

УПРАВЛЕНИЕ ДОСТУПОМ В СИСТЕМЕ ИНФРАМЕНЕДЖЕР

РУКОВОДСТВО АДМИНИСТРАТОРА

ОГЛАВЛЕНИЕ

Общее описание возможностей разграничения доступа в системе ИнфраМенеджер	3
Для распределения ответственности в соответствие с ролью в ИТ-процессах.....	3
Для распределения ответственности в территориально распределенных и/или филиальных организациях	5
Описание настроек для разграничения доступа в системе ИнфраМенеджер.....	10
Права на определение прав доступа	10
Определение зон ответственности пользователей.....	11
Дублирование зоны ответственности у нескольких пользователей.....	12
Работа в службе поддержки	13
Права на ведение справочников и различных настроек модуля Служба поддержки	13
Общие права на работу с заявками / заданиями / проблемами	14
Права на просмотр информации о поступающих в службу поддержки заявках / заданиях / проблемах	15
Работа с неклассифицированными заявками	16
Особенности работы руководителей ИТ-отделов	17
Роли для конечных пользователей	18
Использование зоны ответственности для автоматического назначения владельцев / исполнителей заявок / заданий / проблем.....	18
Исключения: работа администратора системы	19
Часто задаваемые вопросы	19
Описание стандартных ролей.....	21
Работа с базой данных ИТ-конфигураций	22
Права на ведение справочников и различных настроек модуля Управление конфигурациями	22
Права на работу с объектами	22
Описание стандартных ролей.....	23

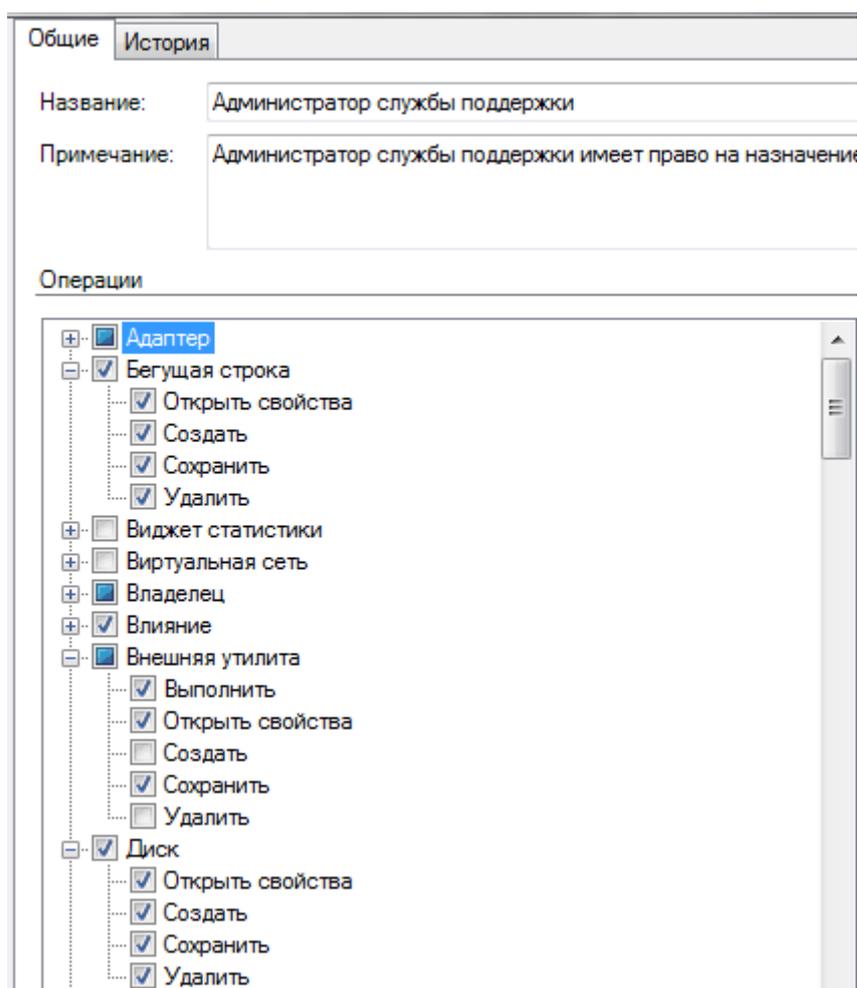
ОБЩЕЕ ОПИСАНИЕ ВОЗМОЖНОСТЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМЕ ИНФРАМЕНЕДЖЕР

ДЛЯ РАСПРЕДЕЛЕНИЯ ОТВЕТСТВЕННОСТИ В СООТВЕТСТВИИ С РОЛЯМИ В ИТ-ПРОЦЕССАХ

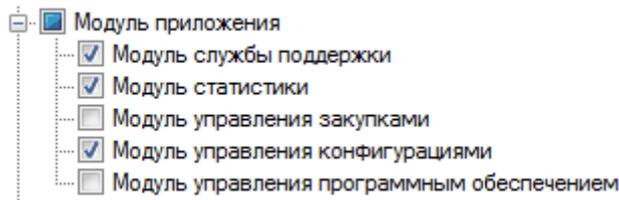
ИнфраМенеджер позволяет гибко разграничить доступ на уровне операций со всеми объектами системы:

1. Ограничить доступ к ведению справочников и выполнению различных настроек, например:
 - a. Выделить отдельно права на ведение портфеля сервисов, справочника кратких описаний заявок, ведение библиотеки шаблонов заданий, формирование регламентных работ и т.п.
 - b. Выделить отдельно права на формирование каталога оборудования разных категорий (ответственность за окончательное оборудование; ответственность за формирование каталога элементов СКС и т.п.)
2. Ограничить доступ к объектам разных видов, например:
 - a. Предоставить возможность работы только с заявками (исключить возможность работы с заданиями и проблемами)
 - b. Предоставить возможность работы только с оборудованием определенных категорий (выделить ответственных только за пользовательскую технику; только за сетевое оборудование; только за объекты СКС и т.п.)

Для настройки данных возможностей используется редактор ролей, позволяющий ограничить доступ к каждой операции с каждым объектом системы:



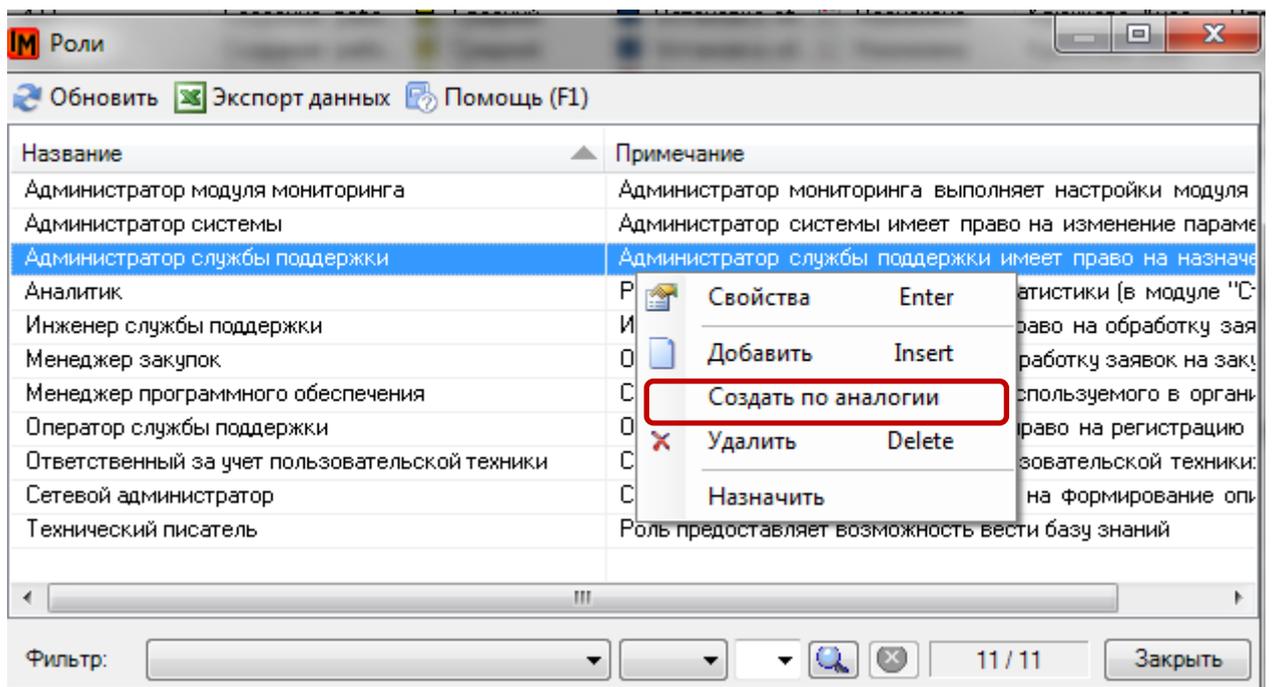
Отдельно можно закрыть доступ на всю информацию, содержащуюся в определенных модулях системы ИнфраМенеджер:



При развертывании базы данных системы ИнфраМенеджер по умолчанию создается набор рекомендуемых ролей с учетом типового распределения ответственности по процессам ИТ:

