Комплекс распределенной обработки сообщений Юпитер-КРОС

Версия 2.5.7

Руководство по эксплуатации

ред 1.10

Санкт-Петербург
2021

SEC.RU | Короткий путь к информации Скачано с sec.ru

Оглавление

Оглавление....2
Введение....7
Назначение руководства....7
Термины и определения....7
1. Основные сведения о программе....9
1.1 Назначение программы....9
1.2 Основные возможности....9
1.3 Рекомендованные системные требования....11
1.4 Рекомендации по эксплуатацию сервера КРОС....13
1.4 Различные СПИ и оконечные устройства, совместимые с Юпитер-КРОС....15
2. Начало работы....17
2.1 Настройка портов....17
2.2 Установка сервера для ОС Windows....19
2.2.1 Установка Java....19
2.2.2 Установка PostgreSQL 9.6....20
2.2.3 Установка сервера Юпитер-КРОС....20
2.3 Установка сервера для ОС Linux....24
2.3.1 Установка Java....24
2.3.2 Установка PostgreSQL 9.6 (На примере Debian)....25
2.3.3 Установка сервера Юпитер-КРОС....26
2.4 Установка сервера для ОС Astra Linux Special Edition....30
2.4.1 Установка ГосJava (Для поставки ГК2019)....30
2.4.2 Установка Oracle Java (Для поставки ГК2020)....31
2.4.3 Установка PostgreSQL 9.6....32
2.4.3 Установка сервера Юпитер-КРОС....33
2.5 Расположение файлов и каталогов Юпитер-КРОС после установки....34
3. Роли пользователей и авторизация....36
3.1 Роли пользователей....36
3.1.1 Администратор сервера....36
3.2.2 Администратор охранной организации....37
3.2.3 Менеджер....37
3.2.4 Инженер....37
3.2 Авторизация пользователя....38
3.3 Смена роли....38
4. Меню «Главная»....39
4.1 Состояние объектов....39
4.2 Состояние приборов....40
4.3 Используемые порты....41
4.4 Монитор....42
5. Меню «Сервер»....43
5.1 Приемники....43

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.1.1 Базовые параметры для каждого приемника....45
5.1.2 Индивидуальные параметры для приемников UdpPK4Jupiter, TcpPK4Jupiter....46
5.2.2 Индивидуальные параметры для приемника GsmModem....47
5.2.3 Индивидуальные параметры для приемника ArmSK....47
5.2.4 Индивидуальные параметры для приемника ArmUpdater....47
5.2 Передатчики....48
5.2.1 Базовые параметры для каждого приемника....48
5.2.2 Индивидуальные параметры для передатчика ArmSK....49
5.3 Трансляции....50
5.3.1 Добавление трансляции....51
5.3.2 Редактирование трансляции....53
5.3.3 Удаление трансляции....53
5.3.4 Базовые параметры для всех типов трансляций....54
5.3.5 Индивидуальные параметры для передатчика TcpSurgard....54
5.3.6 Индивидуальные параметры для передатчика TcpSurgardv4....55
5.3.7 Индивидуальные параметры для передатчика TcpEPPS....56
5.4 Таблицы....58
5.4.1 Добавление таблицы....61
5.4.2 Редактирование сообщений в таблице....61
5.4.3 Выбор таблицы....64
5.4.4 Удаление таблицы....64
6. Меню «Клиенты»....65
6.1 Договоры....65
6.1.1 Добавление, редактирование и удаление договора охраны....65
6.1.1.1 Добавление договора охраны....65
6.1.1.1.1 Вкладка «Ответственные лица»....66
6.1.1.1.2 Вкладка «Реквизиты»....66
6.1.1.1.3 Вкладка «Объекты»....66
6.1.1.2 Редактирование договора охраны....67
6.1.1.3 Удаление договора охраны....67
6.1.1.4 Группов*ые операции с* договорами охраны....67
6.1.2 Добавление объекта охраны к договору охраны....68
6.1.3 Иерархия....68
6.2 Объекты....69
6.2.1 Добавление, редактирование и удаление объекта охраны....70
6.2.1.1 Добавление объекта....70
6.2.1.2 Редактирование объекта....71
6.2.1.3 Удаление объекта....71
6.2.2 Вкладка «Основная»....71
6.2.2.1 Добавление номера договора....71
6.2.2.2 Выбор типа объекта и метки....72
6.2.2.3 Добавление адреса охраны....72
6.2.2.4 Обслуживание....73
6.2.2.5 Номера телефонов....73

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.2.5 Описание объекта....73
6.2.3 Вкладка «Карта»....74
6.2.4 Вкладка «План»....75
6.2.5 Вкладка «ХО (хозорганы)»....76
6.2.6 Вкладка «Информация»....77
6.2.7 Вкладка «Приборы»....79
6.2.8 Вкладка «Изображения»....80
6.2.9 Вкладка «Расписание»....81
6.2.10 Групповые операции с объектами охраны....84
6.3 Приборы....85
6.3.1 Добавление, редактирование и удаление нового прибора....87
6.3.1.1 Добавление нового прибора....87
6.3.1.2 Редактирование прибора....88
6.3.1.3 Удаление прибора....88
6.3.2 Вкладка «Основные»....88
6.3.3 Вкладка «Каналы связи»....90
6.3.3.1 Общие параметры для всех каналов....92
6.3.3.2 Индивидуальные параметры для канала PK4....93
6.3.3.2 Индивидуальные параметры для канала EPPS....93
6.3.3.3 Индивидуальные параметры для канала CID....93
6.3.3.4 Индивидуальные параметры для канала CSD....94
6.3.4 Вкладка «Номера телефонов»....95
6.3.5 Вкладка «Зоны охраны»....96
6.3.6 Вкладка «Разделы»....97
6.3.7 Вкладка «Расширители»....98
6.3.8 Вкладка «События»....99
6.3.9 Групповые операции с приборами охраны....101
6.3.10 Удаленное обновление прошивки....103
6.4 Подмена прибора....104
6.5 Пошаговая инструкция по подключению прибора к серверу-КРОС....106
6.5.1 Настройка портов....106
6.5.2 Добавление договора....108
6.5.3 Добавление объекта....110
6.5.4 Добавление прибора....111
6.6 Ответственные лица....115
7. Меню «Охрана»....117
7.1 Реквизиты....117
7.1.1 Параметры охранной организации....119
7.1.1.1 Параметры соединения....120
7.1.1.2 Активность GSM-модема....121
7.1.1.3 Каналы IP-модема....121
7.1.1.4 Инженерный режим....121
7.1.1.5 Режим работы....122
7.1.1.6 Обработка тревог....124

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.1.7 Режим работы АРМ....125
7.1.1.8 Контроль резервного питания....125
7.1.1.9 Параметры учета состояния договора....126
7.1.2 SMPP сервер....127
7.1.3 Редактирование реквизитов....130
7.1.4 Удаление реквизитов....130
7.2 Учетные записи....131
7.2.1 Добавление учетной записи....132
7.2.2 Редактирование учетной записи....137
7.2.3 Удаление учетной записи....137
7.2.4 Фильтр объектов....138
7.3 Группы задержания....141
7.3.1 Добавление ГЗ....141
7.3.2 Редактирование ГЗ....143
7.3.3 Удаление ГЗ....143
8. Меню «Администрирование»....144
8.1 Система....144
8.1.1 Вкладка «Сервер»....144
8.1.2 Вкладка «SMTP сервер»....147
8.1.3 Вкладка «HTTP сервер»....149
8.1.4 Вкладка «Протоколирование»....151
8.1.5 Вкладка «Часы сервера»....153
8.1.6 Вкладка «Блок DDOS»....154
8.1.7 Вкладка «Репозиторий»....155
8.2 Данные....156
8.2.1 Вкладка «SQL сервер»....156
8.2.2 Вкладка «Резервирование»....158
8.2.2.1 Создание резервной копии....158
8.2.2.2 Восстановление из резервной копии....162
8.2.3 Вкладка «Очистка БД»....164
8.3 Безопасность....166
8.3.1 Вкладка «Роли»....167
8.3.1.1 Добавление новой роли....168
8.3.1.2 Редактирование роли....168
8.3.1.3 Удаление роли....168
8.3.1.4 Описание прав доступа....169
8.3.2 Вкладка «Администратор сервера»....172
8.3.3 Вкладка «Сертификаты»....173
8.4 Заявки....174
8.5 Протокол....176
8.6 Сообщения....177
8.7 Справочники....178
8.7.1 Справочник «Типы объектов»....178
8.7.2 Справочник «Доклад ГЗ»....179

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.7.3 Справочник «Причины тревоги»....180
9. Зеркалирование («Горячий» резерв)....181
9.1 Общая информация....181
9.2 Настройка системы....182
9.3 Создание трансляции....183
9.4 Разрешение приема данных....184
10. Импорт базы данных....185
10.1 Перенос базы данных Юпитер-7 в Юпитер-КРОС....185
10.1.1 Создание файла конфигурации Юпитер-7....185
10.1.2 Импорт файла конфигурации в Юпитер-КРОС....186
10.2 Соответствие карточек Юпитер-7 при переносе в Юпитер-КРОС....187
10.3 Настройка трансляции из Юпитер-7 в Юпитер-КРОС....188
10.4 Настройка работы с мобильным приложением «Личный кабинет» при трансляции из Юпитер-7 в Юпитер-КРОС....189
11. Настройка часов УМКА для работы на сервере «Юпитер-КРОС»....191
11.1 Первоначальная настройка часов....191
11.2 Настройка отслеживания часов в приложении АРМ ДПУ....194
12 Конструктор отчетов....198
12.1 Общий вид конструктора отчетов....199
12.2 Создание отчета по базовому шаблону....200
12.3 Создание шаблона отчета в конструкторе отчетов....202
12.4 Построение оперативной карточки объекта....204
Приложения....206
Приложение №1 Перевод IP-GPRS оборудования Юпитер-7 на Юпитер-КРОС (выгрузка полной конфигурации)....206
1. Концепция....206
2. Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС....207
3. Экспорт конфигурации из Юпитер-7 в Юпитер-КРОС....208
4. Настройка параметров на сервере Юпитер-КРОС....212
5. Замена серверов....212
6. Настройка рабочих мест....213
7. Приборы, подлежащие переносу....213
Приложение №2 Перевод IP-GPRS оборудования Юпитер-7 на Юпитер-КРОС (поэтапный перенос)....214
1. Концепция:....214
2. Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС....215
3. Автоматизированный механизм переноса объектов....216
4. Приборы, подлежащие переносу....224

SEC.RU | Короткий путь к информации Скачано с sec.ru

Введение

Назначение руководства

Настоящее руководство содержит сведения об особенностях инсталляции и эксплуатации программного обеспечения Комплекс Распределенной Обработки Сообщений (в дальнейшем Юпитер-КРОС)

Руководство предназначено для ознакомления пользователей с назначением, возможностями, а также порядком и правилами работы с Юпитер-КРОС , в нем содержатся сведения о выполняемых Юпитер-КРОС функциях, а также описание режимов работы.

Руководство рассчитано на пользователей, имеющих опыт работы с персональным компьютером и операционными системами Windows / Linux. Остальным пользователям в ходе установки, настройки и запуска программного обеспечения рекомендуется, кроме данного документа, руководствоваться документацией на операционную систему, используемый тип персонального компьютера и программно-аппаратные средства локальной вычислительной сети.

Термины и определения

В настоящем руководстве применены перечисленные ниже термины с соответствующими определениями.

АРМ — автоматизированное рабочее место.

АРМ ДПУ — автоматизированное рабочее место дежурного пульта управления.

АРМ ДО — автоматизированное рабочее место дежурного офицера.

АРМ СК — ситуационная карта

ДО — дежурный офицер.

ДПУ — дежурный пульта управления.

Задержка на вход — время после нарушения контролируемого ШС с задержкой, за которое пользователь должен ввести код на снятие с охраны. Используется, если прибор расположен внутри помещения. Задается отдельно для каждого ШС с задержкой.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Задержка на выход — время задержки между вводом кода пользователя на постановку и моментом постановки на охрану. Используется для постановки на охрану раздела прибора, находящегося внутри помещения. Задается сразу для всех разделов прибора.

Имитостойкость — свойство, характеризующее способность системы сигнализировать о несанкционированной подмене устройств.

Карточка объекта — карточка, в которой хранятся полные сведения об объекте.

КТС — кнопка тревожной сигнализации.

Оборудование — комплекс всех технических средств СПИ «Юпитер».

ОПС — охранно-пожарная сигнализация.

Устройство — единица оборудования охранно-пожарной сигнализации, входящая в СПИ «Юпитер».

БД — база данных.

Прибор — см. устройство.

Программа Конфигуратора — программа, предназначенная для конфигурирования (задания настроек) устройства по интерфейсу USB.

ПЦН — пульт централизованного наблюдения.

ПЦО — пункт централизованной охраны.

Раздел — группа подключенных к устройству шлейфов сигнализации, ставящихся/снимающихся с охраны одновременно. Дает возможность охранять несколько объектов, со своими пользователями, используя один многошлейфовый прибор

СПИ — система передачи извещений.

СУБД — система управления базами данных.

Х/О — хоз.орган (ответственное лицо клиента на объекте охраны).

ШС — шлейф охранно-пожарной сигнализации.

ТК — тревожная кнопка.

ЛК — личный кабинет.

ГЗ — группа задержания.

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Основные сведения о программе

1.1 Назначение программы

Юпитер-КРОС-это система организации распределенной пультовой охраны. Юпитер-КРОС является серверной частью системы передачи извещений «Юпитер» (далее СПИ «Юпитер») и представляет собой программный комплекс , предназначенный для приема и обработки извещений.

Юпитер-КРОС предназначен для организации связи сервера с оборудованием СПИ «Юпитер» а также с дополнительным ПО, входящим в состав Юпитер-КРОС, таким как мобильные приложения (тревожная кнопка (далее ТК), личный кабинет пользователя(далее ЛК), группы задержания (далее ГЗ)), устройства Юпитер-УМКА, четырехканальным GSM-модемом, и последующей передачи полученных извещений на Автоматизированное Рабочее Место оператора (далее АРМ).

1.2 Основные возможности

1. Совокупность программных средств, работающих под управлением единого программного ядра, позволяет формировать различные подсистемы, которые могут работать как автономно, так и в сочетании с другими подсистемами, образуя единую распределенную масштабируемую высокопроизводительную систему обеспечения безопасности.

2. Обеспечивает надежную защиту от несанкционированного доступа путем шифрования всего трафика.

3. Позволяет реализовать взаимодействие различных программных средств, независимо от физической среды передачи данных, по протоколам:

- TCP
- UDP
- HTTP(S)

4. Способность работать на любой платформе, поддерживающую установку java и PostgreSQL.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Возможность удаленного подключения из любой точки мира к:

- Системе администрирования сервера
- АРМ
- ДПУ
- ДО
- Инженера
- ЛК

6. Общее количество АРМ в системе не ограничено.

7. Мобильные приложения

- Юпитер-ЛК
- Юпитер-ТК
- Юпитер-ГЗ

8. Открытый протокол ЕППС (Единый Протокол Передачи Сообщений)

SEC.RU | Короткий путь к информации Скачано с sec.ru

9.Работа с системами сторонних производителей по протоколам:

- TCP SurGard
- TCP SurGard V4
- F1 Com (IMEI)

10. Формирование и выдача различных отчетов на основании оперативных и архивных данных.

