созданных рабочих мест удаленной машины в рамках импортированных типов.

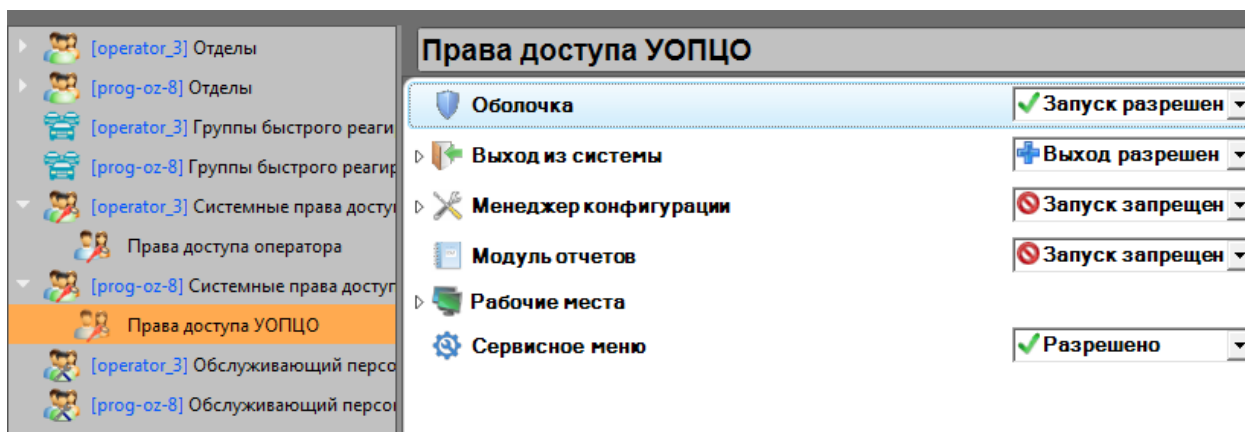


Рис. 21 Пример настройки прав персонала ПЦО удалённого компьютера

Перед созданием учетной записи удаленного оператора, нужно настроить права доступа, в которых будут указаны его полномочия. Для этого создается дочерний элемент во вкладке системные права доступа (на условном сервере) и настраиваются необходимые параметры для каждого из операторов.

После настройки прав доступа, нужно создать операторов, которые будут работать с местом мониторинга удалённой машины, заполнить их учётные данные и присвоить им созданные права доступа.

Рис. 22 Пример созданного оператора ПЦО

В группе настроек «Управление привилегиями» из списка назначенных прав, необходимо выбрать созданные ранее на этой машине права доступа. Создать пароль пользователя. Нажать клавишу применить.

Персоналу удалённой машины, можно задавать только права доступа созданные на этой конкретной машине.

Права доступа персонала удалённого рабочего места рекомендуется создавать уже после добавления рабочих мест и полномочий на управление, поскольку в правах доступа указываются полномочия персонала на запуск тех или иных рабочих мест.

2.3.3 Создание и настройка рабочих места операторов (вкладка «Рабочие места»)

По умолчанию, сразу после импорта типов во вкладке Архитектура, на удалённой машине не создано ни одного рабочего места, поэтому при запуске оболочки на удалённой машине, рабочее место будет отсутствовать.

Подробно о создании рабочих мест и конфигурировании модулей рабочего места (далее - РМ) описано в документе «03-Руководство администратора» подпункт «3.5 Вкладка «Рабочие места»».