Название	Примечание
Администратор модуля мониторинга	Администратор мониторинга выполняет настройки модуля
Администратор системы	Администратор системы имеет право на изменение параметров
Администратор службы поддержки	Администратор службы поддержки имеет право на назначение
Аналитик	Роль позволяет создавать панели статистики (в модуле "С
Инженер службы поддержки	Инженер службы поддержки имеет право на обработку зая
Менеджер закупок	Ответственный за формирование и обработку заявок на закуп
Менеджер программного обеспечения	Сотрудник, отвечающий за каталог используемого в органи
Оператор службы поддержки	Оператор службы поддержки имеет право на регистрацию
Ответственный за учет пользовательской техники	Сотрудник, отвечающий за учет пользовательской техники:
Сетевой администратор	Сетевой администратор имеет право на ведение документ
Системный администратор	Сотрудник, отвечающий за учет сетевого оборудования, ег
Технический писатель	Роль предоставляет возможность вести базу знаний

Разрешения в данных ролях соответствуют названию и описанию роли. Можно использовать данный набор ролей, а можно создать собственные, «с нуля», или по аналогии с существующей:



ДЛЯ РАСПРЕДЕЛЕНИЯ ОТВЕТСТВЕННОСТИ В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННЫХ И/ИЛИ ФИЛИАЛЬНЫХ ОРГАНИЗАЦИЯХ

ИнфраМенеджер позволяет:

1. Ограничить доступ к информации, обрабатываемой в системе, в соответствии с зоной ответственности ИТ-сотрудников:
 - a. **В рамках работы службы Service Desk:** только заявки от пользователей из своих организационных единиц; только задания, назначенные на своих коллег
 - b. **В рамках работы с базой данных ИТ-конфигураций (CMDB):** только с оборудованием определенных типов, находящимся в определенных зданиях / этажах / комнатах
2. Ограничить доступ на ведение справочников системы:
 - a. **Оргструктура и список пользователей** (свои подразделения / организации; пользователи)
 - b. **Каталог оборудования** (только по определенным типам оборудования)

Для этого предусмотрены возможности для каждого ИТ-сотрудника указать:

- **Территориально-организационную зону ответственности** (за пользователей из каких организаций / подразделений, располагающихся в каких зданиях / комнатах / этажах, отвечает данный сотрудник)
- **Территориально-технологическую зону ответственности** (за оборудование каких типов, располагающееся в каких зданиях / комнатах / этажах, отвечает данный сотрудник)

Пример 1: организация имеет несколько территорий, достаточно удаленных друг от друга. На каждой территории выделяется свои ответственные ИТ-сотрудники, выполняющие роли ответственных за учет ИТ-имущества на своей территории и первой линии поддержки на своей территории. Для таких ИТ-сотрудников ИнфраМенеджер позволит:

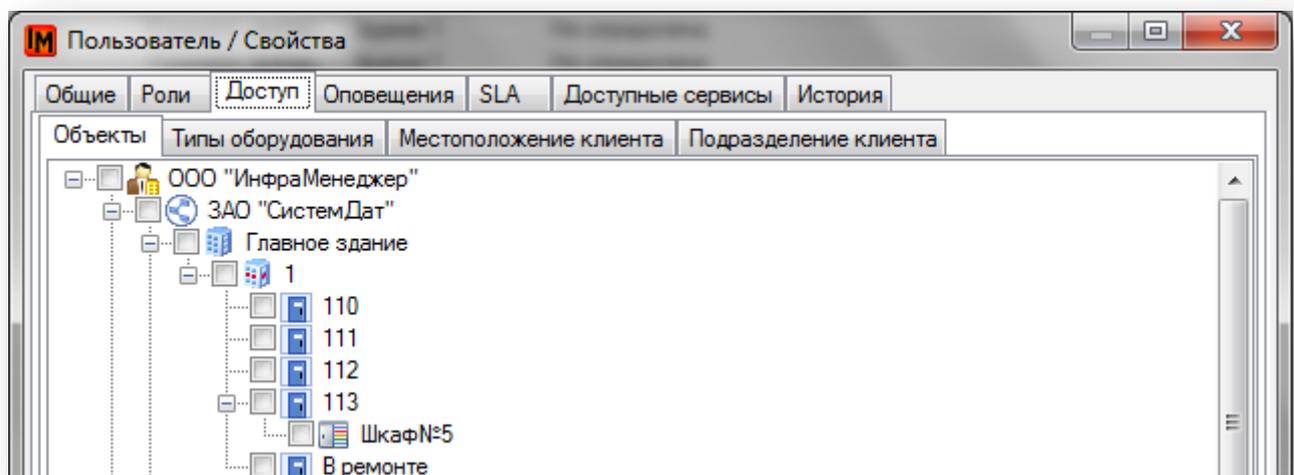
- **По территориально-технологической зоне ответственности:**
 - Ограничить доступ к заявкам по местоположению пользователя (только от пользователей, имеющих рабочие места в **выделенных зданиях / этажах / комнатах**)
 - Ограничить доступ на просмотр и редактирование оборудования по местоположению оборудования (находящееся только в **выделенных зданиях / этажах / комнатах**) и по типу оборудования (например: только компьютеры или только серверы и т.п.)
 - Ограничить доступ на редактирование каталога оборудования в рамках определенных типов оборудования
- **Ограничить доступ к заявкам по определенным сервисам**

Пример 2: организация имеет несколько удаленных филиалов / дочерних компаний, в каждой из которых есть свой ИТ-отдел, обслуживающие свои филиалы. Для сотрудников данных ИТ-отделов ИнфраМенеджер позволит:

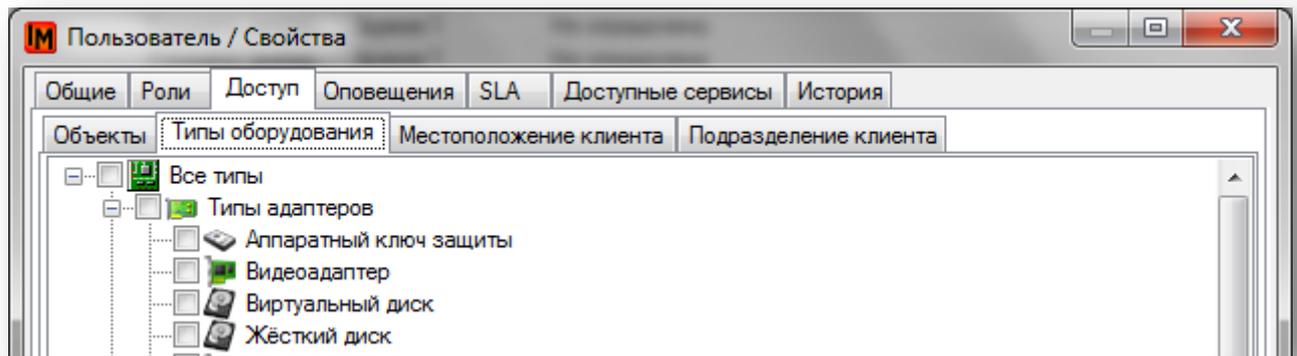
- **По территориально-организационной зоне ответственности:**
 - Ограничить доступ к заявкам по оргструктуре пользователя (только от пользователей, работающих в определенных **организациях / подразделениях**)
- **По территориально-технологической зоне ответственности:**
 - Ограничить доступ на просмотр и редактирование оборудования по местоположению оборудования (находящееся только на рабочих местах пользователей из определенных **организаций / подразделений**)
 - Ограничить доступ на редактирование справочника организаций и подразделений (только в рамках своего **филиала / дочерней компании** или своих **подразделений**)
 - Ограничить доступ на редактирование каталога оборудования в рамках определенных типов оборудования
- **Ограничить доступ к заявкам по определенным сервисам** (например, не показывать заявки, поступающие по централизованным сервисам, ответственность за обслуживание которых лежит на центральном аппарате)

Территориально-технологическая и территориально-организационная зоны ответственности указываются для каждого сотрудника, в его свойствах (пункт меню «Объекты» -> «Пользователи» -> Свойства пользователя):

- **Определение территориально-технологической зоны ответственности (ТТЗ):**
 - На закладке «Объекты» указывается ответственность за оборудование по его местоположению (распространяется на просмотр и редактирование информации об объектах ИТ-инфраструктуры, расположенных в указанных зданиях / этажах / комнатах / шкафах, с учетом типов оборудования, указываемых на закладке «Типы оборудования»)

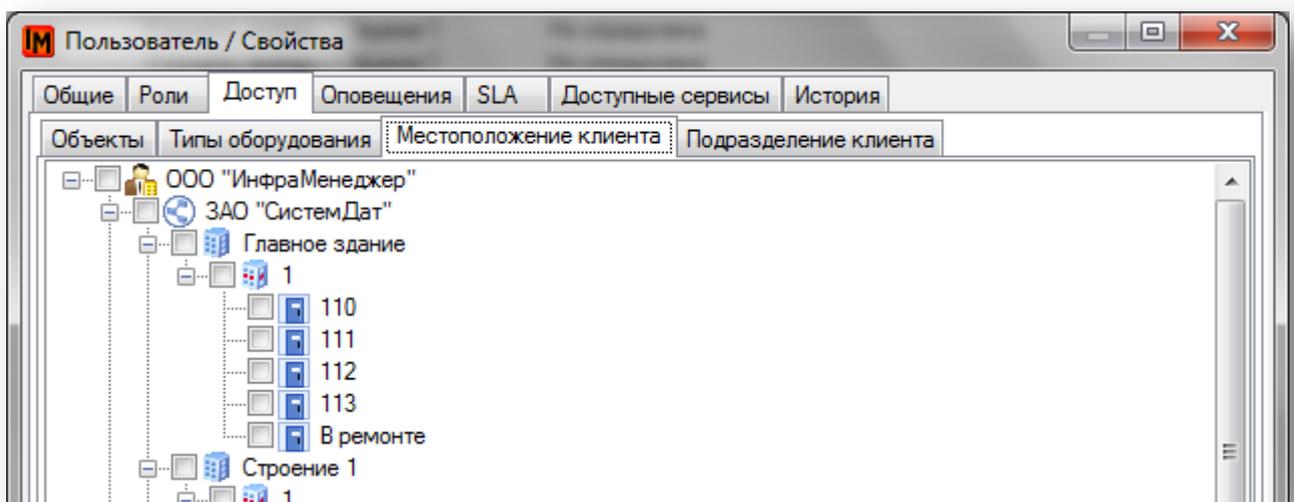


- На закладке «Типы оборудования» указывается ответственность оборудование определенных типов (с учетом местоположения оборудования, указываемого на закладке «Объекты»)