11. API для сторонних разработчиков расширений и драйверов.

1.3 Рекомендованные системные требования

Аппаратные требования:

Кол-во приборов	до 5 000	5 000 - 10 000	10 000 и более
Процессор	4 ядра	4-8 ядер	8-... ядер
RAM	16 Гб	16-32 Гб	32-...Гб
Диск - SSD\HDD	250 ГБ \ 1 ТБ	250 ГБ \ 1 ТБ	250 ГБ \ 1 ТБ
ОС	Linux x64 / Windows 7 или 10 x64	Linux x64	Linux x64
Пропускная способность сети	Не ниже 20 Мбит\сек	Не ниже 50 Мбит\сек	Не ниже 50 Мбит\сек

Внимание:

- Требуется разрешение на передачу Cookie через сеть, в которой установлен сервер (не будет возможности авторизоваться)
- На браузерах Microsoft Internet Explorer и Edge возможны ошибки в отображении web-содержимого страниц
- Для работы серверов в системе зеркалирования из за большой нагрузки на базу данных обязательное требование - диски SSD.
- Для корректной работы АРМ Сервер-КРОС необходимо добавить АРМ в исключения фаервола, а также возможно понадобится корректно настроить или полностью удалить антивирус.

В таблице указаны ориентировочные расчетные значения для выбора аппаратной конфигурации. Реальные значения зависят от множества параметров: стабильность сетевых подключений,

SEC.RU | Короткий путь к информации Скачано с sec.ru

работа всего комплекса в единой локальной сети или размещение всех АРМ-клиентов за её пределами, режимы работы приборов, действия пользователей при работе с web-сервисом КРОС, особенности работы аппаратного обеспечения и прочее.

Для БД рекомендуется устанавливать SSD диски, т.к. операции чтения/записи происходят дольше всех и являются одним из самых узких мест в системе.

Рекомендуемые Linux-дистрибутивы: Debian, Ubuntu, Astra Linux.

Windows: x64 - 7 и выше. Корпорация Майкрософт прекращает поддержку Windows 7 - 14.01.2020 Рекомендуем использовать новые версии с последними обновлениями безопасности.

Рекомендуемые браузеры:

- Google Chrome от 83 версии и новее
- Safari от 9.1.3 версии и новее
- Opera от 74 версии и новее
- Firefox от 72 версии и новее

SEC.RU | Короткий путь к информации Скачано с sec.ru

1.4 Рекомендации по эксплуатацию сервера КРОС

1. Выполнить диагностику и настройку локальной сети на предмет стабильности соединения между компьютерами:
   a) Расписать общую топологию сети (количество роутеров, зависимости между ними, пароли доступа к роутерам)
   b) Обновить роутеры до последних версий прошивок
   c) Настроить доступность портов согласно инструкции по Настройке портов из справочного руководства.
2. Проводить проверки жёсткого диска на предмет наличия ошибок чтения/записи, мониторинг “здоровья” жёсткого диска, следить за наличием битых секторов с помощью специализированных программ CrystalDiskInfo и Victoria HDD/SSD. Проверять жёсткие диски раз в месяц с занесением в журнал проверок.
3. Своевременно делать резервные копии не только сервера КРОС, но и всей операционной системы в целом:
   a) Резервные копии сервера КРОС, ключей лицензии и конфигурационных файлов делать раз в сутки
   b) Резервные копии операционной системы делать раз в неделю
   c) Хранить резервные копии сервера КРОС на диске куда не установлена операционная система, чтобы в случае сбоя операционной системы не потерять все данные вместе с системой.
4. Проверить компьютер с сервером КРОС на соответствие системным требованиям:
   a) Процессор - 8 ядер
   b) Оперативная память - 16 Гб
   c) Жёсткий диск SSD 250Гб (операционная система, база данных PostgreSQL, КРОС)
   d) Жёсткий диск HDD 1000Гб (логи сервера КРОС и бэкапы)
   e) Пропускная способность от 20 Мбит

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Оборудовать компьютер с сервером КРОС источником бесперебойного питания (при аварийных остановках операционной системы страдает в первую очередь жёсткий диск и база данных)
6. Вести логирование действий с сервером для упрощения оказания технической поддержки в случае инцидентов:
   a) Обновления операционной системы
   b) Обновления сервера КРОС
   c) Замена комплектующих компьютера
   d) Логирование действий приведших к аварии
7. Продумать систему резервного/подменного сервера на случай полного выхода из строя основного оборудования:
   a) Запасной компьютер / запасные комплектующие для возможности быстрой замены вышедших из строя
   b) Использовать систему зеркалирования данных, являющуюся частью сервера КРОС.
8. 8. Обеспечить сохранность логинов и паролей для доступа на сервер КРОС и в операционную систему. На ПЦО всегда должен присутствовать сотрудник, знающий пароли от операционной системы, сервера КРОС и роутеров. Хранить пароли в секретных конвертах в сейфе с возможностью доступа. Это необходимо для оказания оперативной помощи сотрудниками технической поддержки сервера КРОС

SEC.RU | Короткий путь к информации Скачано с sec.ru

1.4 Различные СПИ и оконечные устройства, совместимые с Юпитер-КРОС

Сервер Юпитер-КРОС работает со следующими системами передачи извещений и оконечными устройствами:

- GSM/IP-устройства — устройства, связанные с пультом по GSM- или IP-сетям. Система поддерживает следующие устройства:
  - УОО «Юпитер IP/GPRS»
    - Юпитер-2413 (GSM)
    - Юпитер-2443 (Ethernet+GSM)
    - Юпитер 2444 (с ЖК)
    - Юпитер 2445 (подкл.расш.)
    - Юпитер 2463 (с WI-FI)
  - УОО «Юпитер 242х»
    - УОО «Юпитер 2420»
    - УОО «Юпитер 2421»
    - УОО «Юпитер 2422»
    - УОО «Юпитер 2424»
    - УОО «Юпитер 2425»
    - УОО «Юпитер 2426»
    - УОО «Юпитер 2427»
    - УОО «Юпитер 2428»
    - УОО «Юпитер 2429»
  - УОО «Юпитер-232х»
    - УОО «Юпитер 2320»

SEC.RU | Короткий путь к информации Скачано с sec.ru

    - УОО «Юпитер 2321»
    - УОО «Юпитер 2326»
  - ППКОП «Юпитер IP/GPRS»
    - Юпитер-1431, 4 ШС, без клавиатуры
    - Юпитер-1433, 4 ШС, с клавиатурой
    - Юпитер 1831, 8 ШС, без клавиатуры
    - Юпитер 1833, 8 ШС, с клавиатурой
    - Юпитер 1931, 16 ШС, без клавиатуры
    - Юпитер 1933, 16 ШС, с клавиатурой
  - ППКОП "ЮПИТЕР-4GSM"
  - Серия приборов Юпитер-202*
  - Серия приборов Юпитер-208*
  - Юпитер — 6422, Юпитер — 6423

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Начало работы

2.1 Настройка портов

Сервер принимает данные по протоколам TCP и UDP, ожидая соединения на портах, задаваемых в настройках. Поэтому прежде чем открывать порты в системе рекомендуется определиться с настройками внешних соединений.

Для подключения различных типов и моделей приборов в сервере используются драйверы - приемники, имеющие индивидуальные настройки.

Порты как драйверов так и HTTP/HTTPS серверов могут быть изменены в настройках системы. Также ненужные драйверы могут быть отключены.

В текущей версии сервера работают следующие драйверы:

Наименование драйвера	Функции	Протокол	Разрешенный диапазон	Порты по умолчанию при установке сервера	Требуется открыть, если используется
ArmSK	Драйвер поддержки АРМ СК/ДПУ/ДО	TCP/ SSL	2002-2004 / 3002-3004	2002-2004	2002 вход, Lan проброс, если сервер и АРМ в одной сети
Сервер лицензирования	Обновление сервера	TCP/ SSL	2120-2122/ 3120-3122	2120-2122	2120/3120 выход
ArmGZ	Драйвер поддержки ГЗ	TCP	5001-5003	5001-5003	вход
UmkaWatch	Получение данных с часов Умка	TCP	6001	6001	вход
GsmModem	Драйвер GSM Модема	TCP	7101, 7102	7101, 7102	7101 вход, Lan проброс, если сервер и модем в одной сети
ArmUpdater	Драйвер обновления АРМ	TCP	7009	7009	7009 вход/выход, Lan если сервер

SEC.RU | Короткий путь к информации Скачано с sec.ru

					и АРМ в одной сети-после доработки обновления с локального сервера
HTTP/ HTTPS	HTTP Сервер	TCP / SSL	9900 / 9800	9900	9900 вход
AlarmButton	Драйвер приложения Тревожная Кнопка	HTTP / HTTPS	9900 / 9800	9900	9900 вход
CustomerAccount	Драйвер приложения Личный Кабинет	HTTP / HTTPS	9900 / 9800	9900	9900 вход
UdpPK4Jupiter	Драйвер ПК4 и ПК5 UDP	UDP	10000-19999	10093-10095	вход
TcpPK4Jupiter	Драйвер ПК4 и ПК5 TCP	TCP	10000-19999	10093-10095	вход
UdpRoot	Драйвер для обновления сервера	UDP	10000-19999	10093-10095	вход. Открывается тот порт, на котором работают приборы по UDP. Если нет возможности работать по TCP.
TcpSurgard	Прием потока данных	TCP	20000-24999	20000	вход
TcpSurgardDecID	Прием потока данных с десятичным ID	TCP	25000-29999	25000	вход
TcpEPPS	Прием потока данных из Юпитер-7 и резервирование	TCP	30000-34999	30000	вход – если идет поток данных из Юпитер-7 вход / выход – если резервирование
Push CustomerAccount	Push-уведомления Личный кабинет	TCP	443	443	выход
Карта в объекте		TCP	443	443	выход
Геокодер		TCP	80	80	выход

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.2 Установка сервера для ОС Windows

2.2.1 Установка Java

Скачать и установить Oracle Java 8 с параметрами по умолчанию:

https://jupiter8.ru/java/jre-8u201-windows-x64.exe

После установки на Windows перезагрузить компьютер.

Проверить версию java, выполнив в командной строке команду:

java -version

Должна быть установлена Java(TM) SE Runtime Environment версии 8 (1.8.0_201, где 8 - версия, 201 - номер обновления, значения которого могут изменяться в зависимости от версии обновления)(рисунок 2.1).

```
C:\WINDOWS\system32>java -version
java version "1.8.0_201"
Java(TM) SE Runtime Environment (build 1.8.0_201-b09)
Java HotSpot(TM) 64-Bit Server VM (build 25.201-b09, mixed mode)
```

Рисунок 2.1 Версия Java для ОС Windows

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.2.2 Установка PostgreSQL 9.6

Скачать с официального сайта и устанавить PostgreSQL 9.6 под нужную ОС.
Скачать:

https://www.enterprisedb.com/downloads/postgres-postgresql-downloads

В процессе установки PostgreSQL выполнить следующие действия:

- Для пользователя postgres установить пароль postgres
- В конце установки снять выделение с параметра Stack Builder

2.2.3 Установка сервера Юпитер-КРОС

Архив сервера предоставляется по запросу. Требуется написать официальное письмо на elesta@elesta.ru

Для установки сервера Юпитер-КРОС:

1. Распаковать архив с сервером КРОС в C:\
2. Поместить в папку smpo-server файл лицензии с расширением .key, если такой имеется
3. Выполнить в командной строке:
   cd c:\Server_KROS
4. Выполнить команду в командной строке:
   java -jar smpo-server.jar -ports

Будет произведена диагностика системы и выведен результат на экран. Пример вывода представлен в таблице ниже.

```
KROS Server initialization...
Compiled 2018-05-17 14:21:45 +0300 (Thu, 17 May 2018)
Copyright (c) 2015-2018, Elesta Co. LTD., St.Petersburg, Russia
Инициализация системы лицензирования... OK
        Внешний адрес: 5.17.161.235
        Сервер лицензирования: jupiter8.ru:2120
Check database condition...
Database OK
        UUID Сервера: 729c5425-5105-31f7-adbf-74e824c87cef
KROS Server, version 2.3.38.7119

РЕЖИМ ДИАГНОСТИКИ СИСТЕМЫ

[2018-05-17 16:02:08.891] Инициализация системы...
Starting HTTP server on port 9900
Loading Object Conditions...8
Loading Object Types...13
Loading Object Categories...13
Loading Group Conditions...8
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
Loading Equipment types...2
Loading Phone types...6
Loading Device Types...153
Loading Alarm Reports...2
Loading Roles...18, 4
Loading Customers...1
Loading Watchers...2
Loading Devices...4557
Loading Responsibles...0
Loading Objects...4558
Loading Contracts...2
Refresh Objects...4558
Refresh Contracts...2
Loading Personals...0
Loading Groups...3
Loading Users...9
Recalculating objects status...4558
Starting UDP listener at port 10000
Starting UDP listener at port 10093
Starting UDP listener at port 10094
Starting UDP listener at port 10095
Starting TCP listener at port 5001
Starting TCP listener at port 5002
Starting TCP listener at port 5003
Starting TCP listener at port 6003
Starting TCP listener at port 30000
Starting TCP listener at port 30001
Starting TCP listener at port 10000
Starting TCP listener at port 10093
Starting TCP listener at port 10094
Starting TCP listener at port 10095
Starting TCP listener at port 20000
Starting TCP listener at port 20001
Starting TCP listener at port 20002
Starting TCP listener at port 6004
Starting TCP listener at port 6002
Starting TCP listener at port 6001
Starting TCP listener at port 7009
Starting TCP listener at port 7101
Starting TCP listener at port 7102
Starting TCP listener at port 2002
Starting TCP listener at port 2003
Starting TCP listener at port 2004
Starting TCP listener at port 25000
Starting TCP listener at port 25001

[2018-05-17 16:03:56.064] Тестирование доступности портов... Готово
[2018-05-17 16:04:08.001] Работоспособные порты:

[2018-05-17 16:04:08.002] Протокол TCP
[2018-05-17 16:04:08.002] Порт 10095, пинг: 23 мс
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
[2018-05-17 16:04:08.002] Протокол HTTP
[2018-05-17 16:04:08.002] Порт 9900, пинг: 80 мс

[2018-05-17 16:04:08.002] Протокол UDP
[2018-05-17 16:04:08.002] Порт 10095, пинг: 14 мс

[2018-05-17 16:04:08.002] В Вашей системе существуют проблемы с доступом к
портам

[2018-05-17 16:04:08.002] Протокол TCP
[2018-05-17 16:04:08.002] Порт 20000, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 20001, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 7009, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 20002, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 25000, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 5001, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 25001, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 5002, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 5003, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 10093, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10094, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10000, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 30000, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 30001, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6001, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6002, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 2002, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 2003, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6003, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 2004, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6004, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 7101, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 7102, причина: Порт недоступен

[2018-05-17 16:04:08.003] Протокол UDP
[2018-05-17 16:04:08.003] Порт 10000, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10093, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10094, причина: Порт недоступен

[2018-05-17 16:04:08.003] Результат: Имеются проблемы
```

- В разделе работоспособные порты - перечисляются порты доступные для внешнего соединения.
- Порт недоступен - это означает, что он закрыт для внешнего соединения.
- Порты 2002-2004 используются в АРМ. Если планируется использование АРМ только в локальной сети, то пробрасывать эти порты не требуется.
- Настроить проброс для нужных портов.
- Повторить проверку и в случае успешного результата перейти к следующему этапу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Установить сервис вручную следующей командой под Администратором (обладает наивысшими правами):
C:\Server_KROS\bin\server-control install

6. Запустить сервис вручную следующей командой под Администратором (обладает наивысшими правами):
C:\Server_KROS\bin\server-control start

Для входа в систему администрирования нужно в любом браузере (рекомендуется Google Chrome) открыть WEB-страницу по адресу сервера (можно локальному, если он находится в Вашей локальной сети) указав порт 9900.