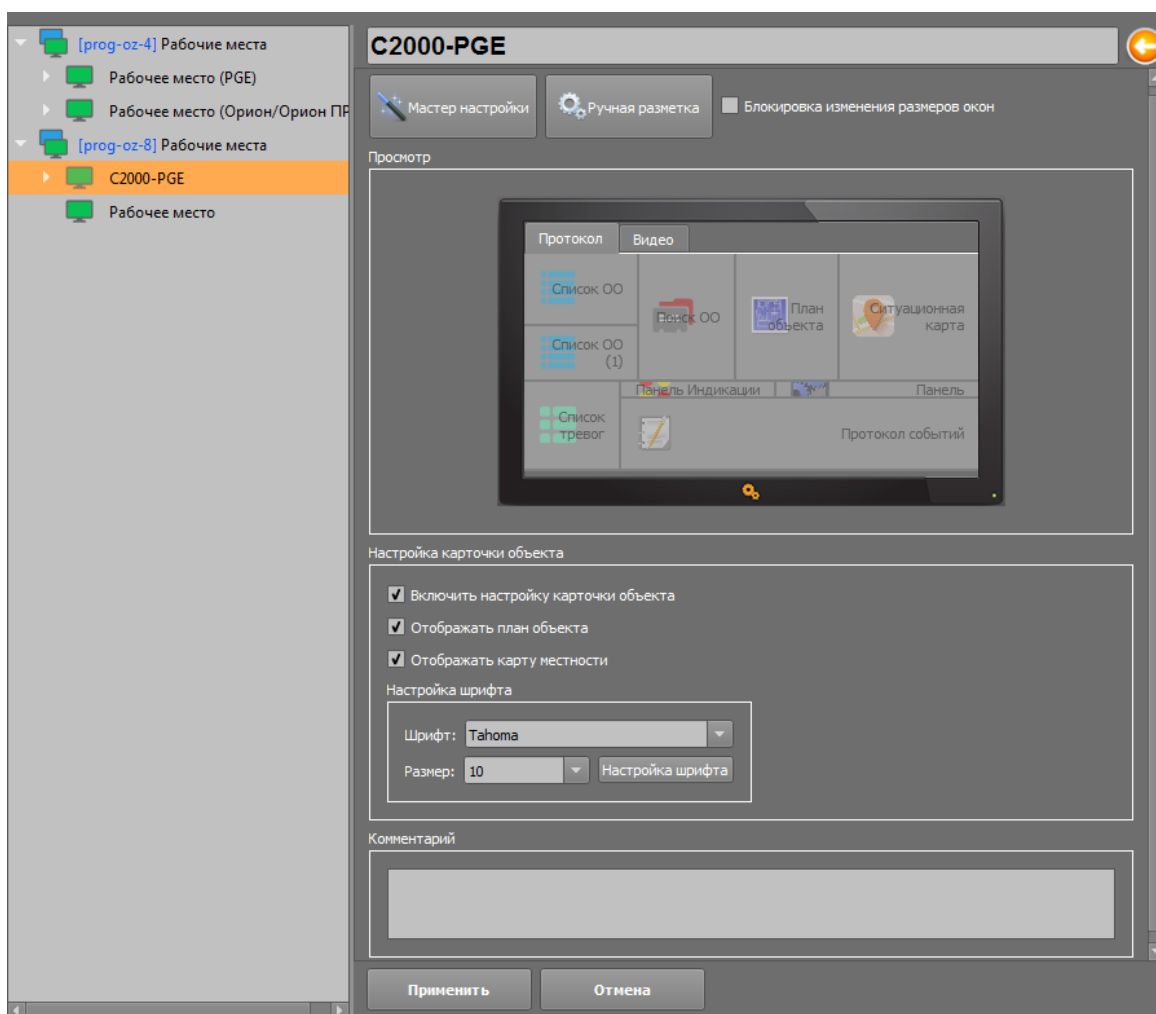


Рис. 23 Настройки рабочего места

Для создания РМ, в системных устройствах на вкладке «Рабочие места» выбрать импортированный ПК, у него создать дочерний элемент - «рабочее место».

Для упрощения процедуры создания рабочих мест со схожим расположением графических модулей на экране, рекомендуется пользоваться шаблонами. Т.е. необходимо предварительно создать шаблоны уже существующих рабочих мест.

Рекомендуется в настройках рабочих мест создавать полномочия на управление и фильтры объектов охраны.

«*Полномочия на управление ОО*» - это модуль рабочего места (компонент), который определяет права операторов на обработку событий (сброс состояний зон, реле, камер, приборов) и управление зонами, разделами, релейными выходами и камерами на конкретном рабочем месте. В системе можно создать только один модуль полномочий на каждое рабочее место.

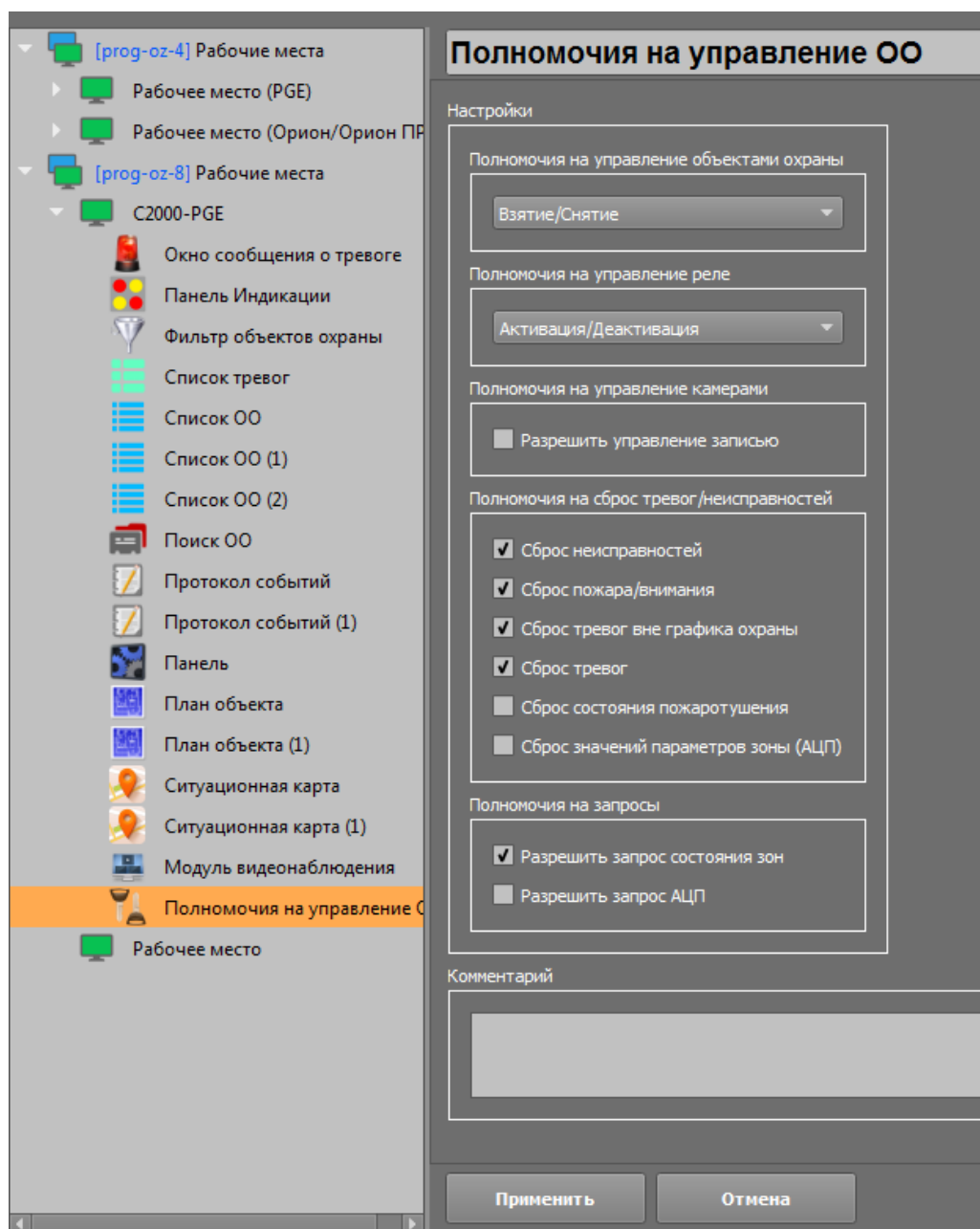


Рис. 24 Полномочия на управление ОО

Полномочия действительны для всех операторов рабочего места, не зависимо от их прав, настроенных во вкладке «Права доступа».