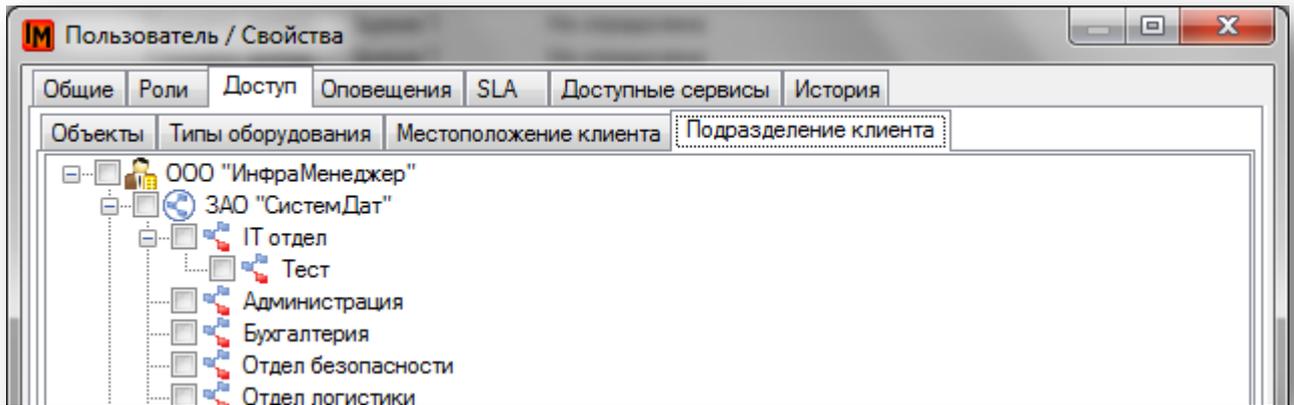


- **Определение территориально-организационной зоны ответственности (ТОЗ):**

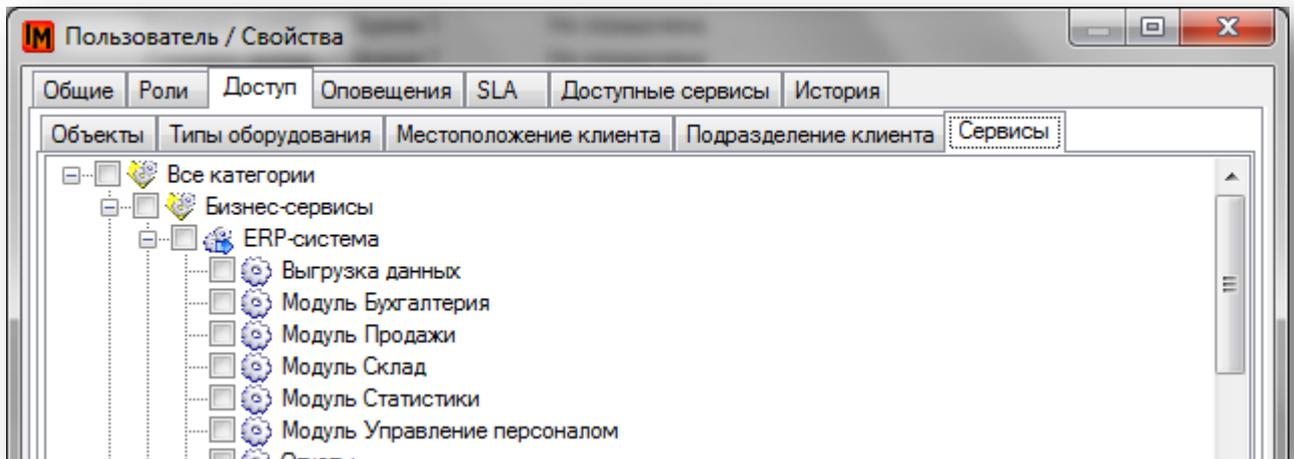
- На закладке «Местоположение клиента» указывается ответственность за заявки, поступающие от пользователей, имеющих рабочие места в определенных зданиях / этажах / комнатах. Распространяется на:
 - просмотр и редактирование заявок, поступивших от сотрудников из определенных зданий / этажей / комнат, с учетом ответственности по подразделению клиента, указываемой на закладке «Подразделение клиента», и по сервисам, указываемой на общей закладке «Доступные сервисы»



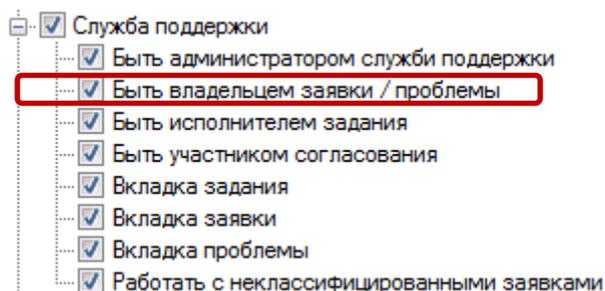
- На закладке «Подразделение клиента» указывается ответственность за заявки, поступающие от пользователей определенных организационных единиц. Распространяется на:
 - просмотр и редактирование заявок, поступивших от сотрудников определенных организаций / подразделений, с учетом ответственности по местоположению клиента и по сервисам, указываемой на общей закладке «Доступные сервисы»
 - возможность выбора в качестве владельцев / исполнителей заявок / заданий / проблем только сотрудников из определенных организационных единиц, имеющих право быть владельцем / исполнителем заявок / заданий / проблем
 - возможность выбора очереди в качестве исполнителя заявок / заданий / проблем только если в очереди участвуют сотрудники из указанных организационных единиц



- **Ответственность за сервисы:**
 - На закладке «Сервисы» указываются те сервисы (категории сервисов), за заявки по которым отвечает данный ИТ-сотрудник

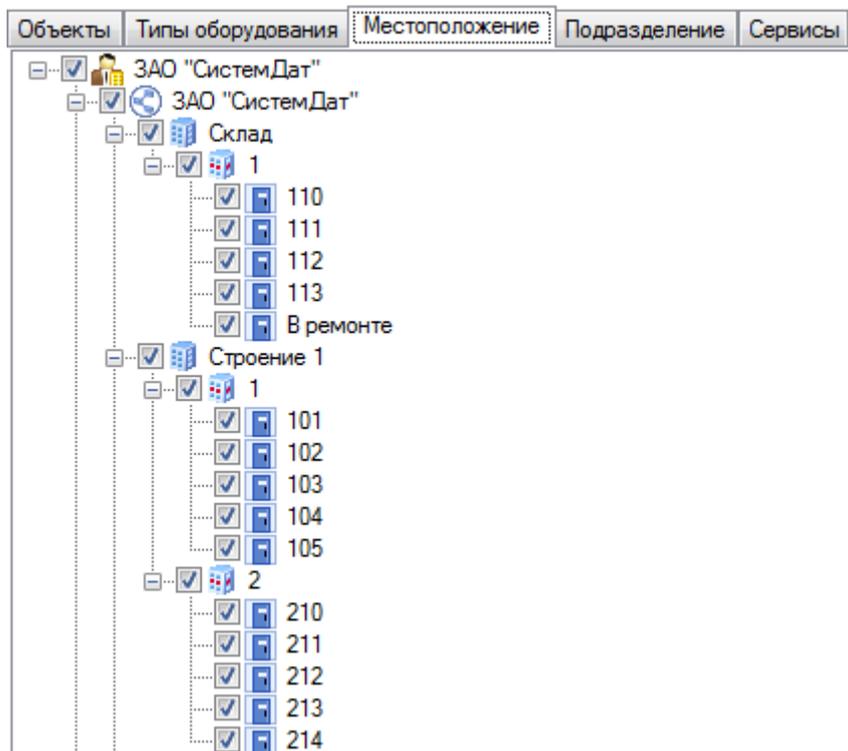


Примечание: данная закладка становится доступна, только если в роли пользователя, в разделе «Служба поддержки», указана операция «Быть владельцем заявки / проблемы»:

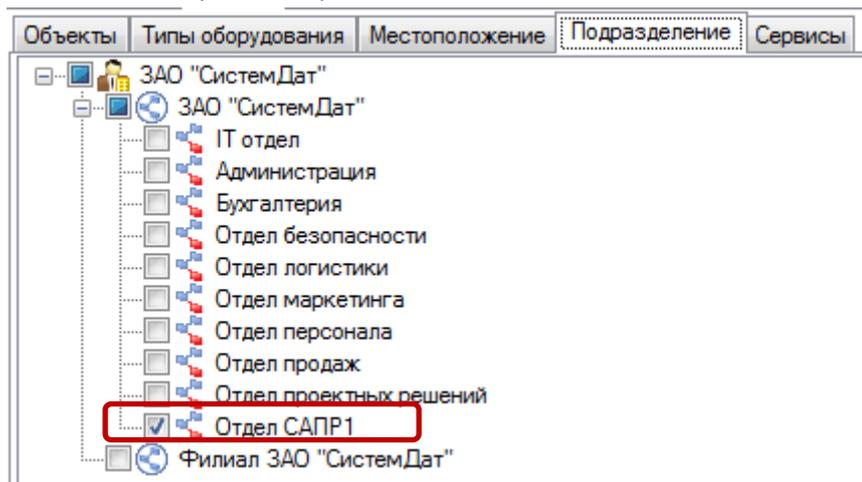


Пример: если пользователи одного подразделения находятся в разных зданиях / комнатах, и нам необходимо в ТОЗ пользователя указать всех, кто входит в данное подразделение, достаточно:

1. Указать все местоположение клиента



2. Указать только нужное подразделение клиента



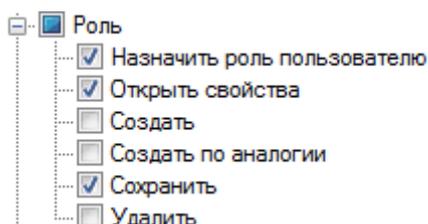
ОПИСАНИЕ НАСТРОЕК ДЛЯ РАЗГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМЕ ИНФРАМЕНЕДЖЕР

ПРАВА НА ОПРЕДЕЛЕНИЕ ПРАВ ДОСТУПА

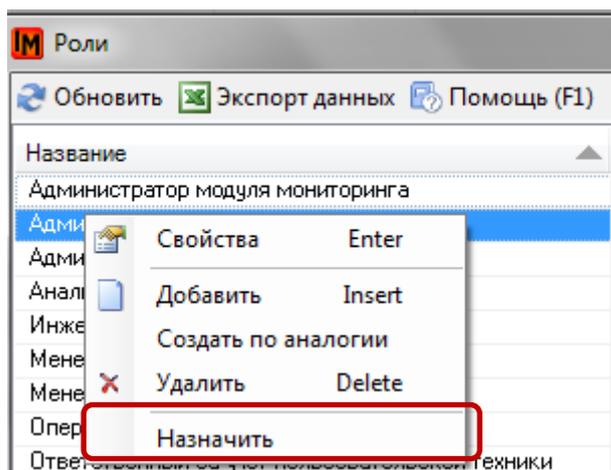
Настройка прав выполняется:

- в редакторе ролей (пункт меню **«Сервис» -> «Редактор ролей»**)
- в свойствах пользователя (пункт меню **«Объекты» -> «Пользователи»**, закладка **«Доступ»**).

Для того чтобы пользователь системы ИнфраМенеджер мог назначать права другим пользователям, не обязательно быть администратором системы. Необходимо и достаточно среди доступных в роли операций иметь следующие:



Данные операции предоставят возможность в пункте меню **«Сервис» -> «Редактор ролей»** назначить список пользователей к каждой роли через пункт контекстного меню **«Назначить»**:



При выборе данного пункта меню система откроет диалог выбора списка пользователей, которые обладают выбранной ролью:

IM Роль / Назначение

Роль:

Пользователи, которым назначена текущая роль

Фамилия	Имя	Отчество	Логин	Табельный ном...	Комната	Здание
Мышин	Вадим	Борисович			104	Строени
Подколичев	Владислав	Иванович			104	Строени

Фильтр: 2 / 2

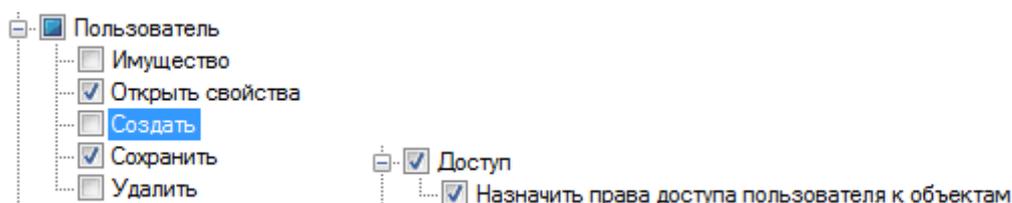
Пользователи без текущей роли

Фамилия	Имя	Отчество	Логин	Табельный ном...	Комната	Здание
Аминов	Админ	Аминович			Нет	Нет
Корнеев	Андрей	Семенович			104	Строени
Соломин	Евгений	Анатолевич			104	Строени
Клочков	Петр				104	Строени

Фильтр: 4 / 62

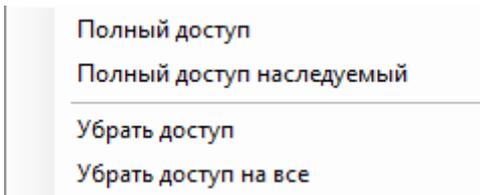
В списке пользователей без текущей роли можно применить фильтр по любому параметру, затем выделить нескольких пользователей и нажать на кнопку «Назначить роль». Аналогично выполняется снятие роли с сотрудников, в верхнем списке данного окна.

Однако если необходимо для каждого пользователя настроить ТОЗ (территориально-организационную зону ответственности) и ТТЗ (территориально-технологическую зону ответственности), необходимо добавить следующие операции:

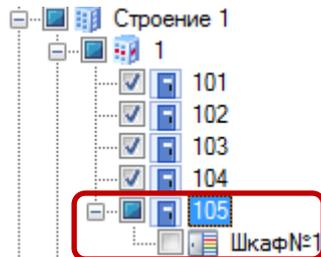


ОПРЕДЕЛЕНИЕ ЗОН ОТВЕТСТВЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ

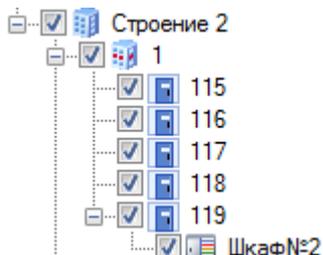
Территориально-технологическая и организационная зоны ответственности указываются на закладке «Доступ» в свойствах пользователя. Для упрощения операции предусмотрены следующие пункты контекстного меню:



1. **«Полный доступ»**: предоставить доступ к выбранному элементу, не включая вложенные элементы списка. **Пример**: предоставить доступ к оборудованию в комнате, но не к оборудованию в шкафу в комнате



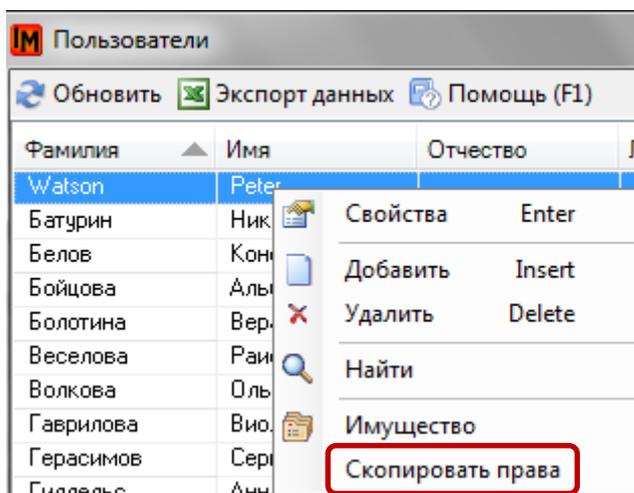
2. **«Полный доступ наследуемый»**: предоставить доступ к выбранному объекту и ко всем вложенным. **Пример**: предоставить доступ к зданию целиком (со всеми этажами и комнатами)



3. **«Убрать доступ»**: убрать доступ к выбранному объекту, не включая вложенные.
4. **«Убрать доступ на все»**: убрать доступ к выбранному объекту, включая все вложенные.

ДУБЛИРОВАНИЕ ЗОНЫ ОТВЕТСТВЕННОСТИ У НЕСКОЛЬКИХ ПОЛЬЗОВАТЕЛЕЙ

Для упрощения назначения одной и той же зоны ответственности нескольким пользователям в системе предусмотрена операция «Скопировать права». Операция доступна из контекстного меню в списке пользователей:



При выборе данного пункта меню система откроет окно назначения прав:

IM Доступ / Назначение

Пользователь: Крючкова Анастасия

Объекты
 Типы оборудования
 Местоположение
 Подразделение
 Сервисы
 Роли

Пользователи с таким же доступом

Фамилия	Имя	Отчество	Логин	Табельный ном...	Комната
Батурин	Николай	Анатольевич			217
Бойцова	Альбина	Романовна			215

Фильтр: Подразделени Like *IT отдел* 2 / 2

Пользователи с другим доступом

Фамилия	Имя	Отчество	Логин	Табельный ном...	Комнат
Маслова	Галина	Алексеевна			210
Маркова	Татьяна	Викторовна			103
Макарова	Елена	Сергеевна			103
Курбашев	Андрей	Анатольевич			213
Климова	Наталья	Алексеевна			117

Фильтр: Подразделение Like *IT отдел* 70 / 70

Копировать зону ответственности можно отдельно по всем параметрам:

- **Объекты:** местоположение оборудования
- **Типы оборудования:** ответственность за определенные типы оборудования
- **Местоположение:** размещение пользователей
- **Подразделения:** принадлежность пользователя к оргединице
- **Сервисы:** ответственность за определенные сервисы

В зависимости от отмеченных прав доступа («Объекты», «Типы оборудования» и т.п.) списки «Пользователи с таким же доступом» и «Пользователи с другим доступом» будут обновляться.