Например:
http://localhost:9900
или
http://192.168.1.13:9900
192.168.1.13 - IP компьютера, на котором установлен сервер.

Появится приглашение ввести логин и пароль пользователя (рисунок 2.2):

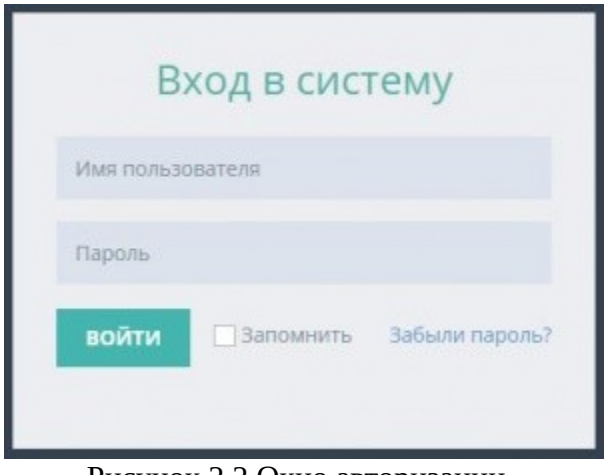


Рисунок 2.2 Окно авторизации

Используйте установленные по умолчанию
Логин : superadmin
Пароль: superadmin

Если удалось выполнить все пункты, можно сделать вывод, что сервер установлен корректно.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.3 Установка сервера для ОС Linux

2.3.1 Установка Java

Скачать с официального сайта и установить последнюю версию Oracle Java 8
Для этого требуется:

1. Авторизоваться в терминале под пользователем root:

   su root (ввести пароль)

2. Удалить Open Java:

   apt-get purge openjdk-* icedtea-* icedtea6-*

3. Удалить папку с оставшимися файлами java:

   rm -rf /usr/lib/jvm

4. Перейти в папку:

   cd /usr/local

5. Скачать с переименованием:
   x64

   https://jupiter8.ru/java/jre-8u201-linux-x64.tar.gz -O jre-linux.tar.gz

   x32

   https://jupiter8.ru/java/jre-8u201-linux-i586.tar.gz -O jre-linux.tar.gz

6. Распаковать полученный tar.gz-архив:

   tar xvfz jre-linux.tar.gz

7. Создать папку для Java:

   mkdir /usr/lib/jvm

8. Переместить туда ранее распакованный архив Java с переименованием:

   mv jre1.* /usr/lib/jvm/jre

9. Удалить скачанный архив java

   rm -f jre-linux.tar.gz

SEC.RU | Короткий путь к информации Скачано с sec.ru

10. Удалить все альтернативы java
    update-alternatives --remove-all java

11. Прописать команду java:

    update-alternatives --install /usr/bin/java java /usr/lib/jvm/jre/bin/java 1

12. Проверить версию java, выполнив команду

    java -version

```
root@debian:/usr/local# java -version
java version "1.8.0_201"
Java(TM) SE Runtime Environment (build 1.8.0_201-b09)
Java HotSpot(TM) Server VM (build 25.201-b09, mixed mode)
root@debian:/usr/local#
```

Рисунок 2.3 Проверка версии Java на ОС Linux

Должна быть установлена Java(TM) SE Runtime Environment версии 8 (1.8.0_201, где 8 - версия, 201 - номер обновления, значения которого могут изменяться в зависимости от версии обновления) (Рисунок 2.3).

2.3.2 Установка PostgreSQL 9.6 (На примере Debian)

Если вы работаете не на Debian, то команды могут отличаться

Выполнить команды в терминале последовательно под root:

1. Для установки PostgreSql:
   apt-get --assume-yes install postgresql-9.6
2. Для пользователя postgres установить пароль postgres следующей командой:
   sudo -u postgres psql -c "ALTER USER postgres with encrypted password 'postgres';"
3. Перезапустить PostgreSql:
   service postgresql restart

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.3.3 Установка сервера Юпитер-КРОС

Архив сервера предоставляется по запросу. Требуется написать официальное письмо на elesta@elesta.ru

Для установки сервера Юпитер-КРОС требуется:

1. Открыть терминал
2. Выполнить команду в терминале:
   cd /usr/
3. Скачать архив с сервером КРОС:
   wget url
   url - ссылка для скачивания
4. Распаковать архив с сервером КРОС:
   sudo unzip /usr/smpo-server.zip
5. Перейти в папку smpo-server:
   cd /usr/smpo-server
6. Сделать исполняемыми файлы с расширением *.sh:
   sudo chmod +x *.sh
7. Запустить установку:
   sudo /usr/smpo-server/install.sh
8. Перейти в:
   cd /usr/local/smpo-server
9. Поместить в папку /usr/local/smpo-server файл лицензии, если имеется, с расширением .key (без ключа лицензии работает в тестовом режиме один месяц)
10. Выполнить команду:
    java -jar smpo-server.jar -ports

Будет произведена диагностика системы и выведен результат на экран. Пример вывода представлен в таблице ниже.

```
KROS Server initialization...
Compiled 2018-05-17 14:21:45 +0300 (Thu, 17 May 2018)
Copyright (c) 2015-2018, Elesta Co. LTD., St.Petersburg, Russia
Инициализация системы лицензирования... OK
        Внешний адрес: 5.17.161.235
        Сервер лицензирования: jupiter8.ru:2120
Check database condition...
Database OK
        UUID Сервера: 729c5425-5105-31f7-adbf-74e824c87cef
KROS Server, version 2.3.38.7119

РЕЖИМ ДИАГНОСТИКИ СИСТЕМЫ

[2018-05-17 16:02:08.891] Инициализация системы...
Starting HTTP server on port 9900
Loading Object Conditions...8
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
Loading Object Types...13
Loading Object Categories...13
Loading Group Conditions...8
Loading Equipment types...2
Loading Phone types...6
Loading Device Types...153
Loading Alarm Reports...2
Loading Roles...18, 4
Loading Customers...1
Loading Watchers...2
Loading Devices...4557
Loading Responsibles...0
Loading Objects...4558
Loading Contracts...2
Refresh Objects...4558
Refresh Contracts...2
Loading Personals...0
Loading Groups...3
Loading Users...9
Recalculating objects status...4558
Starting UDP listener at port 10000
Starting UDP listener at port 10093
Starting UDP listener at port 10094
Starting UDP listener at port 10095
Starting TCP listener at port 5001
Starting TCP listener at port 5002
Starting TCP listener at port 5003
Starting TCP listener at port 6003
Starting TCP listener at port 30000
Starting TCP listener at port 30001
Starting TCP listener at port 10000
Starting TCP listener at port 10093
Starting TCP listener at port 10094
Starting TCP listener at port 10095
Starting TCP listener at port 20000
Starting TCP listener at port 20001
Starting TCP listener at port 20002
Starting TCP listener at port 6004
Starting TCP listener at port 6002
Starting TCP listener at port 6001
Starting TCP listener at port 7009
Starting TCP listener at port 7101
Starting TCP listener at port 7102
Starting TCP listener at port 2002
Starting TCP listener at port 2003
Starting TCP listener at port 2004
Starting TCP listener at port 25000
Starting TCP listener at port 25001

[2018-05-17 16:03:56.064] Тестирование доступности портов... Готово
[2018-05-17 16:04:08.001] Работоспособные порты:
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
[2018-05-17 16:04:08.002] Протокол TCP
[2018-05-17 16:04:08.002] Порт 10095, пинг: 23 мс

[2018-05-17 16:04:08.002] Протокол HTTP
[2018-05-17 16:04:08.002] Порт 9900, пинг: 80 мс

[2018-05-17 16:04:08.002] Протокол UDP
[2018-05-17 16:04:08.002] Порт 10095, пинг: 14 мс

[2018-05-17 16:04:08.002] В Вашей системе существуют проблемы с доступом к
портам

[2018-05-17 16:04:08.002] Протокол TCP
[2018-05-17 16:04:08.002] Порт 20000, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 20001, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 7009, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 20002, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 25000, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 5001, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 25001, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 5002, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 5003, причина: Порт недоступен
[2018-05-17 16:04:08.002] Порт 10093, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10094, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10000, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 30000, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 30001, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6001, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6002, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 2002, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 2003, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6003, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 2004, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 6004, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 7101, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 7102, причина: Порт недоступен

[2018-05-17 16:04:08.003] Протокол UDP
[2018-05-17 16:04:08.003] Порт 10000, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10093, причина: Порт недоступен
[2018-05-17 16:04:08.003] Порт 10094, причина: Порт недоступен

[2018-05-17 16:04:08.003] Результат: Имеются проблемы
```

- В разделе работоспособные порты - перечисляются порты доступные для внешнего соединения.
- Порт недоступен - это означает, что он закрыт для внешнего соединения.
- Порты 2002-2004 используются в АРМ. Если планируется использование АРМ только в локальной сети, то пробрасывать эти порты не требуется.
- Настроить проброс для нужных портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Повторить проверку и в случае успешного результата перейти к следующему этапу.

11. Запустить сервер командой в терминале:

```
sudo /etc/init.d/smpo-server start
```

Для входа в систему администрирования нужно в любом браузере (рекомендуем Google Chrome) открыть WEB-страницу по адресу сервера (можно локальному, если он находится в Вашей локальной сети) указав порт 9900

Например:
http://localhost:9900
или
http://192.168.1.13:9900
192.168.1.13 - IP компьютера, на котором установлен сервер.

Появится приглашение ввести логин и пароль пользователя (рисунок 2.4):

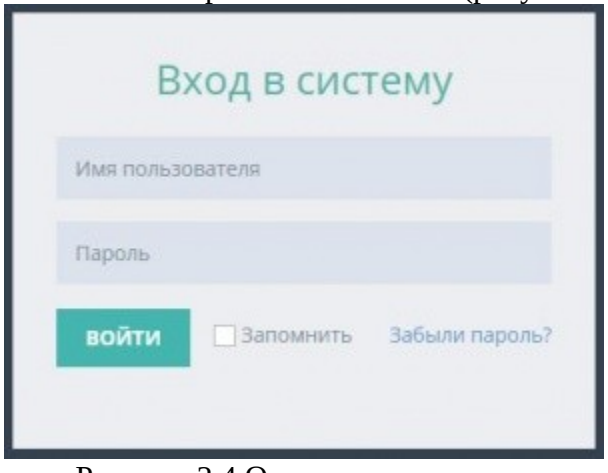


Рисунок 2.4 Окно входа в систему

Используйте установленные по умолчанию

Логин : superadmin
Пароль: superadmin

Если удалось выполнить все пункты, можно сделать вывод, что сервер Юпитер-КРОС установлен корректно.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.4 Установка сервера для ОС Astra Linux Special Edition

2.4.1 Установка ГосJava (Для поставки ГК2019)

Запустить терминал Fly. Для этого нажать на звездочку в левом нижнем углу экрана, выбрать меню Системные, затем Терминал Fly.

1. Требуется подключить репозиторий smolensk из iso образа. Тут возможны два варианта:
    1. Если iso образ ОС Astra Linux Смоленск находится в разделе Recovery на вашем жестком диске, то:
        1. В терминале выполнить команду:

sudo mount -o loop /mnt/hdd/Recovery/AstraSmolenskAmd64.iso /media/cdrom

    2. Если на вашем жестком диске отсутствует раздел Recovery, то:
        1. Необходимо загрузить на флэш-карту образ диска Astra Linux Смоленск в формате .iso и подключить флэш-карту к компьютеру.
        2. Выполнить в терминале команду:

sudo mount /dev/sdc1 /mnt

        3. Далее выполнить команду:

sudo mount -o loop /mnt/AstraSmolenskAmd64.iso /media/cdrom

При успешном выполнении команды в терминале должно появиться следующее сообщение:

```
mount: /dev/loop0 is write-protected, mounting read-only
```

3. Добавить необходимые репозитории. Для этого выполнить команду:

sudo nano /etc/apt/sources.list

4. Добавить следующие строки в sources.list:

deb file:///usr/local/GosJava-2019.4-se16-com/ gosjava main contrib non-free

Сохранить Ctrl + O

Нажать Enter

Выйти Ctrl + X

5. Выполнить команду:

sudo apt-cdrom -m add

6. Выполнить команду:

sudo apt update

8. Перейти в папку командой:

cd /usr/local/

9. Скачать архив ГосJava, выполнив команду:

sudo wget https://jupiter8.ru/java/GosJava-2019.4-se16-com.tar.gz

10. Извлечь из архива файлы командой:

sudo tar -xvf ./GosJava-2019.4-se16-com.tar.gz

11. Подписать дистрибутив ГосJava, выполнив команду:

wget -qO - http://packages.lab50.net/lab50.asc | sudo apt-key add -

12. Выполнить команду:

sudo apt update

13. Установить ГосJava, выполнив команду:

sudo apt install gosjava-8-jre -y

SEC.RU | Короткий путь к информации Скачано с sec.ru

14.Проверить версию java выполнив команду:
java -version
Команда должна выдать сведения о том, что установлена версия 1.8.0_222

2.4.2 Установка Oracle Java (Для поставки ГК2020)

1 Запустить терминал Fly. Для этого нажать на звездочку в левом нижнем углу экрана, выбрать меню Системные, затем Терминал Fly.

2 Требуется подключить репозиторий smolensk из iso образа. Тут возможны два варианта:

2.a Если iso образ ОС Astra Linux Смоленск находится в разделе Recovery на вашем жестком диске, то:

a.i В терминале выполнить команду:
sudo mount -o loop /mnt/hdd/Recovery/AstraSmolenskAmd64.iso /media/cdrom

2.b Если на вашем жестком диске отсутствует раздел Recovery, то:

b.i Необходимо загрузить на флэш-карту образ диска Astra Linux Смоленск в формате .iso и подключить флэш-карту к компьютеру.

b.ii Выполнить в терминале команду:
sudo mount /dev/sdc1 /mnt

b.iii Далее выполнить команду:
sudo mount -o loop /mnt/AstraSmolenskAmd64.iso /media/cdrom

При успешном выполнении команды в терминале должно появиться следующее сообщение:

```
mount: /dev/loop0 is write-protected, mounting read-only
```

3 Выполнить команду:
sudo apt-cdrom -m add

4 Выполнить команду:
sudo apt update

5 Дождавшись обновления, перейти в папку командой:
cd /usr/local/

6 Скачать архив Oracle Java, выполнив команду:
sudo wget https://jupiter8.ru/java/jre-8u201-linux-x64.tar.gz -O jre-linux.tar.gz

7 Извлечь из архива файлы командой:
sudo tar xvfz jre-linux.tar.gz

8 Создать папку для Java:
sudo mkdir /usr/lib/jvm

9 Переместить туда ранее распакованный архив Java с переименованием:
sudo mv jre1.* /usr/lib/jvm/jre

10 Удалить скачанный архив java.