Фильтр объектов – это модуль, предназначенный для настройки отображения «Объектов охраны» и общих зон состояния приборов на рабочем месте. В системе можно создать только один «Фильтр объектов охраны» на каждое рабочее место.



По умолчанию при создании рабочего места на удаленной машине в фильтре ОО не будет выбрано ни одного объекта.

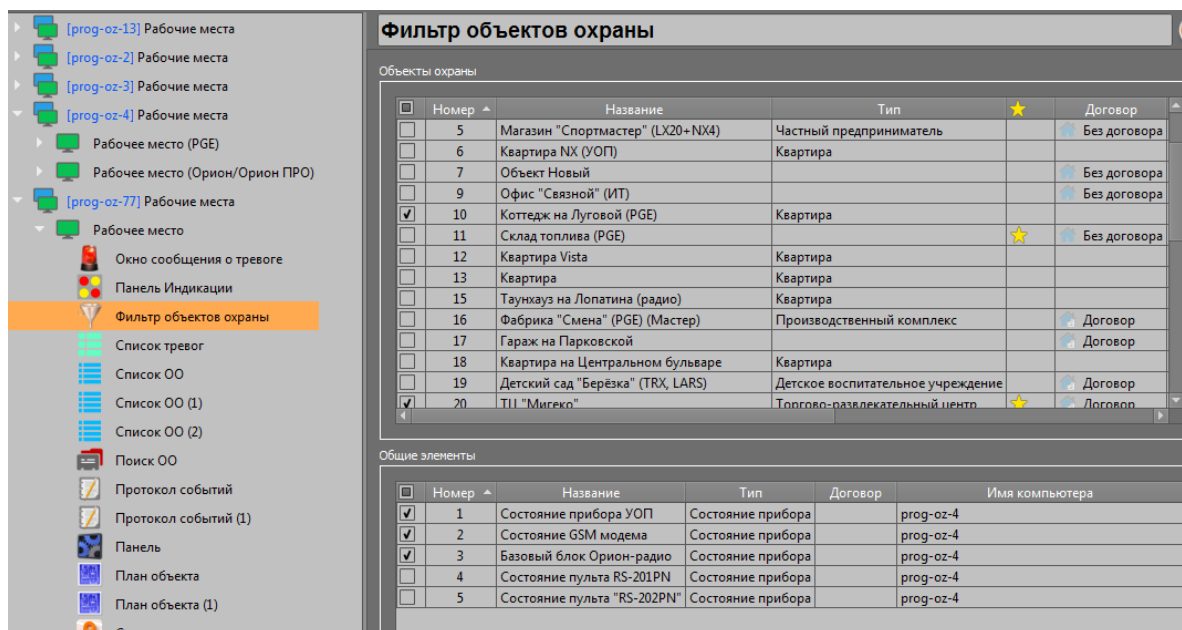


Рис. 25 Фильтр объектов охраны

Фильтр объектов является основным модулем, который определяет, за какими объектами охраны оператор будет вести наблюдение на данном рабочем месте. Распределение объектов охраны по рабочим местам осуществляется только с помощью фильтра объектов охраны.

После выполнения всех пунктов данного руководства необходимо проверить работоспособность системы.

2.3.4 Проверка работы Эгида-3 в сетевом режиме

Проверка работы удаленного рабочего места проходит в несколько этапов:

1. Вход в систему под учетной записью созданного сотрудника;
2. Запуск рабочего места;
3. Проверка отображения ОО в графических модулях списка или сетки объектов;
4. Проверка получения извещений, состояний приборов, тревог;
5. Проверка обработки тревог в модуле поиска (сброс);
6. Проверка управления зонами и разделами с удаленной машины;
7. Проверка работы с мобильными бригадами (вызов, отмена, отслеживание перемещения)
8. Проверка протоколирования действий оператора в протоколе событий на всех ПК, попадание действий оператора в отчёты. При Запуске Эгида-3 в окне выбора пользователя должен отображаться созданный оператор.

При запуске оболочки должен завестись модуль рабочего места, в нем должны отобразиться все объекты, указанные в фильтре ОО. При подключении удаленной машины в протоколе событий отображается сообщение установления связи, в протоколе событий на РМ администратора выводится похожее сообщение.

28.12.2017 Протокол событий - Без фильтра					
Дата/Время	Факт.время	Источник	Раздел	Зона	Сообщение
13:28:00		Рабочее место оператора			Связь установлена
13:27:56		Рабочее место администратора			Связь установлена

Рис. 26 Вывод сообщений о подключении импортированных ПК

Необходимо помнить, что при отсутствии подключения удалённого места к локальной или интернет сети, администратор не сможет изменять параметры импортированных типов, поэтому для внесения изменений в настройку объектов удалённых мест необходимо их постоянное подключение к локальной сети.

Особенности работы оператора в сетевом режиме, работа с видеоподсистемой, группами быстрого реагирования описаны в Главе 3.