При помощи кнопки «**Назначить доступ**» можно скопировать отмеченные права доступа пользователям, выбранным в нижнем списке.

При помощи кнопки «**Отменить назначение**» все отмеченные права доступа у пользователя, выбранного в верхнем списке, сбрасываются.

РАБОТА В СЛУЖБЕ ПОДДЕРЖКИ

ПРАВА НА ВЕДЕНИЕ СПРАВОЧНИКОВ И РАЗЛИЧНЫХ НАСТРОЕК МОДУЛЯ СЛУЖБА ПОДДЕРЖКИ

Настройка таких прав выполняется в рамках роли сотрудника, через прямое указание доступных операций с объектами модуля Службы поддержки. Объектами модуля Служба поддержки являются:

1. Справочники (пункт меню «**Справочники**»)
 - a. Заявки
 - i. Типы заявок
 - ii. Приоритеты заявок (срочность, влияние, приоритет)
 - iii. Краткое описание заявки
 - iv. Результат запросов на услуги
 - v. Результат завершения инцидента
 - b. Задания
 - i. Типы заданий
 - ii. Приоритеты заданий
 - iii. Шаблоны заданий
 - iv. Регламентные работы
 - v. Статьи бюджета
 - c. Проблемы
 - i. Типы проблем
 - ii. Краткая причина проблемы
2. Основные объекты / настройки (пункт меню «**Сервис**»)
 - a. Портфель сервисов
 - b. Соглашения об уровне качества обслуживания (SLA)
 - c. Настройка графика рабочего времени
 - d. Задания планировщика (для запуска регламентных работ)

ОБЩИЕ ПРАВА НА РАБОТУ С ЗАЯВКАМИ / ЗАДАНИЯМИ / ПРОБЛЕМАМИ

Для возможности работы с заявками / заданиями / проблемами пользователю в рамках роли должны быть доступны следующие операции:

- Заявка**
- Видеть заявки ИТ-сотрудников
 - Видеть заявки сотрудников
 - Изменить обещанное время решения
 - Открыть свойства
 - Создать
 - Создать по аналогии
 - Сохранить
 - Удалить

- Задание**
- Видеть задания ИТ-сотрудников
 - Изменить обещанное время выполнения
 - Открыть свойства
 - Создать
 - Создать по аналогии
 - Создать по шаблону
 - Сохранить
 - Удалить

- Проблема**
- Видеть проблемы ИТ-сотрудников
 - Изменить обещанное время решения
 - Открыть свойства
 - Создать
 - Создать по аналогии
 - Сохранить
 - Удалить

- Служба поддержки**
- Быть администратором службы поддержки
 - Быть владельцем заявки / проблемы
 - Быть исполнителем задания
 - Быть участником согласования
 - Вкладка задания
 - Вкладка заявки
 - Вкладка проблемы
 - Работать с неклассифицированными заявками

Примечание. При определении прав на операции с объектами следует иметь в виду следующие моменты.

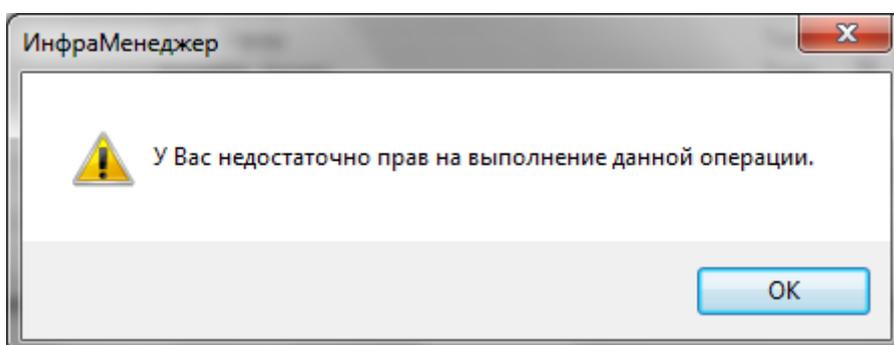
1. Заявка / задания / проблема как объект системы ИнфраМенеджер имеет связи с многими другими объектами (справочниками, сервисами и т.п.). Для того чтобы пользователь мог зарегистрировать заявку, необходимы права на операцию «Открыть свойства» у всех справочников заявок / заданий / проблем
2. Если сотрудник играет роль инженера службы поддержки, потенциально ему может понадобиться:
 - a. Доступ к оборудованию пользователя по заявке. Для этого в роли необходимо указать как минимум – на просмотр карточки оконечного оборудования; как максимум – на внешние утилиты, имущество (ComputerInfo), на добавление новых адаптеров и инсталляций ПО. Последнее понадобится в случае необходимости выполнения опроса оборудования из его карточки и обновления данных об оборудовании по результатам опроса.
 - b. Доступ к схеме зависимостей по сервису заявки
 - c. Доступ (как минимум на просмотр) к информации о сетевом и т.п. оборудовании, участвующем в схемах зависимостей по сервисам заявки.

ПРАВА НА ПРОСМОТР ИНФОРМАЦИИ О ПОСТУПАЮЩИХ В СЛУЖБУ ПОДДЕРЖКИ ЗАЯВКАХ / ЗАДАНИЯХ / ПРОБЛЕМАХ

В модуле «Служба поддержки» присутствует по умолчанию четыре закладки:

- **Мое рабочее место.** Отображаются все объекты (заявки / задания / проблемы), которые:
 - Либо потенциально относятся к зоне ответственности пользователя (но еще не назначен владелец заявок)
 - Либо назначены на данного пользователя
- **Заявки.** Отображаются все заявки, обрабатываемые в рамках системы.
- **Задания.** Отображаются все задания, обрабатываемые в рамках системы.
- **Проблемы.** Отображаются все проблемы, обрабатываемые в рамках системы.

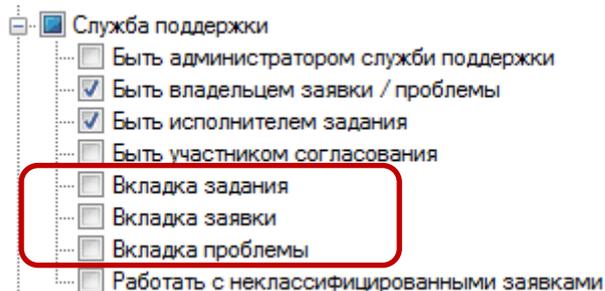
При этом открыть форму заявки / задания / проблемы на общих закладках «Заявки», «Задания», «Проблемы», и отредактировать их поля пользователь имеет возможность только, если данные объекты подпадают под [ТОЗ пользователя](#). В противном случае при попытке открыть форму пользователь получит от системы следующее предупреждение:



Примечание: однако, в нижней части списка, в области предпросмотра, информация по заявке / заданию / проблеме все равно будет доступна пользователю:

Общие	Клиент	Связанные задания [1]	Сообщения	Решение	Файлы [0]	Связи [1]	Согласования [0]	Дополн
Заявка №:	19							
Канал приема:	Телефон							
Тип:	Заявка							
Владелец:	Мышин Вадим Борисович							
Исполнитель:								
Краткое описание:	проблемы с выключением ноутбука							
Сервис:	Стандартные сервисы \ Обслуживание рабочих мест пользователей \ Основной (системный) бл							
Описание:	Ноутбук зависает при выключении							

ИнфраМенеджер позволяет ограничить доступ к общим закладкам «Заявки», «Задания», «Проблемы»:

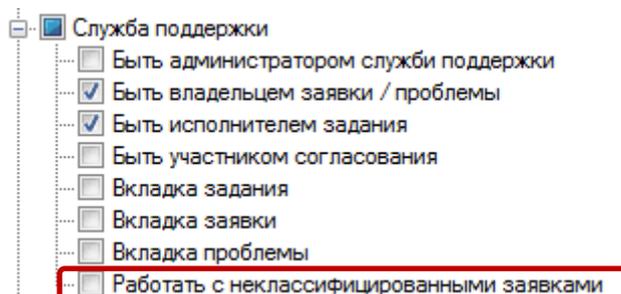


При таких ограничениях пользователь будет работать только со «своими» заявками на закладке «Мое рабочее место».

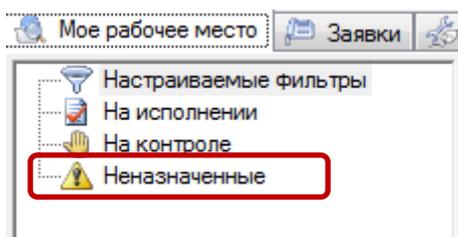
Примечание. При регистрации заявки, после выбора клиента заявки, в полях «Владелец» и «Исполнитель» доступными для выбора остаются только те ИТ-сотрудники, в чью зону ответственности попадает данный клиент.