SEC.RU | Короткий путь к информации Скачано с sec.ru

sudo rm -f jre-linux.tar.gz

11 Удалить все альтернативы java
sudo update-alternatives --remove-all java

12 Прописать команду java:
sudo update-alternatives --install /usr/bin/java java /usr/lib/jvm/jre/bin/java 1

13 Проверить версию java выполнив команду:
java -version

Команда должна выдать сведения о том, что установлена версия 1.8.0_201

2.4.3 Установка PostgreSQL 9.6

Для установки PostgreSQL в операционной системе Astra Linux Special Edition необходимо при установке операционной системы в пункте «Выбор программного обеспечения» установить галочку «СУБД». В этом случае после запуска операционной системы база данных будет установлена, и будет требоваться только настроить ее для работы с сервером Юпитер-КРОС.

После запуска операционной системы необходимо провести первоначальную настройку базы данных.
Для этого выполнить команды в терминале:

1. Для пользователя postgres установить пароль postgres следующей командой:
   sudo -u postgres psql -c "ALTER USER postgres with encrypted password 'postgres';"
2. Создать базу данных “jupiter”
   sudo -u postgres psql -c "CREATE DATABASE jupiter;"
3. Перезапустить PostgreSQL:
   sudo service postgresql restart

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.4.3 Установка сервера Юпитер-КРОС

1. Перейти в:
   cd /usr/
2. Скачать архив с КРОС выполнив команду в терминале:
   sudo wget url
   url – ссылка для скачивания
3. Распаковать архив с сервером КРОС:
   sudo unzip /usr/smpo-server.zip
4. Перейти в папку smpo-server:
   cd /usr/smpo-server
5. Сделать исполняемыми файлы с расширением *.sh:
   sudo chmod +x *.sh
6. Запустить установку:
   sudo /usr/smpo-server/install.sh
7. Поместить в папку /usr/local/smpo-server файл лицензии, если имеется, с расширением .key (без ключа лицензии работает в тестовом режиме один месяц).
8. Запустить сервер:
   sudo /etc/init.d/smpo-server start

Для входа в систему администрирования нужно в любом браузере (рекомендуем Google Chrome) открыть WEB-страницу по адресу сервера (можно локальному, если он находится в Вашей локальной сети) указав порт 9900.

Например:
http://localhost:9900
или
http://192.168.1.13:9900
192.168.1.13 - IP компьютера, на котором установлен сервер.

Появится приглашение ввести логин и пароль пользователя (рисунок 2.5):

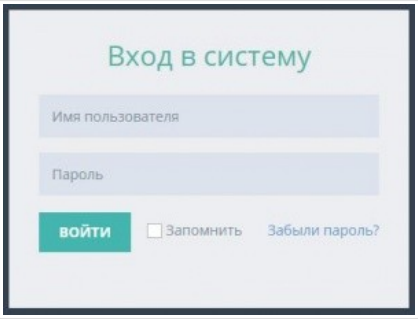


Рисунок 2.5 Окно авторизации

Используйте установленные по умолчанию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Логин : superadmin
Пароль: superadmin

Если удалось выполнить все пункты, можно сделать вывод, что сервер установлен корректно.

2.5 Расположение файлов и каталогов Юпитер-КРОС после установки

По умолчанию, рекомендуется устанавливать сервер Юпитер-КРОС в каталог:

1. ОС Windows
   C:\Server_KROS
2. ОС Linux
   /usr/local/smpo-server/

В дальнейшем описании предполагается, что каталог установки не был изменен.
В состав установленного сервера Юпитер-КРОС входят следующие каталоги:

Хранимые данные	Каталог в Windows	Каталог в Linux
Файлы резервных копий	C:\Server_KROS\smpo-server\backup	/usr/local/smpo-server/backup
Файлы для управления сервером как демоном или сервисом	C:\Server_KROS\smpo-server\bin	/usr/local/smpo-server/bin
Файлы основных настроек сервера	C:\Server_KROS\smpo-server\conf	/usr/local/smpo-server/conf
Временный каталог при создании резервной копии	C:\Server_KROS\smpo-server\db_backup	/usr/local/smpo-server/db_backup
Изображения объектов	C:\Server_KROS\smpo-server\images	/usr/local/smpo-server/images
Служебные библиотеки	C:\Server_KROS\smpo-server\lib	/usr/local/smpo-server/lib
Логи	C:\Server_KROS\smpo-server\logs	/usr/local/smpo-server/logs
Планы объектов	C:\Server_KROS\smpo-server\plans	/usr/local/smpo-server/plans
Шаблоны web-страниц	C:\Server_KROS\smpo-server\templates	/usr/local/smpo-server/templates

SEC.RU | Короткий путь к информации Скачано с sec.ru

В состав установленного сервера Юпитер-КРОС входят следующие файлы:

Файл	Описание
Файлы с расширением .key	Файлы ключей лицензии
Install.sh ; uninstal.sh ; smpo-server.sh	Файлы для управления сервером в ОС Linux
Readme.txt	Файл с описанием установки Юпитер-КРОС
Version.txt	Файл с номером текущей установленной версии сервера
Whatsnew.txt	Файл с описанием последних изменений при обновлении

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Роли пользователей и авторизация

3.1 Роли пользователей

В системе существует базовый список предустановленных ролей с возможностью их редактирования. Доступно введение новых ролей с гибкой настройкой и совмещением нескольких ролей в одной учетной записи. Роли — это шаблоны наборов прав доступа, использующиеся охранным предприятием.

В системе Юпитер-КРОС существует четыре предустановленных роли пользователей:

Название роли	Логин	Пароль
Администратор сервера	superadmin	superadmin
Администратор охранной организации	admin	admin
Менеджер	data	data
Инженер	tech	tech

В таблице приведены логины и пароли по-умолчанию, которые могут быть изменены

3.1.1 Администратор сервера

Функции:

- Настройка приемников;
- Настройка передатчиков;
- Добавление таблиц перекодировки сообщений\извещений;
- Выбор таблицы перекодировки сообщений\извещений;
- Создание охранной организации в рамках сервера;
- Настройка прав доступа учетных записей;
- Обновление версии сервера;
- Настройка базы данных;
- Распределение прав доступа.
- Резервное копирование сервера

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.2.2 Администратор охранной организации

Функции:

- Добавление трансляций передачи сообщений;
- Добавление таблиц перекодировки сообщений\извещений;
- Добавление договоров охраны;
- Добавление объектов охраны;
- Подключение приборов;
- Редактирование реквизитов охранной организации;
- Добавление учетных записей;
- Добавление ГЗ.

3.2.3 Менеджер

Функции:

- Добавление договоров охраны;
- Добавление объектов охраны.

3.2.4 Инженер

Функции:

- Добавление трансляций передачи сообщений;
- Добавление таблиц перекодировки сообщений\извещений;
- Добавление объектов охраны;
- Подключение приборов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.2 Авторизация пользователя

Для авторизации пользователя на сервере необходимо:
1. Открыть браузер.
2. Ввести в адресной строке:

http://localhost:9900

либо

http:// IP-адрес сервера:9900

в том случае если сервер запущен на удаленном компьютере.
3. В открывшемся окне «Вход в систему» ввести имя пользователя и пароль, которые соответствуют роли пользователя (рисунок 3.1).

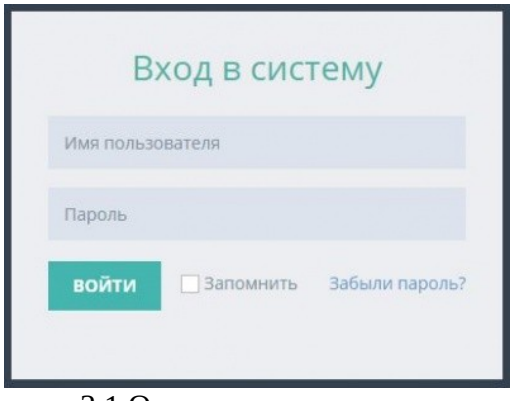


Рисунок 3.1 Окно авторизации пользователя

4. Нажать «Войти».

3.3 Смена роли

1. Нажать по названию пользователя в правом верхнем углу экрана.
2. В появившемся выпадающем меню выбрать пункт «Выйти» (рисунок 3.2).

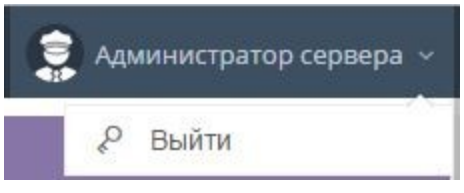


Рисунок 3.2 Окно выхода из учетной записи

3. В открывшемся окне «Вход в систему» ввести имя пользователя и соответствующий пароль.
4. Нажать «Войти».

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Меню «Главная»

4.1 Состояние объектов

Данное меню служит для мониторинга текущего состояния объектов охраны, и дает общую сводку по охраняемым объектам (рисунок 4.1).

1. Время работы сервера КРОС без перезагрузки отображается в верхнем правом углу (цифра 1 на изображении внизу).
2. Состояние объектов и их состояния (цифра 2 на изображении внизу).
3. Статистика событий по объектам за 24 часа (цифра 3 на изображении внизу).

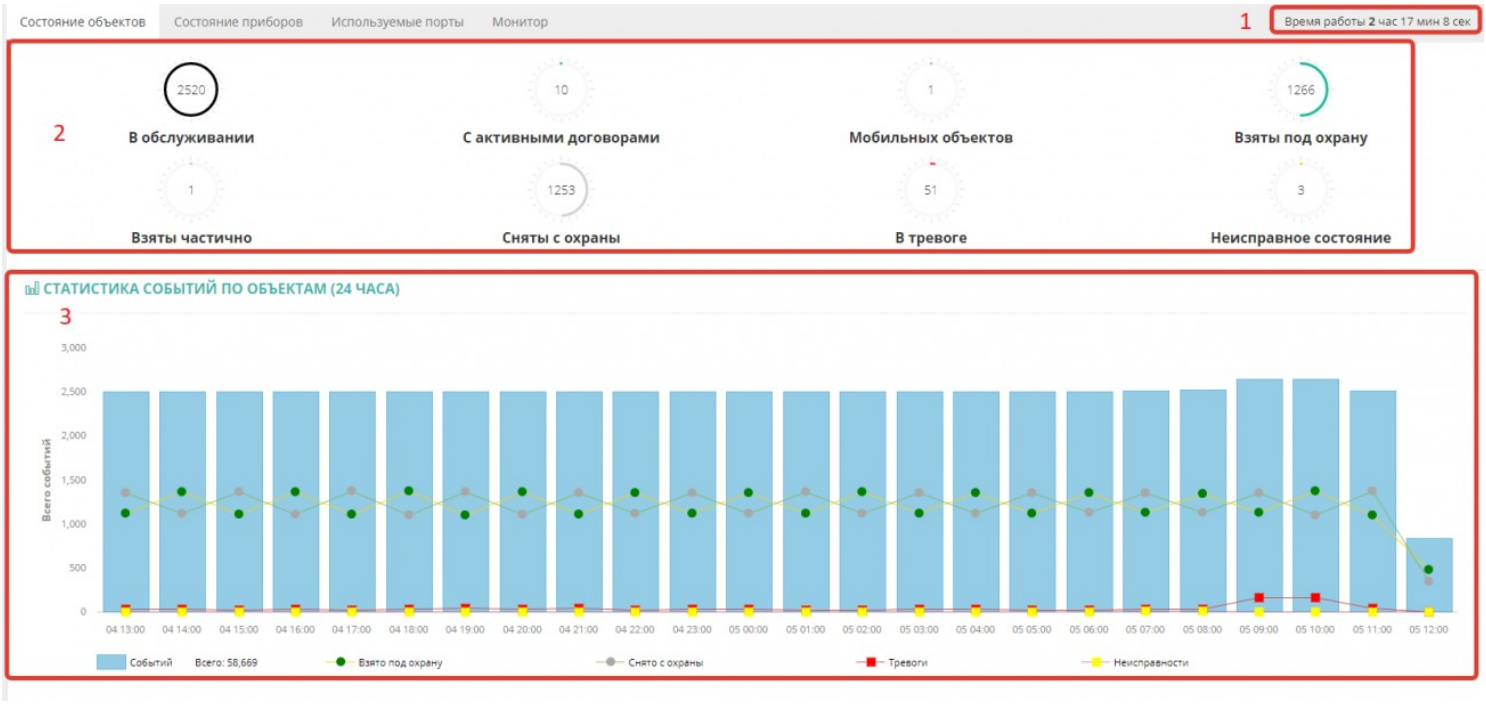


Рисунок 4.1 Состояние объектов

SEC.RU | Короткий путь к информации Скачано с sec.ru

4.2 Состояние приборов

Данное меню служит для мониторинга текущего состояния приборов охраны, и дает общую сводку по приборам (рисунок 4.2).

1. Время работы сервера КРОС без перезагрузки отображается в верхнем правом углу (цифра 1 на изображении внизу).
2. Состояние приборов и их состояния (цифра 2 на изображении внизу).
3. Статистика событий по объектам за 24 часа (цифра 3 на изображении внизу).