Глава 3 Особенности работы удаленных рабочих мест в сетевом режиме

3.1 Особенности работы при разрыве связи с удаленным ПК

При разрыве связи между компьютерами, работающими в сетевом режиме, удалённые рабочие места узнают об этом от ядра Эгиды. В рабочее место будет выведено тревожное окно с сообщением о потере связи с конкретным рабочим местом, в протокол событий добавится соответствующая запись. Состояния объектов охраны, при потере связи с базой данных или другим ПК меняться не будет, поскольку в действительности не известно состояние объектов до момента возобновления связи, все эти объекты могут продолжать находиться на связи, в дежурном режиме, в состоянии охраны или в состоянии «снятия с охраны».

События о потере и восстановления связи с компьютерами сети Эгида-3 формируются и транслируются благодаря сервису транспортного уровня ядра Эгида-3.

При восстановлении связи с удаленным рабочим местом оператора в графических модулях рабочего места (протокол событий, окно тревожных сообщений, список объектов, список тревог и неисправностей и т.д.) отобразятся все накопленные события и состояния, которые приходили с объектов за время пропадания связи. После получения всех событий, в модулях «Список ОО» и «Поиск ОО» отобразятся последние состояния объектов, если тревоги до момента восстановления связи не были обработаны на других рабочих местах, то они появятся в списке тревог. Если тревожные события на момент разрыва связи были обработаны на других машинах работающих в сетевом режиме, то в списке тревог они отображены не будут.

На ПК с подключенным оборудованием, каналами связи и БД (место администратора) при разрыве связи с одной из машин появиться окно тревожных сообщений, сообщающее о разрыве соединения. Это событие также отобразиться в протоколе событий. При этом работа с объектами охраны и остальными удаленными местами не будет прерываться и продолжится в штатном режиме.

3.2 Особенности работы графических модулей рабочего места в сетевом режиме

При работе в сетевом режиме, на всех машинах синхронно осуществляется:

1. Смена состояний объектов охраны в «Списке ОО», на плане объекта, и на ситуационной карте;
2. Смена состояний реле, зон, разделов и камер в «Поиске ОО»;
3. Отображение всех событий, операций взятия\снятия с охраны, работы с ГБР в протоколе событий;
4. Отображение видео в видеомониторе с сетевых камер

При работе в сетевом режиме, при поступлении нештатного (тревожного события, неисправности, пожара, внимания и т.д.) события «Окно тревожных сообщений» появляется на рабочих местах всех удалённых машин. Одновременно с окном тревожных сообщений в протоколы событий приходит соответствующее событие, меняется состояния элементов объектов

охраны. Если оператор принимает данное извещение (реагирует), то окно «пропадает» только с конкретного рабочего места. На остальных рабочих места удалённых машин окно тревожных сообщений будет отображаться до тех пор, пока их операторы не отреагируют на него.

В настройках рабочего места (вкладка «Рабочие места») в конфигурации окна тревожных сообщений, существует возможность задать «Время реакции оператора на тревогу». При включении данного параметра в протоколе событий будет отображаться запись об отсутствии реакции оператора на тревожное событие. При принятии тревожного сообщения в протоколе событий выводится информация о времени, которое потребовалось оператору для реагирования на тревожное событие.

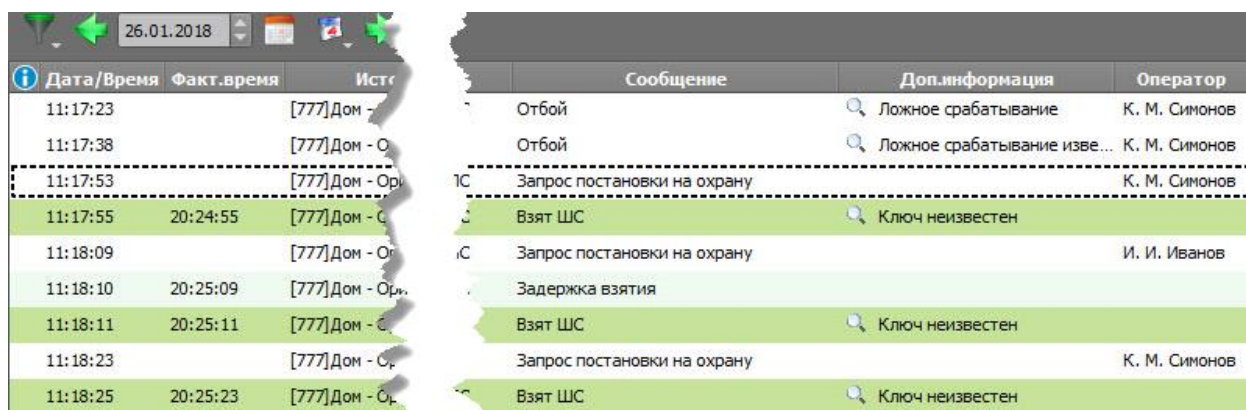


Дата/Время	Факт.время	Источник	Сообщение	Доп.информация	Оператор
11:08:24	20:15:23	[777]Дом - Ормон Про	Тревога		
11:08:29		Окно сообщения о тревоге	Отсутствие реакции оператора на тре...	Симонов Константин Михай...	
11:08:39		Окно сообщения о тревоге	Задержка реакции оператора на трев...	Время задержки: 10 с.	К. М. Симонов

Рис. 27 Отображение задержки реакции оператора

Список тревог, в отличие от окна тревожных сообщений, отображает событие до момента, пока оно не будет обработано кем-то из операторов одной из машин. По мере отбоя тревог в списке операторами, они удаляется из списка тревог на всех машинах. В протоколе событий в столбце «Дополнительная информация», отображается комментарий оператора к данному действию, в столбце «Оператор» отображается ФИО оператора, выполнившего действие по отбою тревоги в списке.

Принцип протоколирования действий оператора общий для всех действий оператора: принятие событий, отбой, вызов и работа с мобильными группами, сброс тревог и неисправностей, управление объектами, камерами и прочее. Все эти действия оператора, включая смену рабочих мест, выгрузку и загрузку оболочки будут отображаться на других сетевых рабочих местах в протоколе событий.