РАБОТА С НЕКЛАССИФИЦИРОВАННЫМИ ЗАЯВКАМИ

Неклассифицированными заявками в системе «ИнфраМенеджер» являются заявки, приходящие по э-почте. Для запуска таких заявок в работу необходимо назначить ответственного за их регулярный разбор и классификацию. Права для работы с такими заявками назначаются в разделе «Служба поддержки» в рамках роли:

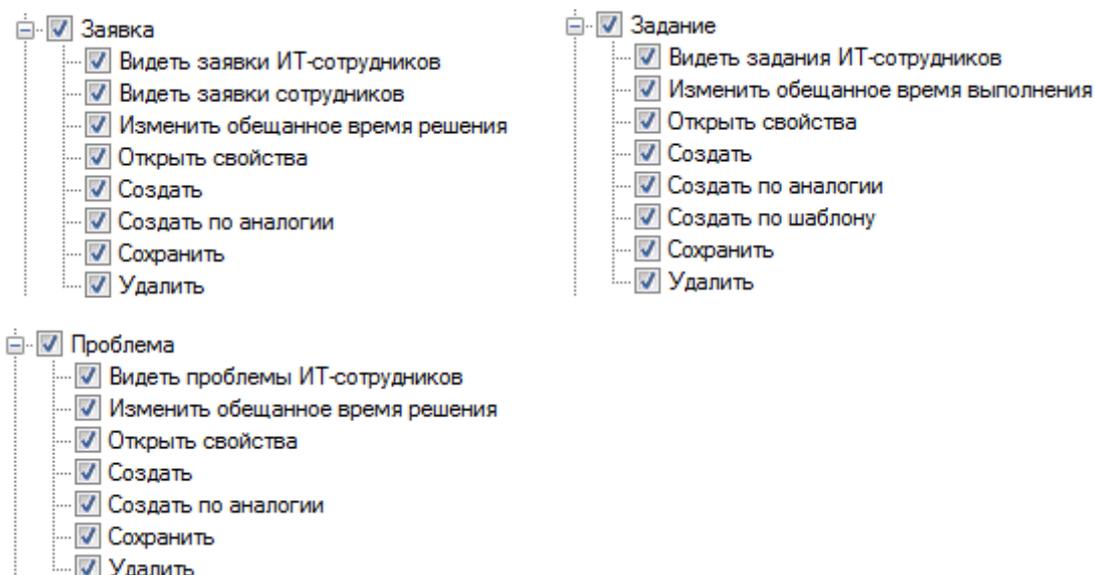


При наличии таких прав на закладке «Мое рабочее место» заявки, пришедшие по э-почте, отображаются в папке «Неназначенные»:



ОСОБЕННОСТИ РАБОТЫ РУКОВОДИТЕЛЕЙ ИТ-ОТДЕЛОВ

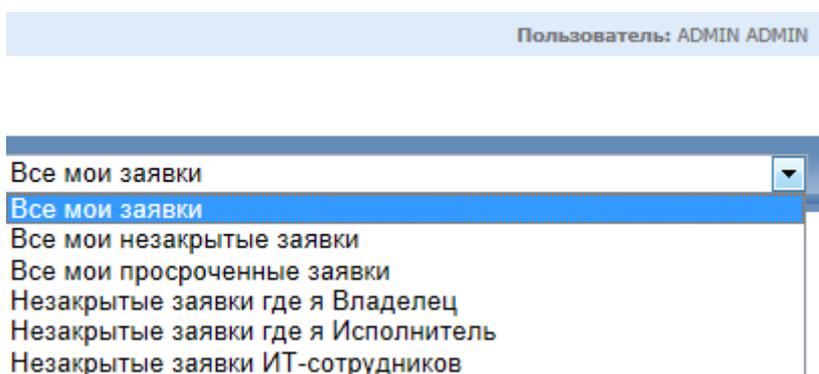
Признаком руководителя ИТ-отдела является разрешение на операции «Видеть заявки ИТ-сотрудников», «Видеть задания ИТ-сотрудников», «Видеть проблемы ИТ-сотрудников».



Данные операции позволяют получить доступ к следующим фильтрам в Web-интерфейсе инженера:

1. Незакрытые заявки ИТ-сотрудников
2. Незавершенные задания ИТ-сотрудников
3. Незакрытые проблемы ИТ-сотрудников

В данных фильтрах система отображает все заявки / задания / проблемы, назначенные на сотрудников подразделения пользователя (своего подразделения и всех дочерних единиц).



Дополнительно, при указании в роли данных операций, система по умолчанию предоставляет пользователю возможность работы с заявками / заданиями / проблемами с учетом объединения всех зон ответственности подчиненных пользователя (т.е. сотрудников его подразделения и всех дочерних организационных единиц, имеющих права работать с заявками / заданиями / проблемами).

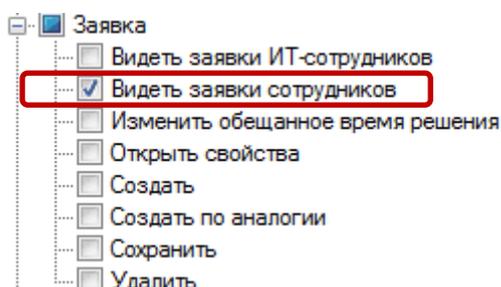
Т.е. руководитель ИТ-отдела будет иметь возможность работать со всеми заявками / заданиями / проблемами, с которыми в соответствии с ТОЗ могут работать его подчиненные (сотрудники его или дочерних подразделений). В свойствах самого руководителя дополнительно отмечать ТОЗ нет необходимости.

РОЛИ ДЛЯ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ

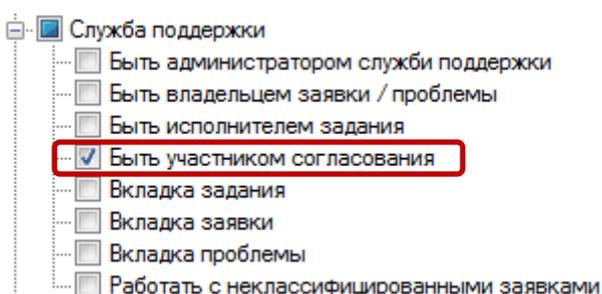
Для обычного пользователя нет необходимости назначать роли. По умолчанию пользователь, у которого не назначено ни одной роли, считается обычным клиентом службы поддержки с единственными возможностями работать с системой через Web-интерфейс клиента.

Однако, возможно, понадобится создать две роли для:

1. **Руководителя подразделения.** Ему система может предоставить возможность видеть список не только своих заявок, но и заявок, созданных его подчиненными (сотрудниками его подразделения и всех дочерних организационных единиц). Для такой роли достаточно выдать одну операцию:



2. **Согласующее лицо.** Некоторые заявки могут требовать согласования с бизнес-пользователями (отделом безопасности, кадры, финансы и т.п.). Пользователей с такой ролью система позволит назначить согласующими лицами по заявкам / заданиям / проблемам. Для такой роли достаточно выдать одну операцию:



ИСПОЛЬЗОВАНИЕ ЗОНЫ ОТВЕТСТВЕННОСТИ ДЛЯ АВТОМАТИЧЕСКОГО НАЗНАЧЕНИЯ ВЛАДЕЛЬЦЕВ / ИСПОЛНИТЕЛЕЙ ЗАЯВОК / ЗАДАНИЙ / ПРОБЛЕМ

И ограничения территориально-технологической зоны ответственности (ТТЗ), и ограничения территориально-организационной зоны ответственности (ТОЗ) могут быть использованы для автоматического выбора ответственных за заявки / задания / проблемы. Для этого в редакторе Workflow необходимо использовать способы автоназначения «Сотрудник с наименьшей нагрузкой по ТТЗ» и «Сотрудник с наименьшей нагрузкой по ТОЗ»:

Автоназначение не используется

Сотрудник с наименьшей нагрузкой
Сотрудник с наименьшей нагрузкой из очереди, ответственной за сервис
Сотрудник с наименьшей нагрузкой по ТОЗ
Сотрудник с наименьшей нагрузкой по ТТЗ
Сотрудник, ответственный за сервис
Фиксированный сотрудник

ИСКЛЮЧЕНИЯ: РАБОТА АДМИНИСТРАТОРА СИСТЕМЫ

По умолчанию в создаваемых ролях присутствует системная роль «Администратор системы». Пользователь, получающий эту роль, имеет права на все, без ограничений. Поэтому у пользователя, обладающего данной ролью, отсутствует закладка «Доступ».

Если пользователю назначена одна роль – «Администратор системы», - система не будет учитывать данного пользователя как возможного владельца / исполнителя любых заявок / заданий / проблем.

Для корректной работы системы в условиях необходимости ограничивать права доступа к объектам системы по территориальной зоне ответственности рекомендуется:

1. Не назначать роль «Администратор системы» операторам / инженерам, участвующим в обработке заявок / заданий / проблем
2. При необходимости включить в работу с заявками / заданиями / проблемами ИТ-сотрудника, совмещающего роль «Администратор системы» с другими обязанностями в рамках процессов, назначать такому сотруднику несколько ролей, например: «Администратор системы» и «Оператор службы поддержки» и т.п.