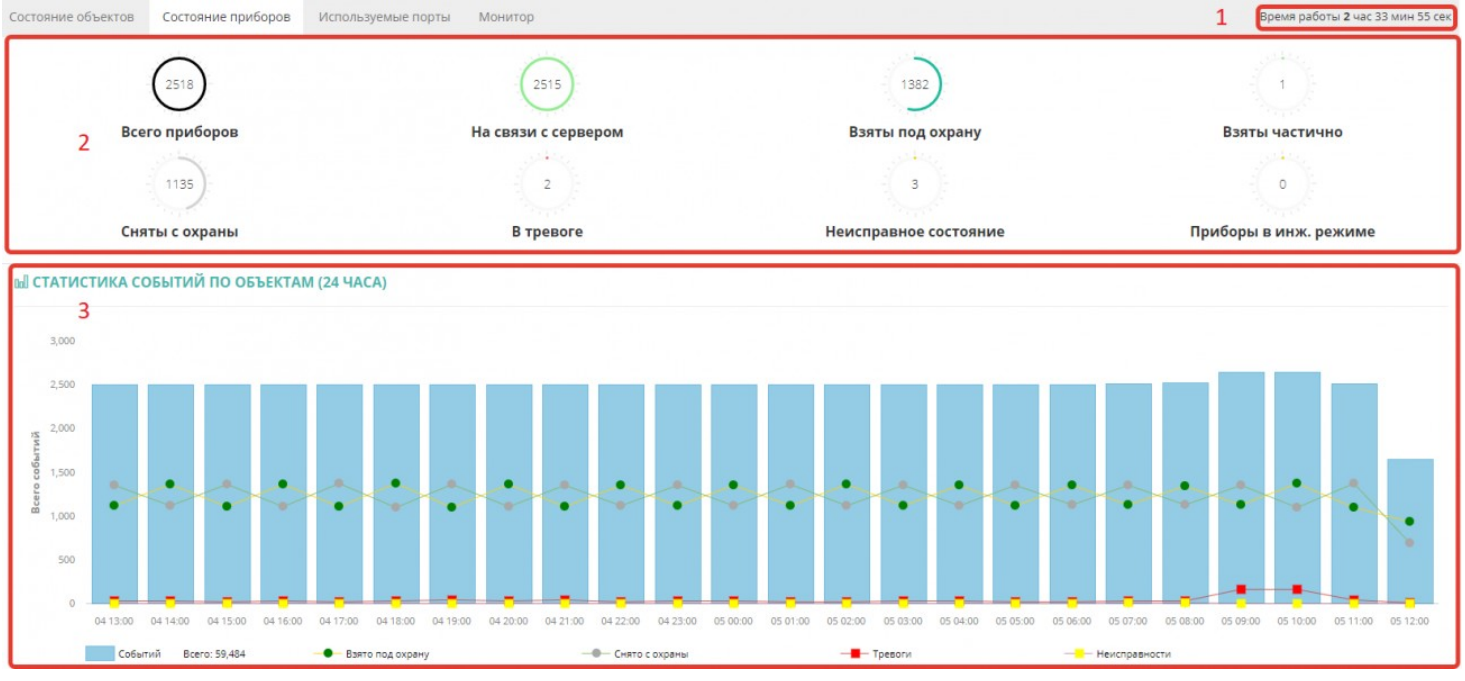


Рисунок 4.2 Состояние приборов

SEC.RU | Короткий путь к информации Скачано с sec.ru

4.3 Используемые порты

В данной вкладке указаны все порты, которые необходимы серверу КРОС для сопряжения со всеми приборами, компонентами и системами (рисунок 4.3).
Данная вкладка исключительно информативная, для изменения портов следует воспользоваться меню Охрана--->Реквизиты--->Редактирование охранной организации

Состояние объектов | Состояние приборов | Используемые порты | Монитор

UDP 10093-10095,10327	**Юпитер ППКОП/УОО UDP**
TCP 10093-10095,10327	**Юпитер ППКОП/УОО TCP**
TCP 4000	**Прием потока данных ЕППС по TCP**
TCP 20000	**Прием потока данных Surgard TCP**
Unknown	**Имитация прибора ПК4**
TCP 30000	**Прием потока данных от АРМ V7 по TCP/ЕППС**
TCP 25000	**Прием потока данных Surgard TCP (Десятичный ID)**
TCP 5001-5003	**Мобильное приложение Юпитер-ГЗ**
TCP 6001	**Система получение данных с часов Умка**
TCP 7009	**Система обновления АРМ**
TCP 2002-2004	**АРМ ДПУ/ДО/СК**
HTTP 9900	**Мобильное приложение Личный Кабинет**
HTTP 9900	**Мобильное приложение Тревожная Кнопка**
TCP 7101,7102	**GSM Модем**

Рисунок 4.3 Используемые порты

SEC.RU | Короткий путь к информации Скачано с sec.ru

4.4 Монитор

Данная вкладка предназначена для мониторинга входящих и исходящих соединений сервера КРОС (рисунок 4.4).
Здесь отображаются соединения для приемников (приборы по разным каналам связи) и для передатчиков (трансляции в АРМ, трансляции Surgard и прочие).
Также имеется возможность отслеживать нагрузку на трансляторы, следить за трафиком и очередью на передачу.

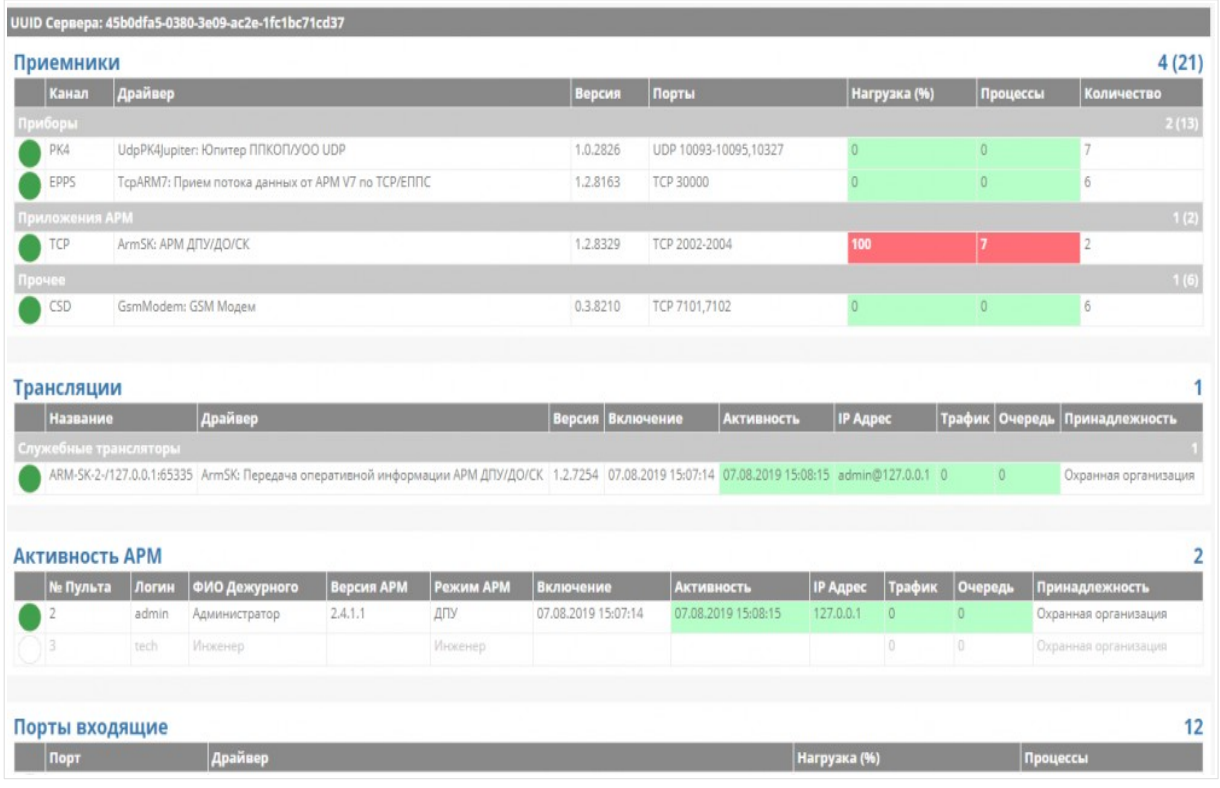


Рисунок 4.4 Монитор

Под учетной записью Администратора Сервера (superadmin) у вкладки появляется дополнительная информация о состоянии сервера (рисунок 4.5).

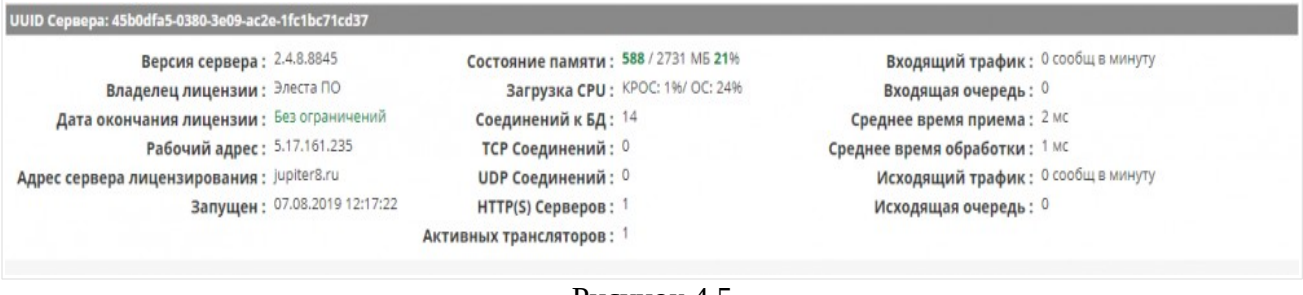


Рисунок 4.5

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Меню «Сервер»

5.1 Приемники

Окно «Приемники» доступно только **Администратору сервера** (рисунок 5.1).

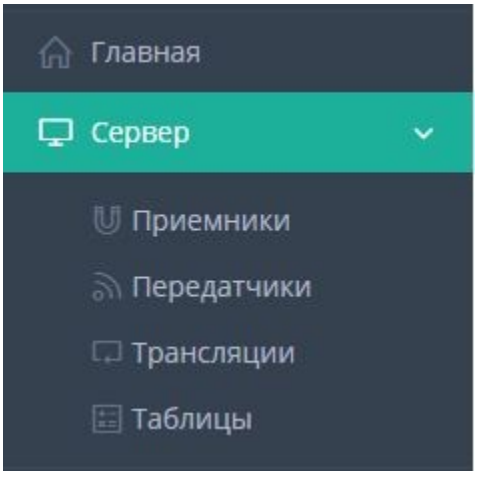


Рисунок 5.1 Меню «Приемники»

В окне «Приемники» (меню «Сервер»→«Приемники») представлен список драйверов, использующихся для сопряжения различных типов оборудования и внешнего программного обеспечения с комплексом КРОС, с возможностью их редактирования (рисунок 5.2).

В случае открытия (добавления) нового порта в приемнике, требуется дописать этот порт в настройках охранной организации (Охрана-Реквизиты-редактирование-Параметры-Диапазон разрешенных портов).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Активен	Драйвер	Версия	Список портов	Протокол	Описание	
☑	UdpRoot	1.2.7325	10000-19999 10027, 10093-10095	UDP	Поддержка Сервера Лицензирования	
☑	UdpPK4Jupiter	1.0.2826	10000-19999 10027, 10093-10095	UDP	Юпитер ППКОП/УОО UDP	
☑	ArmGZ	1.2.6146	5001-5003	TCP	Мобильное приложение Юпитер-ГЗ	
☑	TcpEPPS	1.2.8163	30000-34999 30000-30002	TCP	Прием потока данных ЕППС по TCP	
☑	TcpPK4Jupiter	1.0.323	10000-19999 10000, 10001, 10027, 10093-10095	TCP	Юпитер ППКОП/УОО TCP	
☑	CustomerAccount	1.2.604	9900	HTTP	Мобильное приложение Личный Кабинет	
☑	AlarmButton	1.2.604	9900	HTTP	Мобильное приложение Тревожная Кнопка	
☑	TcpSurgard	1.2.7206	20000-24999 20000-20002	TCP	Прием потока данных Surgard TCP	
☐	UdpEPPS	1.2.7325	10000-19999 10027, 10093-10095	UDP	Прием потока данных ЕППС по UDP	
☑	UmkaWatch	1.2.8290	6001	TCP	Система получение данных с часов Умка	
☑	ArmUpdater	1.3.8254	7009	TCP	Система обновления АРМ	
☑	GsmModem	0.3.8210	7101, 7102	TCP	GSM Модем	
☑	ArmSK	1.2.8329	2002-2004	TCP	АРМ ДПУ/ДО/СК	
☑	TcpSurgardDecID	1.2.7136	25000-29999 25000-25002	TCP	Прием потока данных Surgard TCP (Десятичный ID)	

Рисунок 5.2 Список драйверов

Для редактирования настроек необходимо:

1. В строке приемника нажать кнопку “Редактировать” (белый карандаш в синем квадрате), для вызова окна редактирования.
2. Перейти на вкладку «Параметры».
3. Внести изменения.
4. Нажать «Сохранить».

Имеется возможность включить\отключить нужные приемники. Для этого необходимо нажать на кнопку «Редактировать» (белый карандаш в синем квадрате), и в открывшемся окне снять галочку в пункте «Драйвер активен».

Чтобы закрыть без сохранения, нужно нажать на кнопку «Закрыть» в окне «Параметры приемника».

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.1.1 Базовые параметры для каждого приемника

- Драйвер активен

Индикация активности драйвера. Возможно включение и выключение драйвера, для этого необходимо установить режим активности и сохранить параметры. Перезагрузка сервера после этого не обязательна для всех драйверов, за исключением работающих по протоколу HTTP/HTTPS, т.к. они используют общий HTTP сервер.

- **Шифрование SSL**

Включение или отключение SSL шифрования для TCP и HTTP протоколов. Работает только в случае поддержки со стороны драйвера.

- **Наименование драйвера**

Информационное поле. Технический символьный идентификатор драйвера.

- **Краткое описание**

Информационное поле. Краткое описание драйвера.

- **Версия**

Информационное поле. Номер версии драйвера.

- **Сетевой протокол**

Информационное поле. Протокол, который используется в драйвере. Используемые варианты TCP, UDP, HTTP.

- **Служебный драйвер**

Информационное поле. Признак “служебный” имеют драйверы, которые

a) Имеют общий пул портов для всех охранных организаций. Остальным драйверам выделяется отдельный порт для каждой охранной организации, в рамках общего диапазона портов.
b) Не приводят к автоматическому созданию записи прибора в инженерном режиме (см. Инженерный режим).

В случае необходимости для драйвера могут быть определены специфические параметры:

- **Список портов**

диапазон TCP или UDP портов, выделяемых для драйвера из общего пула портов системы. Каждый драйвер имеет собственный диапазон, не пересекающийся с остальными. В случае если драйвер не является служебным - каждой охранной организации, регистрируемой в системе КРОС, выделяется индивидуальный порт из этого диапазона.

- **TCP таймаут (мс)**

Таймаут, устанавливаемый на TCP соединение и чтение. Устанавливается для TCP сокета на системном уровне.

- **Таблица перекодировки по умолчанию**

Базовая таблица перекодировки, используемая для преобразования и нормализации получаемых сообщений перед их поступлением на обработку в КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.1.2 Индивидуальные параметры для приемников UdpPK4Jupiter, TcpPK4Jupiter

- **Транслировать сообщения дежурного режима**

Разрешение обработки сообщений 20602 Дежурный режим и 10602 Периодический тест устройства . По умолчанию эти сообщения не поступают на обработку в КРОС, соответственно не попадают в трансляцию, т.к. драйвер ПК4 сам контролирует состояние связи с прибором. Для того чтобы сообщения дежурного режима попадали в ленту сообщений и транслировались необходимо включить этот параметр.

- **Удалять отключенные разделы после опроса**

После получения информации от прибора о его конфигурации КРОС проверяет, о каких разделах были получены данные. Если о каком-то из имеющихся разделов данных не было - он удаляется из конфигурации прибора в базе данных КРОС. Однако в случае большого количества сетевых ошибок КРОС может получить от прибора неполную или искаженную информацию, несмотря на несколько уровней контроля целостности. Чтобы гарантированно исключить случайное удаление разделов нужно деактивировать этот параметр.

- **Удалять отключенные зоны после опроса**

То же самое для зоны (шлейфа).

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.2.2 Индивидуальные параметры для приемника GsmModem

- **Список соответствий номеров телефонов модема**

Определение базового соответствия набора функций “Дозвон без соединения” с номерами телефона GSM модема. Для этой функции по умолчанию используются настройки, заданные индивидуально для охранной организации. Однако в случае использования одного модема для нескольких охранных организаций и/или отсутствия этих настроек в параметрах охранной организации - будет использован этот базовый список (см. Параметры охранной организации).

○ Номер телефона - номер телефона канала GSM модема.