Дата/Время	Факт.время	Ист	Сообщение	Доп.информация	Оператор
11:17:23		[777]Дом -	Отбой	Ложное срабатывание	К. М. Симонов
11:17:38		[777]Дом - О	Отбой	Ложное срабатывание изве...	К. М. Симонов
11:17:53		[777]Дом - О	Запрос постановки на охрану		К. М. Симонов
11:17:55	20:24:55	[777]Дом - С	Взят ШС	Ключ неизвестен	
11:18:09		[777]Дом - О	Запрос постановки на охрану		И. И. Иванов
11:18:10	20:25:09	[777]Дом - О	Задержка взятия		
11:18:11	20:25:11	[777]Дом - С	Взят ШС	Ключ неизвестен	
11:18:23		[777]Дом - О	Запрос постановки на охрану		К. М. Симонов
11:18:25	20:25:23	[777]Дом - О	Взят ШС	Ключ неизвестен	

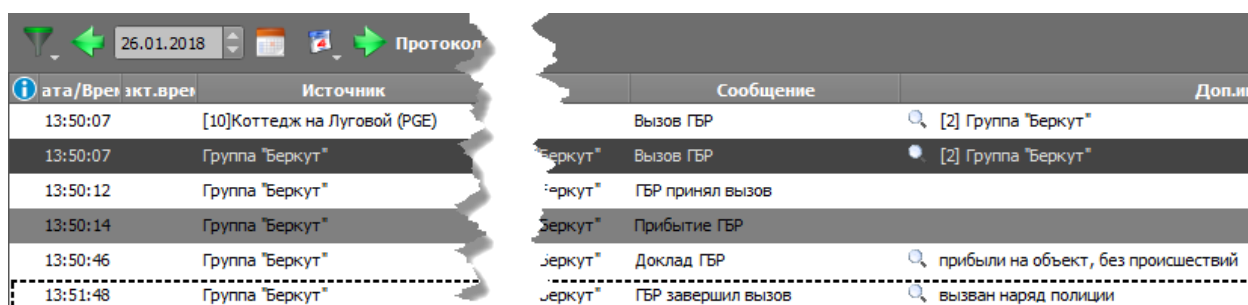
Рис. 28 Работа в сетевом режиме

На ситуационной карте операторы получают информацию о состоянии объектов охраны, и о передвижении групп быстрого реагирования, если данные группы импортированы на удаленные машины. При этом построение треков передвижения импортированных групп возможно на всех рабочих местах, куда производился импорт.

3.3 Работа с ГБР в сетевом режиме

Существует несколько вариантов распределения групп быстрого реагирования по рабочим местам:

Одна из распространённых моделей построения клиент-серверной архитектуры, это модель где все группы, мобильные устройства и GPS - трекеры созданы на одном ПК, где расположена БД и подключены пульты устройства или каналы связи (условном сервере). Эти группы импортированы на удалённые рабочие места операторов. Соответственно, все операторы одновременно могут видеть эти группы у себя на рабочих местах и работать с ними: вызывать эти группы на объекты охраны, отменять вызовы, следить за передвижением групп на интерактивной карте.



The screenshot displays a software interface with two main panels. The left panel shows a log of events with columns for time, source, and message. The right panel shows a list of messages with columns for message content and additional information.

Дата/Время	Источник	Сообщение	Доп.ин
13:50:07	[10]Коттедж на Луговой (PGE)	Вызов ГБР	[2] Группа "Беркут"
13:50:07	Группа "Беркут"	Вызов ГБР	[2] Группа "Беркут"
13:50:12	Группа "Беркут"	ГБР принял вызов	
13:50:14	Группа "Беркут"	Прибытие ГБР	
13:50:46	Группа "Беркут"	Доклад ГБР	прибыли на объект, без происшествий
13:51:48	Группа "Беркут"	ГБР завершил вызов	вызван наряд полиции

Рис. 29 Вызов ГБР на объект

В этом случае, все данные координат групп, отчёты по действиями групп отсылаются на WEB сервер условного сервера и далее транспортом ядра рассылаются на другие рабочие места операторов. Аналогично и для отправки вызовов – вызов идёт через WEB сервер условного сервера, а команды до сервера с удалённых машин передаёт транспорт ядра.

Преимущества такой схемы – использование одного WEB сервера, удобство редактирования параметров групп, замены IMEI мобильных устройств, удобство при импортировании групп на удалённые рабочие места.

Из недостатков можно выделить невозможность распределения групп по рабочим местам, если устав предусматривает работу оператора только со «своими» мобильными группами.

Если требуется распределение мобильных групп по рабочим местам, то, мобильные устройства и веб-сервер создаются на условном сервере, а группы быстрого реагирования – на сетевых рабочих местах операторов. Для корректной работы данной конфигурации необходимо кроме основных «Импортированных типов»: «Объекты охраны», «Рабочие места» операторов и «ГБР», импортировать тип «Системные устройства (вкладка «Оборудование»)».

После этого, созданным ГБР привязываются мобильные устройства или GPS-трекеры, созданные на условном сервере.

Если необходимо работать с одной и той же группой на нескольких рабочих местах, то необходимо осуществить импорт типа на данную машину.