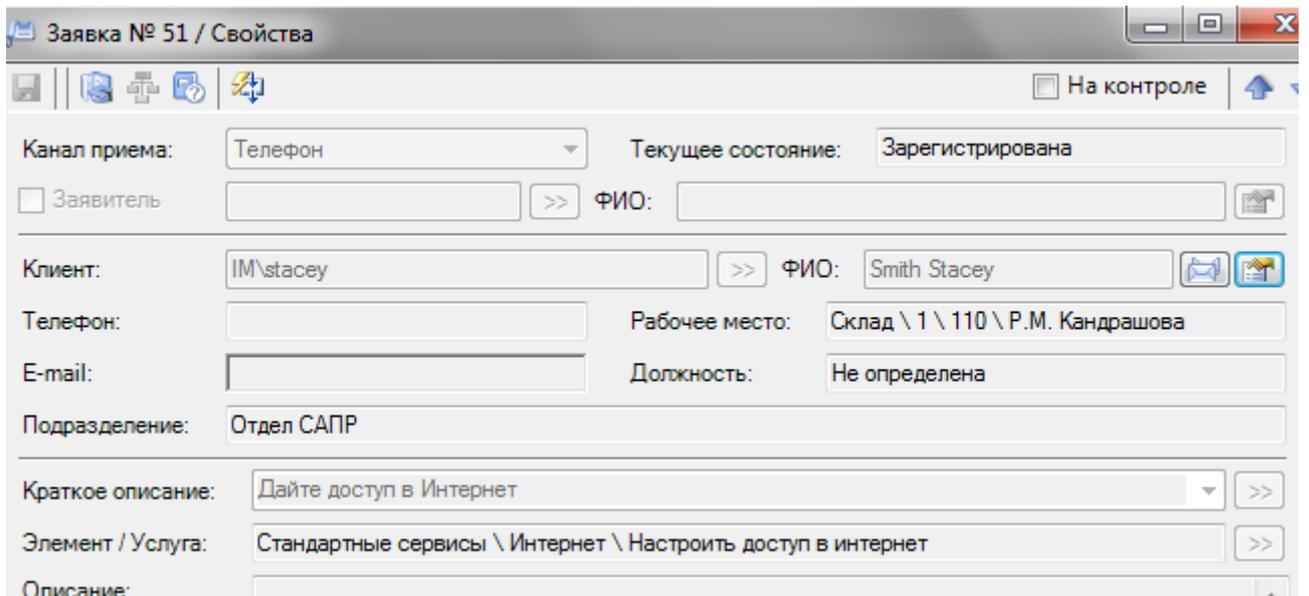
Однако следует иметь в виду: если пользователю назначена и роль «Администратор системы», и еще какая-либо роль, такой пользователь будет иметь возможность быть владельцем / исполнителем любых заявок / заданий / проблем:

- Пользователь будет доступен для выбора вручную из списка возможных владельцев / исполнителей
- При автоматическом выборе владельца / исполнителя по правилу «Сотрудник с наименьшей нагрузкой по ТОЗ» / «Сотрудник с наименьшей нагрузкой по ТТЗ» система включит в список возможных владельцев / исполнителей и такого пользователя (поскольку по умолчанию его ТОЗ и ТТЗ покрывает все возможные значения)

Проще всего использовать отдельную учетную запись для администрирования системы.

ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

ВОПРОС 1. После регистрации заявки, она становится недоступной для редактирования. Форма заявки имеет вид:



Заявка № 51 / Свойства

Канал приема: Телефон Текущее состояние: Зарегистрирована

Заявитель ФИО:

Клиент: IM\stacey ФИО: Smith Stacey

Телефон: Рабочее место: Склад \ 1 \ 110 \ Р.М. Кандрашова

E-mail: Должность: Не определена

Подразделение: Отдел САПР

Краткое описание: Дайте доступ в Интернет

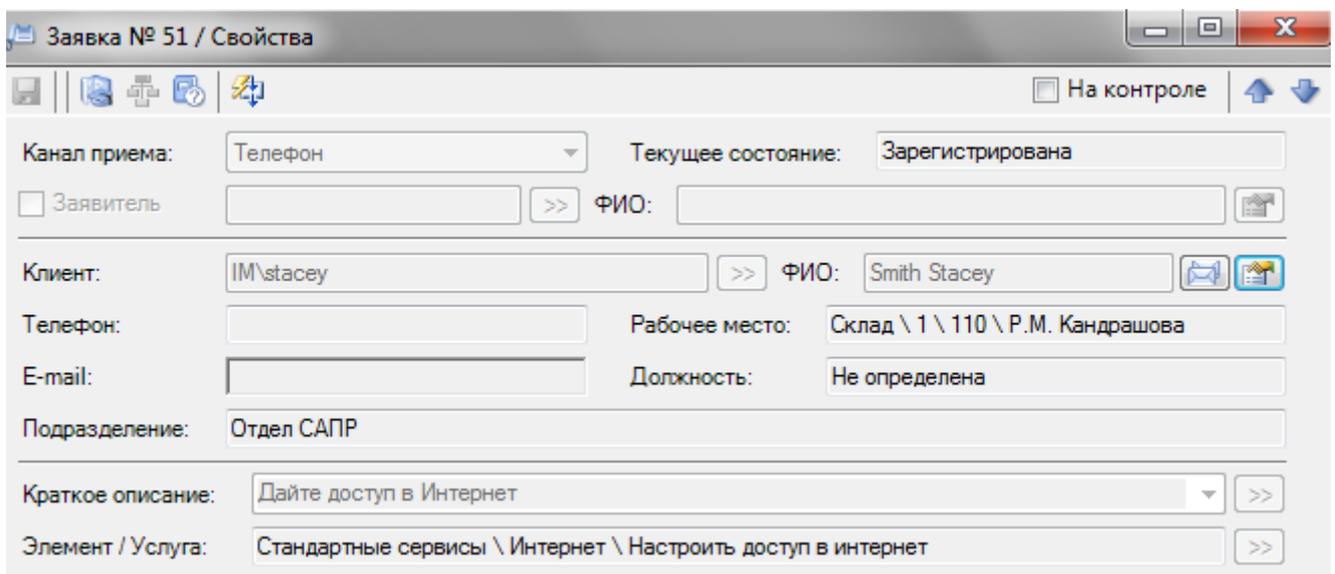
Элемент / Услуга: Стандартные сервисы \ Интернет \ Настроить доступ в интернет

Описание:

В списке данная заявка не отображается. Почему так происходит?

ОТВЕТ: заявка была зарегистрирована от имени пользователя, не находящегося в ТОЗ регистратора заявки. Регистрация заявки проходит, после чего заявка считается недоступной пользователю в соответствии с ТОЗ

ВОПРОС 2. После регистрации заявки, несмотря на то, что заявка назначена на меня, заявка становится недоступной для редактирования. Форма заявки имеет вид:



Заявка № 51 / Свойства

Канал приема: Телефон Текущее состояние: Зарегистрирована

Заявитель ФИО:

Клиент: IM\stacey ФИО: Smith Stacey

Телефон: Рабочее место: Склад \ 1 \ 110 \ Р.М. Кандрашова

E-mail: Должность: Не определена

Подразделение: Отдел САПР

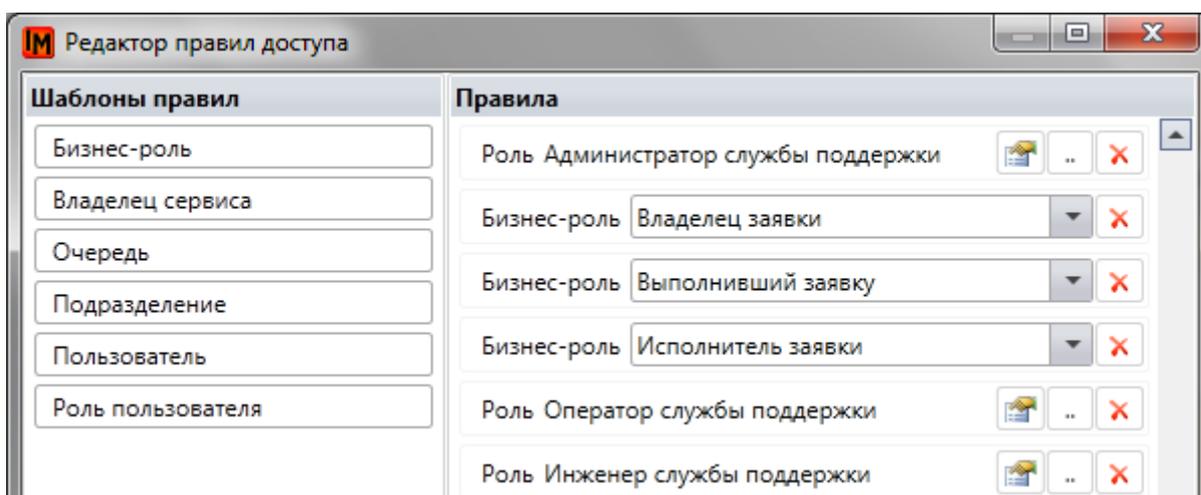
Краткое описание: Дайте доступ в Интернет

Элемент / Услуга: Стандартные сервисы \ Интернет \ Настроить доступ в интернет

Описание:

В списке данная заявка отображается. Почему невозможно редактировать заявку?