○ Действие - действие, инициируемое КРОС, в случае получения звонка на указанный канал модема. Возможные варианты:

■ Дежурный режим

■ Тревога

■ Взять

■ Снять

5.2.3 Индивидуальные параметры для приемника ArmSK

- **Период контроля повторного входа (сек)**

Период времени, после которого “зависшие” сессии АРМ (ДПУ/ДО/СК) считаются неактивными системой контроля повторного входа. При установленном параметре “Запрет работы в нескольких АРМ под одним именем” в Параметры охранной организации происходит блокировка входа в АРМ, в случае если предыдущая сессия работы пользователя не завершена. Параметр ограничивает период, в течение которого незавершённые сессии будут считаться активными, т.о. отсекая “зависшие” сессии.

5.2.4 Индивидуальные параметры для приемника ArmUpdater

- **Путь к дистрибутиву**

Путь к каталогу, куда будут помещены обновления версий АРМ. В настоящее время используется только для централизованной системы обновления на jupiter8.ru, в дальнейшем планируется возможность создания локальных синхронизируемых репозиториев для каждого сервера КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.2 Передатчики

Окно «Передатчики» доступно только **Администратору сервера**.
В окне «Передатчики» (меню «Сервер»→«Передатчики») представлен список драйверов, предназначенных для передачи потока информации в реальном времени на программы и устройства, работающими с ними (рисунок 5.3 и 5.4).

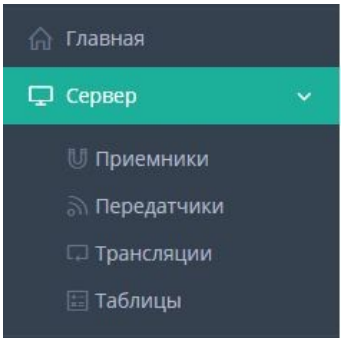


Рисунок 5.3 Меню «Передатчики»

Имеется возможность включить\отключить нужные передатчики. Для этого необходимо нажать на кнопку «Редактировать» (белый карандаш в синем квадрате), и в открывшемся окне снять галочку в пункте «Драйвер активен».

Активен	Драйвер	Версия	Описание	
✓	UmkaWatch	1.2.0	Отправка сообщения на часы Umka	
✓	F1ComImei	1.2.6547	Трансляция данных по протоколу F1Com (IMEI)	
✓	SmsSMPP	1.2.7575	Передача оперативной информации по SMS	
✓	CsvWriter	1.2.6213	Запись потока сообщений в CSV файл	
✓	RawSender	1.2.6635	Ретранслятор пакетов в формате Envelope/JSON	
✓	TcpSurgardV4	1.0.7374	Трансляция данных по протоколу TCP Surgard V4	
✓	F1Com	1.0.6547	Трансляция данных по протоколу F1Com	
✓	TcpEPPS	1.2.7226	Передача информации по протоколу ЕППС (Beta)	
✓	CustomerAccount	1.2.7418	Передача оперативной информации приложению Личный Кабинет	
✓	TcpSurgard	1.0.7374	Трансляция данных по протоколу TCP Surgard	
✓	ArmSK	1.2.7252	Передача оперативной информации АРМ ДПУ/ДО/СК	

Рисунок 5.4 Список передатчиков

5.2.1 Базовые параметры для каждого приемника

- **Драйвер активен**

Индикация активности драйвера. Возможно включение и выключение драйвера, для этого необходимо установить режим активности и сохранить параметры. Перезагрузка сервера после этого не обязательна. Деактивация драйвера приведет к остановке всех трансляторов, использующих этот драйвер (см. Трансляции).

- **Наименование драйвера**

Информационное поле. Технический символьный идентификатор драйвера.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Краткое описание**

Информационное поле. Краткое описание драйвера.

- **Версия**

Информационное поле. Номер версии драйвера.

- **Сетевой протокол**

Информационное поле. Протокол, который используется в драйвере. Используемые варианты TCP, UDP, HTTP.

- **Служебный драйвер**

Информационное поле. Признак “служебный” имеют драйверы, которые используются КРОС для создания системных трансляций, создаваемых автоматически, и недоступны для создания трансляций вручную. Если признак снят - трансляцию с этим драйвером можно создать только вручную.

5.2.2 Индивидуальные параметры для передатчика ArmSK

Обычно параметры трансляции, необходимые для работы конкретного драйвера передатчика, определяются при создании трансляции. Однако ArmSK является служебным драйвером, поэтому необходимые параметры задаются в параметрах драйвера, и действуют на все автоматически создаваемые трансляции.

- **Использовать пакетный режим передачи данных**

АРМ может работать в режиме пакетной передачи данных. В этом режиме на стороне КРОС сообщения из очереди трансляции передаются не индивидуально, а собираются в пакет с установленным максимальным размером, и только после этого передаются, а поскольку сетевой обмен имеет наиболее критичные временные показатели в системе клиент-сервер - достигается значительное ускорение обмена данными.

- **Максимальный размер блока данных (байт)**

Установка максимального размера пакета данных для пакетного режима.

- **Период отправки PING пакетов (сек)**

Периодичность проверки активности TCP сессии со стороны КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3 Трансляции

В окне «Трансляции» (меню «Сервер» → «Трансляции») создаются, настраиваются и удаляются трансляции передачи событий (например трансляция в протоколе Surgard) (рисунок 5.5).

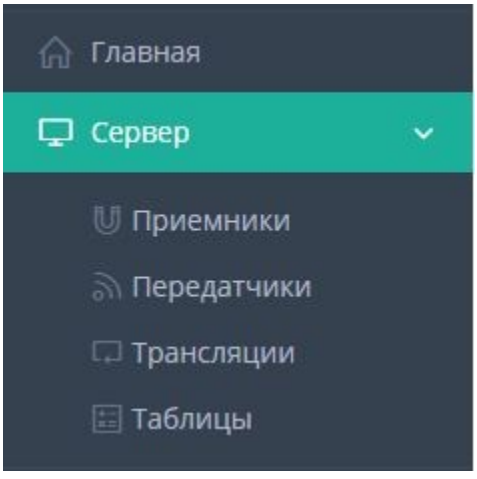


Рисунок 5.5 Меню «Трансляции»

Окно «Трансляции» по-умолчанию доступно **Администратору сервера, Администратору и Инженеру.**

Администратор сервера не может добавлять новые трансляции передачи событий (кроме трансляции зеркалирования), но может редактировать и удалять существующие.

Трансляции передачи событий позволяют **администратору охранной организации** организовать передачу данных в выбранном протоколе на сторонний сервер, для дублирования событий по выбранным объектам охраны.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.1 Добавление трансляции

Для добавления новой трансляции передачи событий:

1. Нажать на кнопку«Добавить трансляцию».
Откроется окно«Трансляция» (рисунок 5.6)

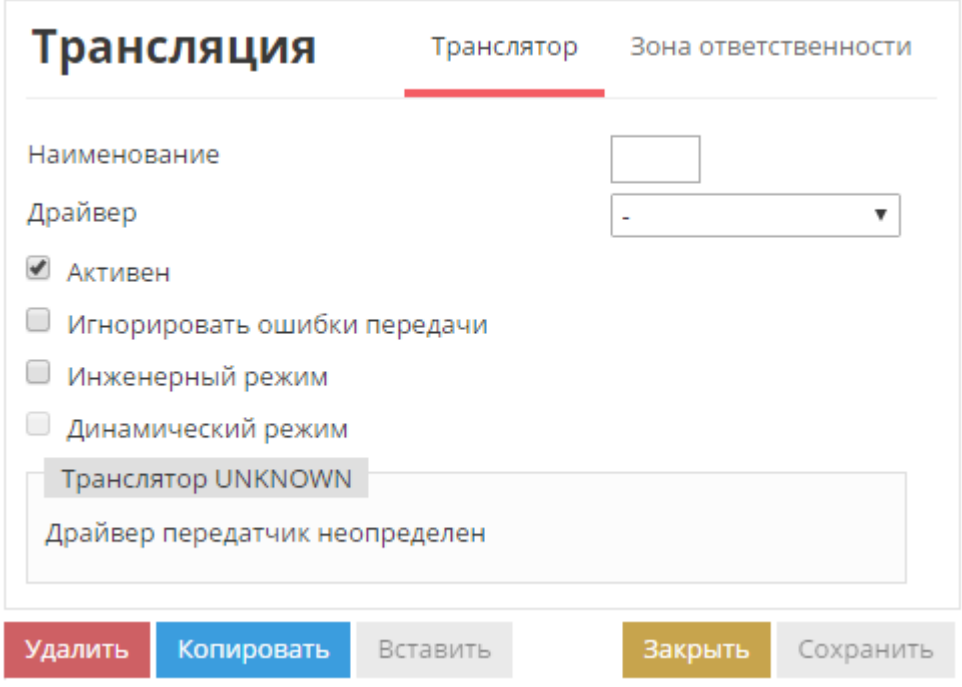


Рисунок 5.6 Окно «Трансляция»

2. Заполнить поле «Наименование» и выбрать «Драйвер» (рисунок 5.8).

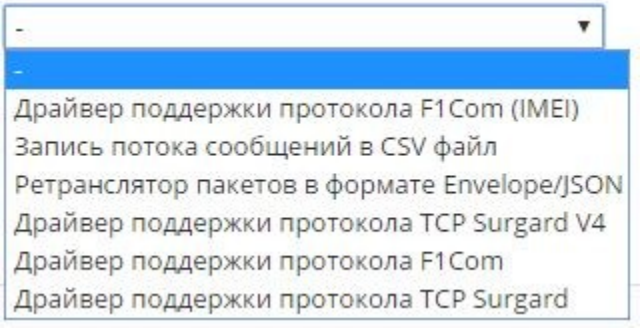


Рисунок 5.8 Список драйверов

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Ввести IP4-адрес и TCP порт куда будет осуществляться трансляция передачи событий (рисунок 5.9).

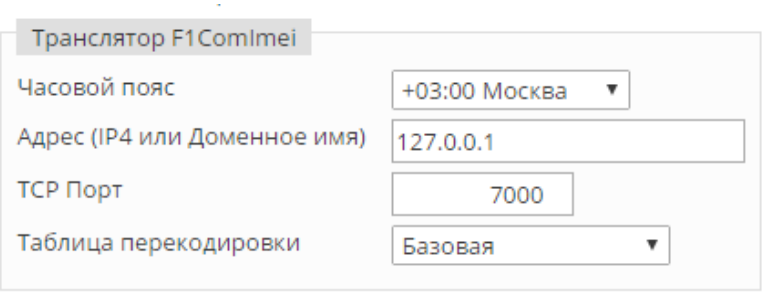


Рисунок 5.9 Адрес назначения трансляции

4. Из выпадающего списка «Таблицы перекодировки», если он есть, выбрать таблицу перекодировки сообщений\извещений.

5. Перейти на вкладку «Зона обслуживания».

6. Выбрать объекты охраны, данные по которым будут транслироваться.

Примечание: Чтобы отобразить список объектов охраны, которые входят в определенную территорию на карте, необходимо создать зону обслуживания.

Для этого нужно кликнуть на пятиугольник (добавить зону обслуживания), расположенный в левом углу окна и отметить территорию.

После нанесения на карту зоны обслуживания в списке «Результаты фильтрации» отобразятся объекты охраны которые входят в отмеченную зону.

7. Нажать на кнопку «Сохранить» в окне «Трансляция».

Для закрытия без сохранения, нажать на кнопку «Закрыть» или «Удалить» в окне «Трансляция».

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.2 Редактирование трансляции

Для редактирования настроек необходимо:

1. Нажать на кнопку «редактировать» (синий карандаш) трансляцию.

2. Внести изменения в трансляцию.

3. Нажать «Сохранить».

Для закрытия без сохранения, нажать на кнопку «Закрыть» в окне «Трансляция».

5.3.3 Удаление трансляции

Для удаления трансляции:

1. Нажать на кнопку «Редактировать» (синий карандаш) трансляцию.

2. Нажать «Удалить» в окне «Трансляция».

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.3.4 Базовые параметры для всех типов трансляций

- **Наименование**

Индивидуальное наименование трансляции, которое будет отображаться в списке и окне статистики.

- **Драйвер**

Выбор драйвера для трансляции из списка доступных драйверов передатчиков. В зависимости от выбранного драйвера будет установлено содержимое блока Параметры.

- **Активен**

Индикация активности трансляции. Позволяет остановить уже созданную трансляцию. При этом очередь на отправку не будет формироваться.

- **Игнорировать ошибки передачи**

Параметр действует для трансляций, взаимодействующих с внешними приемниками по сети. Определяет является ли доставка сообщений гарантированной. В случае если этот параметр отключен при возникновении ошибки передачи сообщение не удаляется из очереди и будет отправляться повторно до тех пор пока не будет успешно принято. Если параметр установлен - сообщение удаляется из очереди независимо от результатов передачи.

- **Инженерный режим**

По умолчанию система КРОС транслирует только сообщения от приборов и их разделов, работающих в штатном режиме, т.е. связанных с охраняемыми объектами. Если требуется трансляция данных только от приборов в Инженерном режиме - можно использовать этот параметр.

- **Динамический режим**

Признак того что для формирования очереди на трансляцию используется только оперативная память, т.е. данные очереди не сохраняются в базе данных. При перезапуске сервера очередь на трансляцию будет обнулена. Этот признак определяется свойствами используемого драйвера и не может быть изменен.

5.3.5 Индивидуальные параметры для передатчика TcpSurgard

- **Часовой пояс**

Часовой пояс, в котором работает внешний приемник. Все временные параметры отправляемых пакетов будут приведены к локальному времени этого приемника.

- **Адрес (IP4 или Доменное имя)**

Целевой адрес трансляции - адрес внешнего приемника.Может быть указано доменное имя или IP адрес сети интернет или локальной сети.

- **TCP Порт**

Целевой порт для трансляции.

- **TCP Таймаут (мс)**

Таймаут соединения и чтения, устанавливаемый для TCP сокета, используемого для связи с внешним приемником.

- **PING Период (сек)**

SEC.RU | Короткий путь к информации Скачано с sec.ru

Периодичность отправки контрольных пакетов для поддержания неразрывной TCP сессии с внешним приемником. По умолчанию 5 секунд.

- **Таблица перекодировки**

Таблица, в соответствии с которой будет преобразован поток данных, отправляемый на внешний приемник.

- **Передавать идентификатор в десятичном формате**

Пакет SurGard может содержать идентификатор OID в десятичном или шестнадцатеричном формате. При этом диапазон идентификаторов в первом случае ограничивается 0..9999, во втором 0..65535. Установка зависит от возможностей внешнего приемника.

- **Ожидать подтверждения о получении пакета данных**

По умолчанию драйвер передатчик ожидает подтверждения от внешнего приемника о получении для каждого отправленного пакета. Этим достигается гарантированность доставки данных. Этот параметр позволяет отключить ожидание подтверждений и отправлять поток данных без гарантии доставки.

- **Кодировать порт и канал источника**

Параметр задает способ формирования заголовка SurGard сообщения. По умолчанию номер порта и номер канала устанавливаются в 1, и заголовок выглядит как “5011 18”. Если параметр установлен, то в качестве номера порта устанавливается порядковый номер порта охранной организации, на который было принято исходное сообщение, в качестве номера канала - порядковый номер канала передачи данных прибора, по которому было принято исходное сообщение. Параметры заголовка устанавливаются только если существует такая возможность.