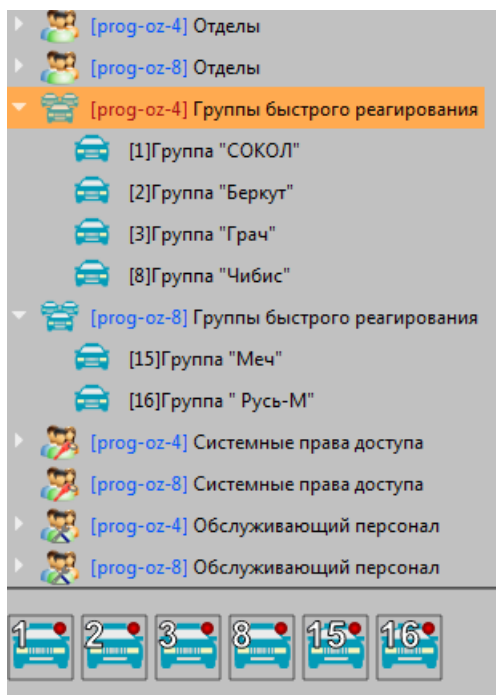


Рис. 30 ГБР, созданные на нескольких РМО

Вызов группе с разных рабочих мест ничем не отличается друг от друга, в мобильном приложении отображается только объект охраны с адресом без уточнения события, по которому осуществлён вызов.

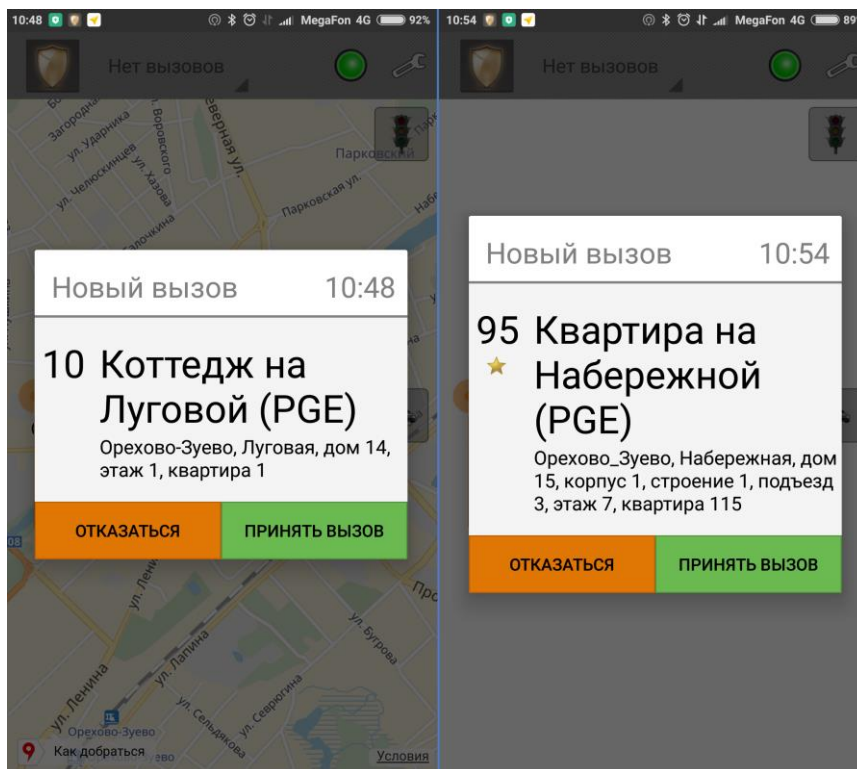


Рис. 31 Вызов группы с разных рабочих мест

Доклад группы попадает на ПК, где настроен канал связи и запущен WEB сервер и далее рассылается только тем ПК, у которых осуществлён импорт этих групп. При изменении статуса группы (прибытие, отмена, завершение вызова), статус группы в списке тревог, списке объектов, панели ГБР, ситуационной карты меняется синхронно на всех рабочих местах.

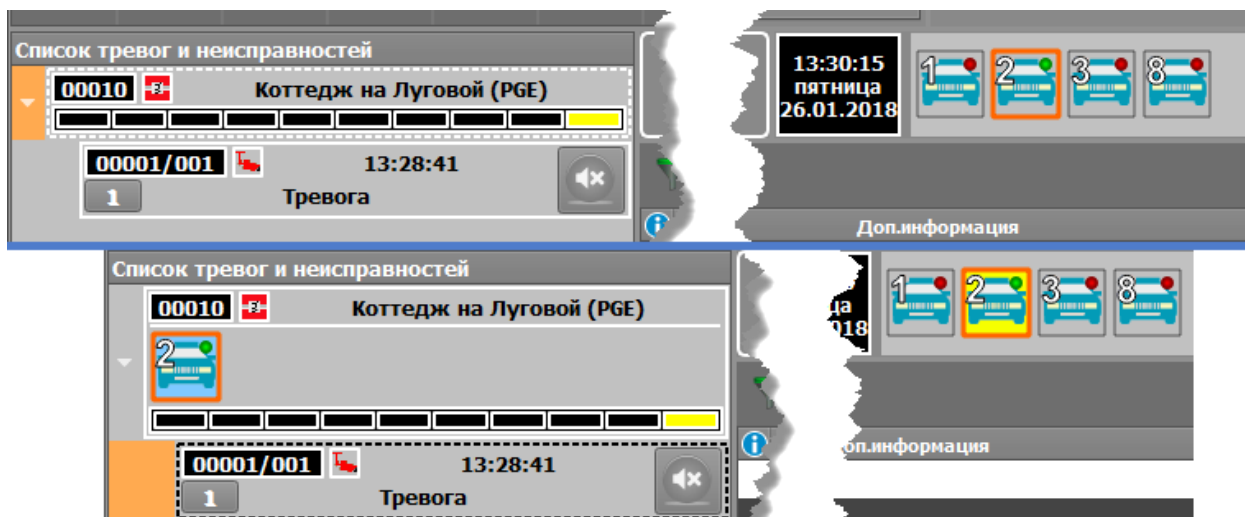


Рис. 32 Изменение статуса ГБР

Если кто-то из операторов в сети завершает или отменяет вызов группы, то на всех рабочих местах статус группы меняется, при этом в протоколе событий выводиться сообщение отмены вызова с ФИО оператора отменившего вызов.