ОТВЕТ: в схеме рабочих процедур, применимой к заявкам данного типа / по данной услуге сервиса, не предусмотрен доступ для роли пользователя к заявкам, находящимся в начальном состоянии:



ОПИСАНИЕ СТАНДАРТНЫХ РОЛЕЙ

В любой пустой базе присутствует следующий набор готовых ролей, предназначенных для организации работы в рамках Службы поддержки:

1. Администратор службы поддержки

- a. Имеет доступ ко всем модулям системы ИнфраМенеджер
- b. Имеет возможность создания и редактирования заявок / заданий / проблем
- c. Имеет возможность просмотра и редактирования элементов ИТ-инфраструктуры
- d. Получает уведомления по всем заявкам / заданиям / проблемам (как Администратор)
- e. Имеет доступ на редактирование всех справочников / объектов / настроек модуля Служба поддержки
- f. Имеет доступ к отчетам и редактирование панелей статистики
- g. Имеет доступ к справочникам типов оборудование, на просмотр и редактирование

2. Оператор службы поддержки

- a. Имеет доступ ко всем модулям системы ИнфраМенеджер
- b. Имеет возможность создания и редактирования заявок / заданий
- c. Имеет возможность просмотра элементов ИТ-инфраструктуры

3. Инженер службы поддержки

- a. Имеет доступ ко всем модулям системы ИнфраМенеджер
- b. Имеет возможность создания и редактирования заявок / заданий
- c. Имеет возможность просмотра элементов ИТ-инфраструктуры
- d. Имеет возможность опроса элементов ИТ-инфраструктуры, использования внешних утилит

4. Технический писатель

- a. Имеет право редактирования базы знаний

5. Аналитик

- a. Имеет право создания и редактирования панелей статистики в модуле «Статистика»

Комбинируя данные роли в рамках свойств одного пользователя, вы сможете обеспечить гибкое распределение прав в рамках своей ИТ-службы. В то же время вы можете взять любую роль за основу и создать новую, удалив / добавив нужные права (пункт контекстного меню в списке ролей «Создать по аналогии»)

РАБОТА С БАЗОЙ ДАННЫХ ИТ-КОНФИГУРАЦИЙ

ПРАВА НА ВЕДЕНИЕ СПРАВОЧНИКОВ И РАЗЛИЧНЫХ НАСТРОЕК МОДУЛЯ УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ

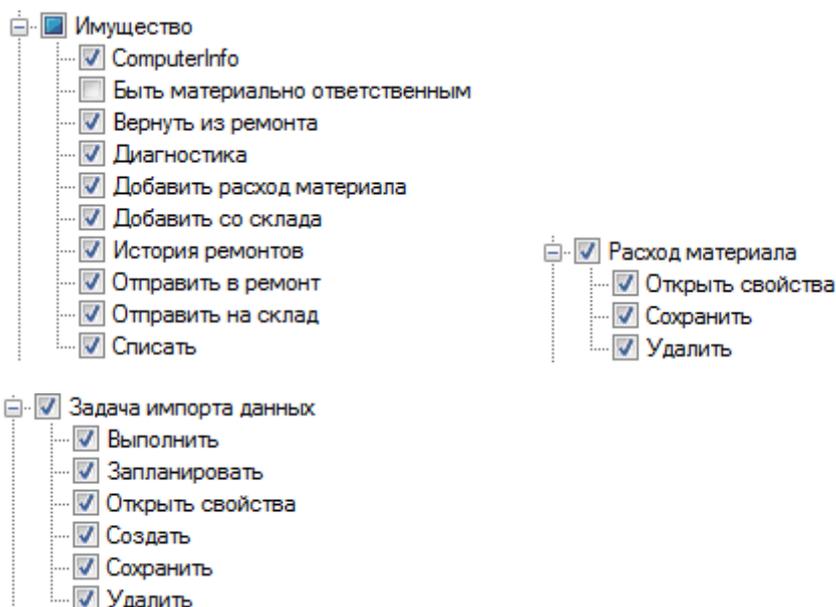
Настройка таких прав выполняется в рамках роли сотрудника, через прямое указание доступных операций с объектами модуля Управление конфигурациями. Такими объектами являются:

1. Каталог оборудования
 - a. Типы оборудования (пункт меню «Справочники»)
 - b. Модели оборудования (пункт меню «Модели»)
2. Разные категории элементов ИТ-инфраструктуры (пункт меню «Объекты»)

Отдельно выделяются права на различные операции с ИТ-имуществом, например:

1. Расход материала
2. Списание
3. Отправка в ремонт
4. И т.п.

Настройка таких прав выполняется в роли, в пунктах, соответствующих названиям объектов системы, а также:



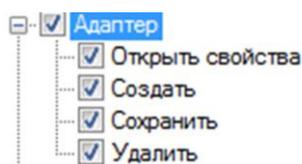
ПРАВА НА РАБОТУ С ОБЪЕКТАМИ

Права на создания объектов любого типа определяются:

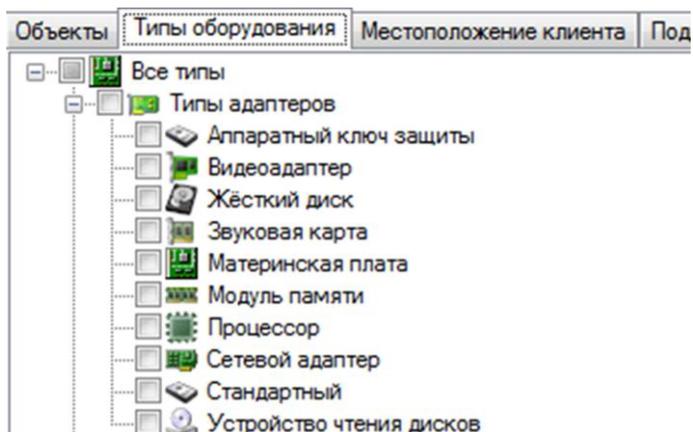
1. Доступными операциями «Создать» в роли, по соответствующим объектам
2. Территориально-технологической зоной ответственности, указанной в свойствах пользователя.

Всегда действуют максимально возможные ограничение по совокупности условий и в операциях с объектами (Роль), и в зоне ответственности пользователя.

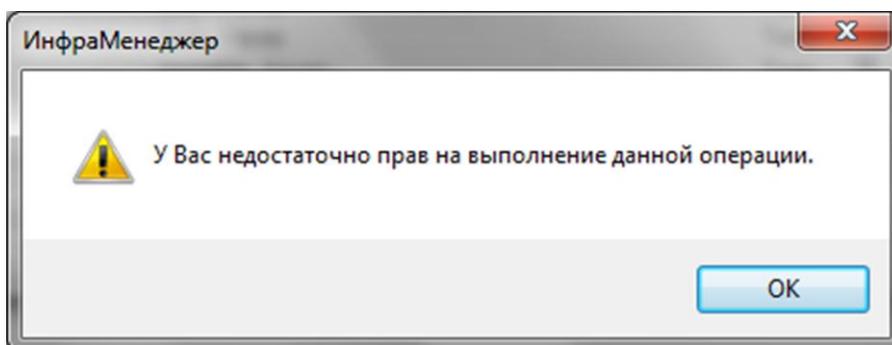
Пример 1. Если роль предоставляет возможность создавать адаптеры:



Однако в территориально-технологической зоне ответственности отсутствует возможность работать с типами «Адаптер»:



Система не позволит добавить новый адаптер в любое оборудование, вне зависимости от его местоположения. При этом пользователю будет выдано оповещение:



Пример 2. Если в роли указаны права на работу с адаптерами, и в территориально-технологической зоне ответственности указана возможность работы с типами адаптеров, однако пользователь попытается добавить адаптер в оборудование, располагающееся вне его территориальной зоны ответственности, результат будет таким же.

ОПИСАНИЕ СТАНДАРТНЫХ РОЛЕЙ

В любой пустой базе присутствует следующий набор готовых ролей, предназначенных для организации работы с базой данных ИТ-конфигураций:

1. Администратор модуля Мониторинг

- a. Имеет доступ ко всем модулям системы ИнфраМенеджер
- b. Имеет доступ на открытие свойств и сохранение оконечного и сетевого оборудования
- c. Имеет доступ ко всем элементам модуля Мониторинг (показатель; перечисление SNMP; сообщение и т.п.)

2. **Ответственный за учет пользовательской техники**
 - a. Имеет доступ ко всем модулям системы ИнфраМенеджер
 - b. Имеет возможность создания и редактирования окончного оборудования, периферийного оборудования, адаптеров
 - c. Имеет доступ к задачам по опросу (Задача импорта данных)
 - d. Имеет доступ к имущественным операциям, расходу материалов;
 - e. Имеет доступ к функции опрос через ComputerInfo;
3. **Сетевой администратор**
 - a. Имеет доступ ко всем модулям системы ИнфраМенеджер
 - b. Имеет возможность создания и редактирования элементов СКС и справочников, необходимых для ведения документации по СКС
4. **Системный администратор**
 - a. Имеет доступ ко всем модулям системы ИнфраМенеджер
 - b. Имеет возможность создания и редактирования сетевого оборудования, логических объектов (приложение, информационный объект), элементов дискового пространства (дисковый массив, том данных)
 - c. Имеет возможность работы со схемой зависимостей
 - d. Предусмотрены права для создания регламентных работ (в рамках модуля Служба поддержки)

Комбинируя данные роли в рамках свойств одного пользователя, вы сможете обеспечить гибкое распределение прав в рамках своей ИТ-службы. В то же время вы можете взять любую роль за основу и создать новую, удалив / добавив нужные права (пункт контекстного меню в списке ролей «**Создать по аналогии**»)