- **Автоматически создавать канал ContactID для подключаемых приборов**

В случае трансляции данных от прибора, не содержащего канала CID (ContactID), канал будет автоматически создан и добавлен в прибор. В качестве OID будет использован идентификатор ID6 в случае если прибор имеет канал PK4, либо идентификатор записи из базы данных, если нет. В качестве IMEI будет использован ИН прибора.

5.3.6 Индивидуальные параметры для передатчика TcpSurgardv4

- **Часовой пояс**

Часовой пояс, в котором работает внешний приемник. Все временные параметры отправляемых пакетов будут приведены к локальному времени этого приемника.

- **Адрес (IP4 или Доменное имя)**

Целевой адрес трансляции - адрес внешнего приемника.Может быть указано доменное имя или IP адрес сети интернет или локальной сети.

- **TCP Порт**

Целевой порт для трансляции.

- **TCP Таймаут (мс)**

Таймаут соединения и чтения, устанавливаемый для TCP сокета, используемого для связи с внешним приемником.

- **PING Период (сек)**

Периодичность отправки контрольных пакетов для поддержания неразрывной TCP

SEC.RU | Короткий путь к информации Скачано с sec.ru

сессии с внешним приемником. По умолчанию 5 секунд.

- **Таблица перекодировки**

Таблица, в соответствии с которой будет преобразован поток данных, отправляемый на внешний приемник.

- **Ожидать подтверждения о получении пакета данных**

По умолчанию драйвер передатчик ожидает подтверждения от внешнего приемника о получении для каждого отправленного пакета. Этим достигается гарантированность доставки данных. Этот параметр позволяет отключить ожидание подтверждений и отправлять поток данных без гарантии доставки.

- **Ожидать подтверждения о получении пакета PING**

По умолчанию драйвер передатчик ожидает контрольного подтверждения от внешнего приемника о получении для каждого отправленного контрольного пакета. Этот параметр позволяет отключить ожидание подтверждений.

- **Кодировать порт и канал источника**

Параметр задает способ формирования заголовка SurGard сообщения. По умолчанию номер порта и номер канала устанавливаются в 1, и заголовок выглядит как “5011 18”. Если параметр установлен, то в качестве номера порта устанавливается порядковый номер порта охранной организации, на который было принято исходное сообщение, в качестве номера канала - порядковый номер канала передачи данных прибора, по которому было принято исходное сообщение. Параметры заголовка устанавливаются только если существует такая возможность.

- **Автоматически создавать канал ContactID для подключаемых приборов**

В случае трансляции данных от прибора, не содержащего канала CID (ContactID), канал будет автоматически создан и добавлен в прибор. В качестве OID будет использован идентификатор ID6 в случае если прибор имеет канал PK4, либо идентификатор записи из базы данных, если нет. В качестве IMEI будет использован ИН прибора.

5.3.7 Индивидуальные параметры для передатчика TcpEPPS

- **Отправитель**

Выбор охранной организации, данные которой будут транслироваться по протоколу ЕППС. Этот параметр появляется только в режиме Администратора сервера при создании Зеркалирования.

- **Код идентификации получателя**

Идентификатор охранной организации в контексте удаленного приемника, для которой будет происходить трансляция.

- **Адрес (IP4 или Доменное имя)**

Целевой адрес трансляции - адрес внешнего приемника.Может быть указано доменное имя или IP адрес сети интернет или локальной сети.

- **Порт**

Целевой порт для трансляции.

- **TCP Таймаут соединения (мс)**

Таймаут соединения, устанавливаемый для TCP сокета, используемого для связи с целевым сервером. В системах с зеркалированием попытка соединения происходит

SEC.RU | Короткий путь к информации Скачано с sec.ru

при старте сервера, и если целевой сервер не отвечает то это приведет к задержке старта. С целью минимизации ожидания запуска сервера таймауты соединения и чтения разделены. По умолчанию 5 секунд.

- **TCP Таймаут чтения (мс)**

Таймаут чтения, устанавливаемый для TCP сокета, используемого для связи с целевым сервером. По умолчанию 2 минуты.

- **PING Период (сек)**

Периодичность отправки контрольных пакетов для поддержания неразрывной TCP сессии с целевым сервером. По умолчанию 5 секунд.

- **Максимальный размер блока (байт)**

ЕППС драйвер использует бинарный протокол с оптимизацией передачи данных, путем группировки нескольких пакетов в один. Этот параметр устанавливает максимально допустимый размер передаваемого бинарного пакета.

- **Использовать SSL шифрование**

Передача данных по протоколу ЕППС может быть защищенной с помощью SSL шифрования.

- **Таблица перекодировки**

Таблица, в соответствии с которой будет преобразован поток данных, отправляемый на целевой сервер.

- **Зеркалирование**

Индикация режима зеркалирования. Отображается только для трансляций созданных в режиме Администратора сервера и обеспечивающих Зеркалирование.

- **Период подтверждающей синхронизации (секунд)**

Только для режима Зеркалирования - период контрольной проверки соответствия данных по базовым объектам зеркалирования.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.4 Таблицы

В окне «Таблицы» (меню «Сервер» → «Таблицы») создаются, редактируются и удаляются таблицы перекодировки сообщений\извещений (рисунок 5.10).

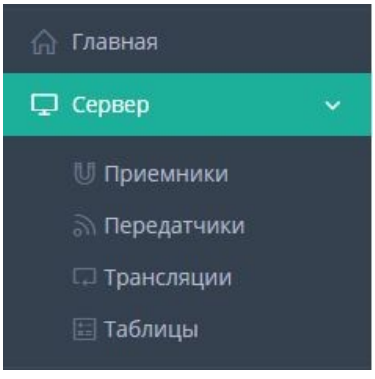


Рисунок 5.10 Меню «Таблицы»

Юпитер-КРОС содержит конечный список обрабатываемых сообщений, поступающих от внешних

источников. Каждому сообщения сопоставлен 5-значный десятичный системный код. Каждое сообщение имеет тип, или категорию. Возможные варианты категорий сообщений:

- Управление
- Тревога
- Взятие/Снятие
- Неисправность
- Информация
- Внимание
- Саботаж
- Питание
- Связь
- Диагностика

В зависимости от категории сообщению присваивается цвет отображения текста и фона. Кроме того каждому сообщению в соответствие ставится код SurGard для возможности двусторонних

SEC.RU | Короткий путь к информации Скачано с sec.ru

преобразований потоков данных.

Таблицы перекодировки служат для преобразования, нормализации и фильтрации сообщений.

В системе КРОС существует базовая таблица сообщений, все остальные таблицы - производные от нее, которые “накладываются” на базовую таблицу и хранят только список изменений.

Существует несколько общих таблиц, доступных для редактирования только Администратору сервера. Локальные таблицы для индивидуального использования может создать Администратор охранной организации, и они буду работать только в одной охранной организации.

Таблицы перекодировки сообщений\извещений служат для возможности изменения формируемых сообщений выводимых в ленту событий:

- АРМ
- мобильное приложение "Личный кабинет"
- трансляции в протоколе SurGard

Возможные операции с таблицами:

- Блокировка таблицы

Параметр доступный только Администратору сервера, определяет будет ли текущая таблица доступны для изменения сотрудникам охранных организаций.

- **Добавить таблицу**

Создать новую таблицу. Будет запрошено имя для новой таблицы. Если операция вызвана Администратором сервера - будет создана общедоступная таблица, если Администратором охранной организации - будет создана локальная таблица, доступная только в рамках охранной организации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Дублировать таблицу**

Будет создана копия текущей таблицы и запрошено для нее новое имя. Если операция вызвана Администратором сервера - будет создана общедоступная таблица, если Администратором охранной организации - будет создана локальная таблица, доступная только в рамках охранной организации.

- **Удалить таблицу**

Удаление текущей таблицы. Базовую таблицу удалить нельзя. Администратор сервера может удалить общие таблицы. Администратор охранной организации - только локальные.

- **Экспорт**

Сохранить текущую таблицу в файл в формате XML. Будет запрошено имя файла.

- **Импорт**

Создать новую таблицу из ранее сохраненного XML файла. Будет создана таблица с именем сохраненной таблицы с добавлением даты и времени импорта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.4.1 Добавление таблицы

Чтобы добавить таблицу перекодировки сообщений\извещений нужно:

1. Нажать на кнопку добавить (Белый плюс на зеленом фоне).
2. В появившемся окне подтверждения ввести название таблицы (рисунок 5.11).

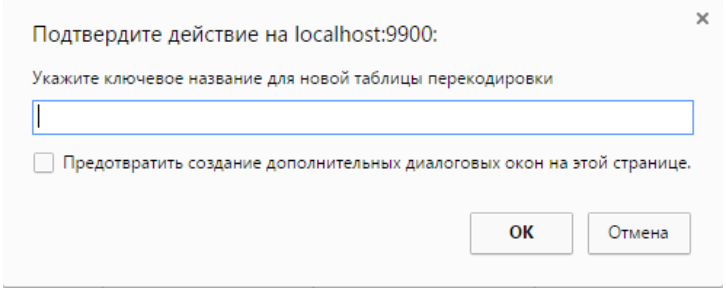


Рисунок 5.11 Ввод названия таблицы

3. Нажать «OK».

5.4.2 Редактирование сообщений в таблице

Сообщения из таблицы отображаются в строке сообщений АРМ, можно отредактировать сообщение если не подходят какие-либо его параметры.

Например, можно сделать так, чтобы вместо сообщения «Нажата Кнопка Паники» (E101) приходило сообщение «Нажата Кнопка Тревога», изменив значение поля «Формируемое сообщение».

Для редактирования сообщения в таблице:

1. Через поиск найти текущее название сообщения.
2. Нажать на кнопку редактировать (Белый карандаш на синем фоне).
3. После нажатия открывается окно редактирования сообщения(рисунок 5.12).

В данном окне имеется возможно задать:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Блокировка передачи сообщения**

Блокировка сообщения. Фильтры использующие редактируемую таблицу не будут пропускать это сообщение.

- **Внешний квалификатор**

SurGard квалификатор, соответствующий выбранному сообщению - R или E.

- **Внешний код**

SurGard код, соответствующий выбранному сообщению - 3 десятичные цифры.

- **Тип сообщения**

Категория, к которой относится выбранное сообщение. Изменение этого параметра может повлиять на логику обработки сообщения. Выбор из списка.

- **Формируемое сообщение**

Текст формируемого сообщения для ленты.

- **Цвет сообщения**

Цвет текста сообщения для отображения.

- **Цвет фона**

Цвет фона сообщения для отображения.

- **Удалить**

В случае редактирования производной таблицы будут удалены только изменения относящиеся к этой таблице. т.е. “удаленную” запись заменит запись с тем же кодом из базовой таблицы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

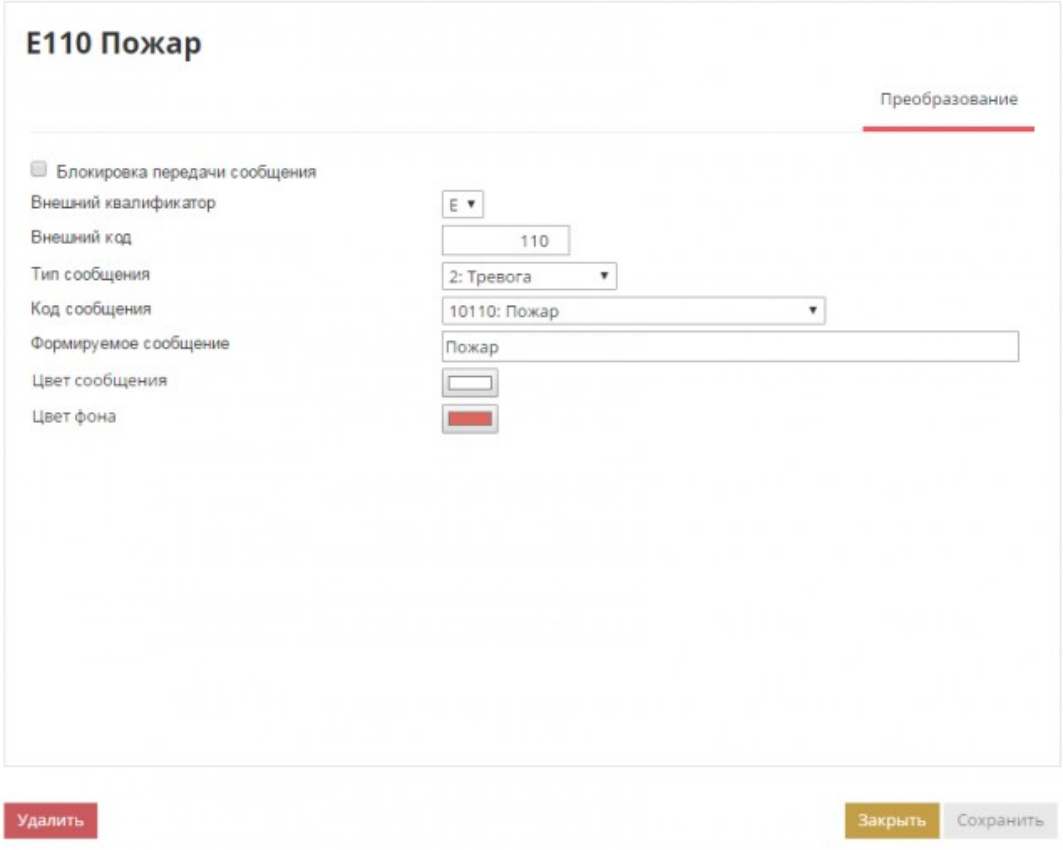


Рисунок 5.12 Окно редактирования сообщения

4. После изменения нажать «Сохранить»
Для закрытия без сохранения, нажать на кнопку «Закрыть» в окне сообщения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.4.3 Выбор таблицы

Для переключения таблицы перекодировки сообщений\извещений нужно:

1. Нажать по выпадающему меню.
2. Выбрать нужную таблицу (рисунок 5.13).

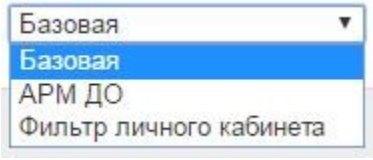


Рисунок 5.13 Выбор таблицы

5.4.4 Удаление таблицы

Для удаления таблицы перекодировки сообщений\извещений нужно:

1. Выбрать таблицу.
2. Нажать на кнопку «Удалить таблицу».

Для удаления доступны только таблицы перекодировки сообщений\извещений, созданные пользователями.
Таблицы «Базовая», «АРМ ДО» и «Фильтр личного кабинета» удалить нельзя.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6. Меню «Клиенты»

6.1 Договоры

В окне «Договоры» (меню «Клиенты» → «Договоры») создаются, настраиваются и удаляются договоры охраны. Так же в этом окне производится добавление объекта охраны к существующему договору охраны (рисунок 6.1).

Окно «Договоры» по-умолчанию доступно **Администратору и Менеджеру**.

Под договорами охраны подразумеваются договоры с физическими или юридическими лицами, подключенными на пульт централизованного наблюдения.