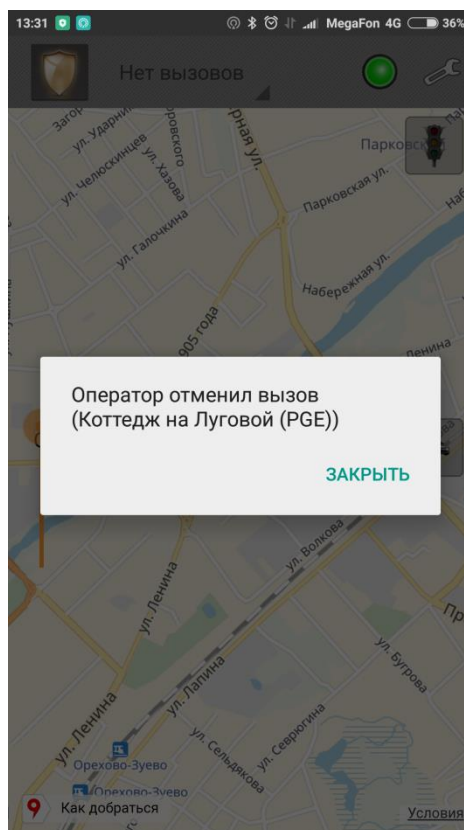


Рис. 33 Сообщение об отмене вызова на мобильном устройстве

На самом же мобильном устройстве отображается только сообщение об отмене вызова оператором на данный объект охраны.

3.4 Удаленное управление реле, зонами и разделами в сетевом режиме

Существует несколько вариантов управления зонами и разделами, релейными выхода, удалённых рабочих мест:

- С помощью SMS сообщений используя GSM модем;
- Путём непосредственной отправки команд управления в интерфейс линии связи, используя протоколы «Орион» и «Орион - ПРО».

При управлении через GSM модем, необходимо помнить, что управление возможно только теми объектами охраны, которые импортированы на данный ПК, при этом сама иерархия приборов (вкладка «Оборудование» менеджера конфигурации) может быть не импортирована на другую машину. GSM модем, как правило, подключен к условному серверу, т.е. компьютеру где создана иерархия оборудования.

При наличии нескольких ПК с подключенным охранным оборудованием, для их удаленного управления необходимо наличие модема на каждом из них. В данной схеме, GSM модем управляет объектами охраны только конкретного рабочего места (соответственно иерархия оборудования и объектов охраны создана непосредственно на нём). Такой вариант схемы работы позволяет распределить нагрузку по объектам на несколько модемов, обеспечить раздельное управление объектами по правам операторов.

При управлении через протоколы «Орион/Орион - ПРО», команды управления передаются непосредственно в интерфейс линии связи с оборудованием (RS232/485, локальная сеть), при этом в сетевом режиме работы сохраняется тот же принцип работы, что и при управлении по GSM – если объекты охраны импортированы на ПК, а само оборудование подключено к другому компьютеру, то команды управления транслируются ядром Эгиды (при наличии соответствующих полномочий у оператора). При использовании нескольких ПК, к каждому из которых подключено оборудование, необходимо осуществить взаимный импорт объектов охраны, чтобы можно было вести перекрёстное управление. Последний вариант сетевого режима может быть использован в крупных мониторинговых центрах, куда сводится информация с каких-то более мелких региональных центров со своей сетью объектов охраны и оборудованием.

3.5 Работа с видеоподсистемой в сетевом режиме

Видеоподсистема Эгида-3 - служит для получения видеокадров с установленных на объектах охраны сетевых камер, по каналу Ethernet / Internet. Сетевой режим предусматривает работу как с FTP камерами, так и с камерами, работающими по сети (Onvif). Особенности работы с камерами видеоподсистемы подробно описаны в руководстве: «15-Видеоподсистема».

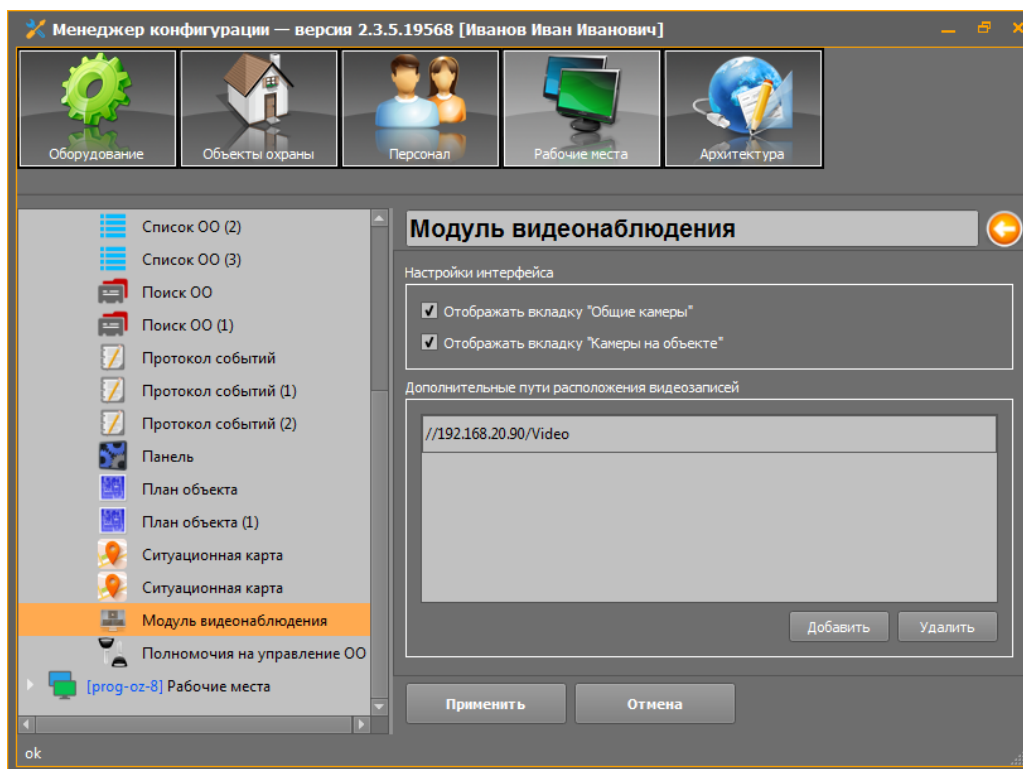


Рис. 34 Модуль видеонаблюдения

При работе с сетевыми камерами, работающими по FTP, оператор может получить тревожный вызов в рабочем месте при тревоге детектора камеры, получить доступ к удалённому видеоархиву и просмотреть тревожные видеозаписи в плеере, управлять режимами охраны камер (постановка и снятие с охраны).

При работе с сетевыми камерами, подключенными по RTSP (камеры с поддержкой технологии Onvif), механизмы сетевого режима передают видеопоток с камер, которые могут быть реально подключены к другим компьютерам сети. Т.е. оператор удалённой машины в рабочем месте может получать видеоизображение с камеры, подключённой, например, к условному серверу.

В обоих случаях, для работы оператора с камерами необходимо добавить в компоновку рабочего места модуль видеонаблюдения и указать дополнительные пути расположения видеозаписей, если на объектах охраны используются FTP камеры. Для совместной работы с камерами, необходимо импортировать объекты охраны машин, куда подключены камеры, а также импортировать вкладку «Рабочие места».

Начиная с версии 6.3.3, в Эгиде появилась возможность хранить видеоархивы на удалённом сервере, т.е. FTP сервером для хранения видеофрагментов не обязательно должен быть ПК с Эгидой, а может выступать компьютер, который входит в одну локальную сеть с ПК, на котором размещена БД и модули Эгиды-3.

Для доступа к видеофрагментам с удалённых рабочих мест по сетевому пути, необходимо прописать этот абсолютный путь в настройках модуля видеоподсистемы (вкладка Рабочие места). После этого, каждое из рабочих мест оператора будет иметь доступ к общей папке, где хранятся видеофайлы FTP камер. Обязательным условием является наличие доступа к данной папке для всех ПК, на которых будет запущено рабочее место оператора.

Для того, чтобы разрешить оператору управлять камерами необходимо выбрать соответствующий пункт в «Полномочия на управление ОО» на рабочем месте оператора.

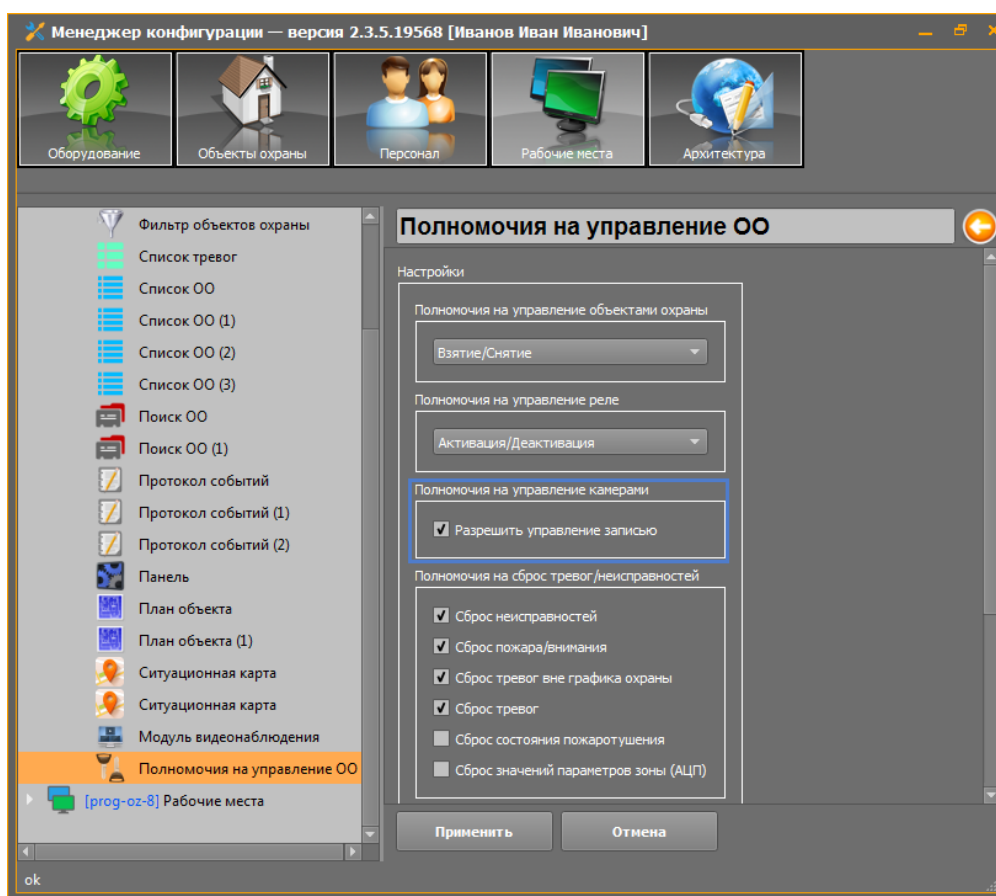


Рис. 35 Полномочия на управление ОО

При управлении камерами - постановкой и снятием с охраны, включении и отключении записи, обработки событий, в протоколе событий сетевых рабочих мест отображается информация по действиям оператора с подписью ФИО оператора, выполнившего операцию.