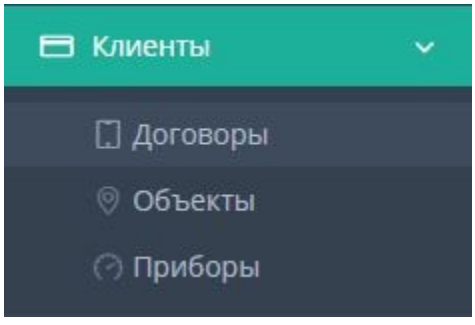


Рисунок 6.1 Меню «Договоры»

6.1.1 Добавление, редактирование и удаление договора охраны

6.1.1.1 Добавление договора охраны

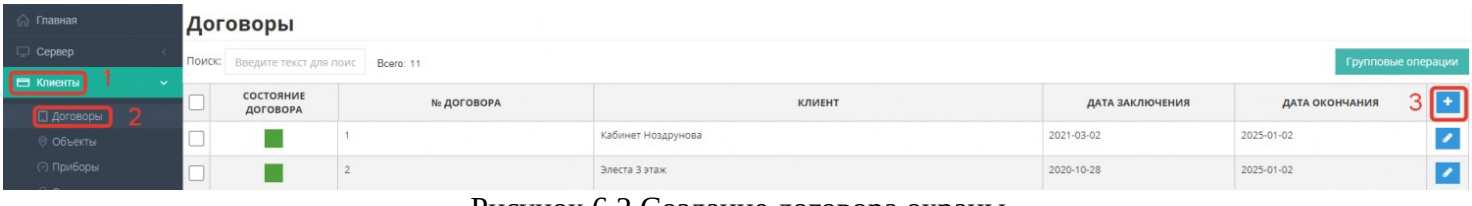


Рисунок 6.2 Создание договора охраны

1. Зайти под учетной записью, имеющей право на добавление договоров (admin - логин и пароль по умолчанию).

2. Перейти в меню Клиенты ---> Договоры ---> Создать новый договор (рисунок 6.2).

3. В открывшемся окне на вкладке «Основная» ввести номер договора охраны, дату заключения, дату окончания, выбрать состояние.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Также в меню "Реквизиты" поле "Наименование" обязательно к заполнению при создании договора. Остальные поля заполняются по необходимости.

6.1.1.1.1 Вкладка «Ответственные лица»

1. Нажать на кнопку добавить (белый плюс на синем фоне), чтобы добавить новое ответственное лицо (задаются данные пользователя, который имеет возможность использовать Личный кабинет или Тревожную кнопку).

2. Нажать «Да», чтобы подтвердить добавление новой записи.

3. Заполнить поля

Логин и пароль предоставляют доступ к «Личному кабинету» и «Тревожной кнопке».

Внимание! В договоре, помимо ответственных лиц, будут отображаться все ХозОрганы, созданные в карточках объектов, привязанных к данному договору.

6.1.1.1.2 Вкладка «Реквизиты»

1. Перейти на вкладку «Реквизиты».

2. В поле «ИНН» ввести номер ИНН.

3. Нажать кнопку («Найти по ИНН»)

Внимание! В меню "Реквизиты" поле "Наименование" обязательно к заполнению при создании договора.

6.1.1.1.3 Вкладка «Объекты»

1. Перейти во вкладку «Объекты».

2. Выбрать объекты, которые необходимо привязать к договору.

Во вкладке "Объекты" можно привязать объект только в том случае, если он был заранее создан во вкладке Клиенты ---> Объекты, в ином случае привязка происходит через карточку объекта.

Для сохранения договора охраны, нужно нажать кнопку «Сохранить» в окне «Договор», чтобы не сохранять, нужно нажать кнопку «Закрыть» в окне «Договор».

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.1.1.2 Редактирование договора охраны

1. Нажать на кнопку «Редактировать» (Белый карандаш на синем фоне) договор охраны.

2. Внести изменения в договор охраны.

3. Нажать кнопку «Сохранить».

Для закрытия договора охраны без сохранения, нажать «Закрыть» в окне «Договор».

6.1.1.3 Удаление договора охраны

1. Нажать на кнопку «Редактировать» (Белый карандаш на синем фоне) договор охраны.

2. Нажать кнопку «Удалить» в окне «Договор».

6.1.1.4 Групповые операции с договорами охраны

При выборе нескольких договоров и нажатии на "Групповые операции" появляется окно (рисунок 6.2.1), в котором можно:

1. Активировать договора, Приостановить до, Закрыть договора и Изменить дату окончания

2. Удалить выбранные договора

3. Для отмены нажать кнопку "Закрыть окно"

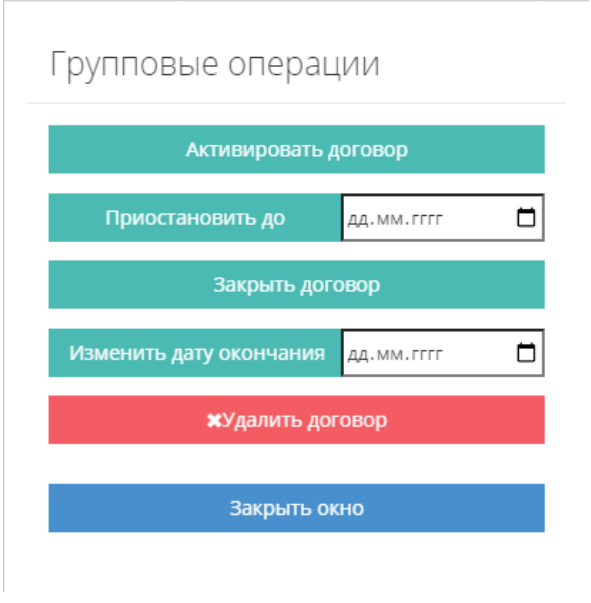


Рисунок 6.2.1 Групповые операции с договорами

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.1.2 Добавление объекта охраны к договору охраны

1. Перейти на вкладку Клиенты ---> Договоры ---> Редактировать договор.
2. В карточке договора перейти в меню "Объекты".
3. Выбрать объекты, которые хотите привязать (рисунок 6.3).

Во вкладке "Объекты" можно привязать объект только в том случае, если он был заранее создан во вкладке Клиенты ---> Объекты , в ином случае привязка происходит через карточку объекта.

Для сохранения договора охраны, нужно нажать кнопку «Сохранить» в окне «Договор», чтобы не сохранять, нужно нажать кнопку «Закрыть» в окне «Договор».

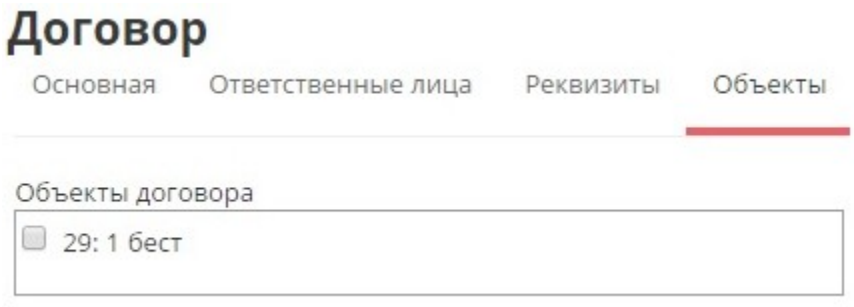


Рисунок 6.3 Привязка объекта к договору

6.1.3 Иерархия

На охрану объекта или нескольких объектов заключается **договор охраны,** к которому будет привязан **объект охраны**.

Объект охраны состоит из **разделов** одного или нескольких приборов.

Раздел состоит из зон.

Зона — это часть охраняемого **объекта**, контролируемого одним **шлейфом** охранной организации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2 Объекты

Вверху окна «Объекты» (меню «Клиенты» → «Объекты») отображается количество объектов охраны (в рамках одной охранной организации), поле для поиска объекта охраны и кнопка сортировки (рисунок 6.4).

Окно «Объекты» по-умолчанию доступно для **Администратора, Менеджера и Инженера.**

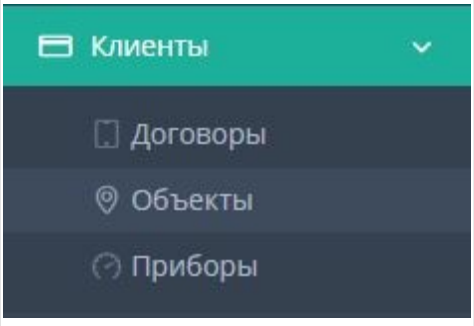


Рисунок 6.4 Меню "Объекты"

Сортировка объектов охраны делиться на четыре типа:

- Без договоров (Объекты охраны не привязанные к договору).
- С договорами (Объекты охраны привязанные к договорам).
- Приостановленные (Объекты охраны с приостановленным обслуживанием).
- Импортированные (Импортированные из Юпитера-7 объекты охраны)
- Все (Все объекты охраны).

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.1 Добавление, редактирование и удаление объекта охраны

6.2.1.1 Добавление объекта

Для добавления нового объекта охраны необходимо:

1. Зайти под учетной записью, имеющей права на добавление нового объекта (admin - логин и пароль по умолчанию).

2. Перейти в меню Договоры ---> Объекты ---> Создать новый объект (рисунок 6.5).

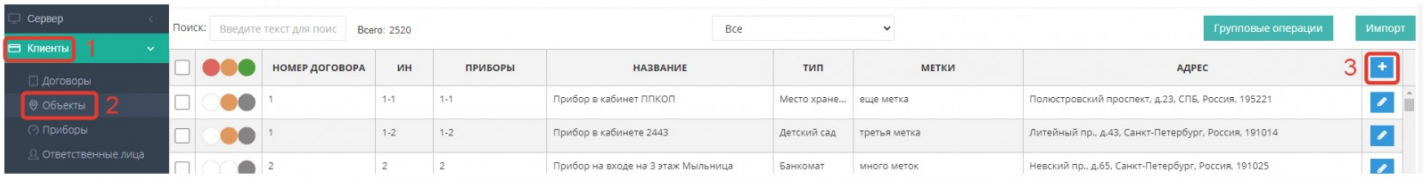


Рисунок 6.5 Создание нового объекта

3. Заполнить все необходимые поля и нажать кнопку "Сохранить", либо кнопку "Закрыть", чтобы выйти без сохранения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.1.2 Редактирование объекта

Чтобы отредактировать объект охраны нужно:

1. Нажать на кнопку (редактировать) объект.

2. Внести изменения в объект.

3. Нажать кнопку «Сохранить» в окне объекта.

Чтобы закрыть окно объекта охраны без сохранения, нажать «Закрыть» в окне объекта охраны.

6.2.1.3 Удаление объекта

Чтобы удалить объект охраны нужно:

1. Нажать на кнопку (редактировать) объект охраны.

2. Нажать кнопку «Удалить» в окне объекта охраны.

6.2.2 Вкладка «Основная»

6.2.2.1 Добавление номера договора

В строке «Номер договора» указывается номер договора охраны, к которому требуется привязать созданный объект (рисунок 6.6).

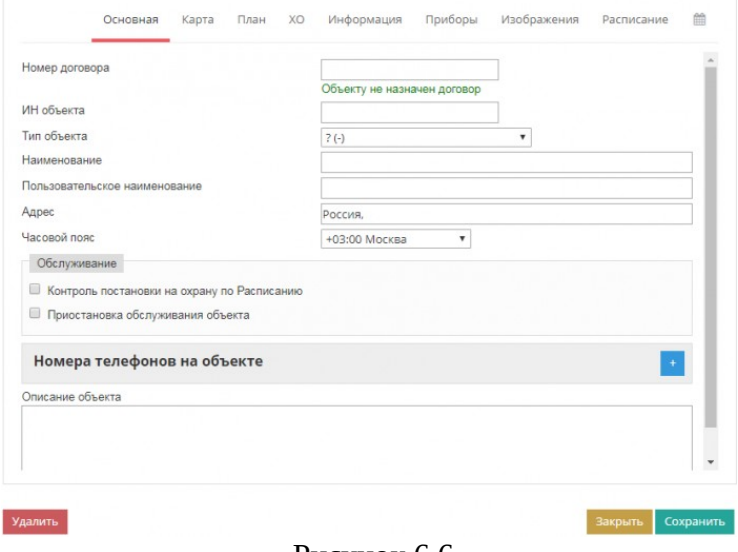


Рисунок 6.6

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.2.2 Выбор типа объекта и метки

Имеется возможность выбрать тип объекта (Школа, Банк, МХЛИГ и т.д.), а также метку объекта. Метки:

- Упрощают поиск подобных (имеющих один тип, местоположение, приоритетность и т.п.) объектов.
- Возможность выставлять расписание на подобных объектах, имеющих одинаковый график работы (подробнее в разделе Вкладка «Расписание»)
- Разделение объектов в учетных записях АРМа (подробнее в разделе Учетные записи)

6.2.2.3 Добавление адреса охраны

1. Кликнуть по строке «Адрес».

2. Заполнить поля в открывшемся окне «Адрес».

3. Нажать «Сохранить» (рисунок 6.7).

Поля координат - «Координаты. Широта/Долгота» - заполняются автоматически после ввода адреса. Также имеется возможность устанавливать координаты вручную (например при отсутствии точного адреса у охраняемого объекта). Для этого необходимо установить галочку «Установить координаты вручную», и ввести координаты. Они будут отображены на карте.

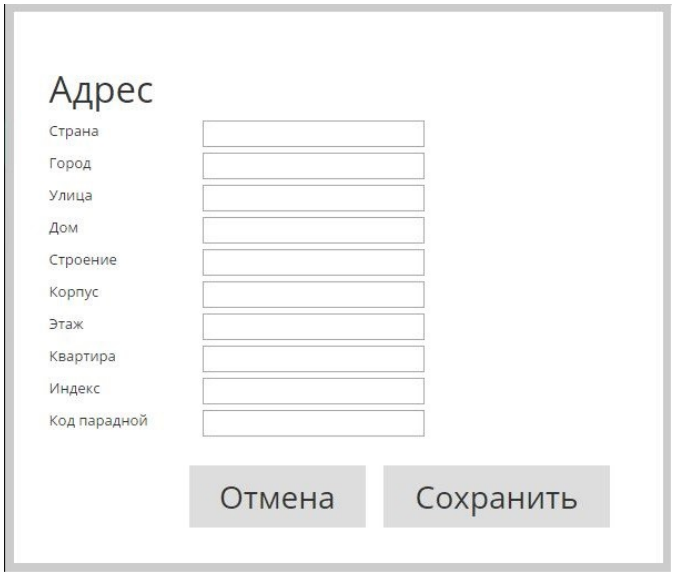


Рисунок 6.7 Меню добавления адреса

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.2.4 Обслуживание

1. Контроль постановки на охрану по расписанию:
   a) Если галочка установлена, то АРМ будет принимать тревожные извещения согласно расписанию охраны, установленному во вкладке "Расписание".
   b) Если галочка снята, то АРМ будет обрабатывать тревожные извещения в штатном режиме.
2. Постановка на прогон.
   a) Если установлена галочка, то в АРМ не будут приходить события от данного объекта.

6.2.2.5 Номера телефонов

В данном меню указываются номера телефонов для связи с объектом. Они также будут отображены в АРМ в поле информации по объекту (рисунок 5.8).

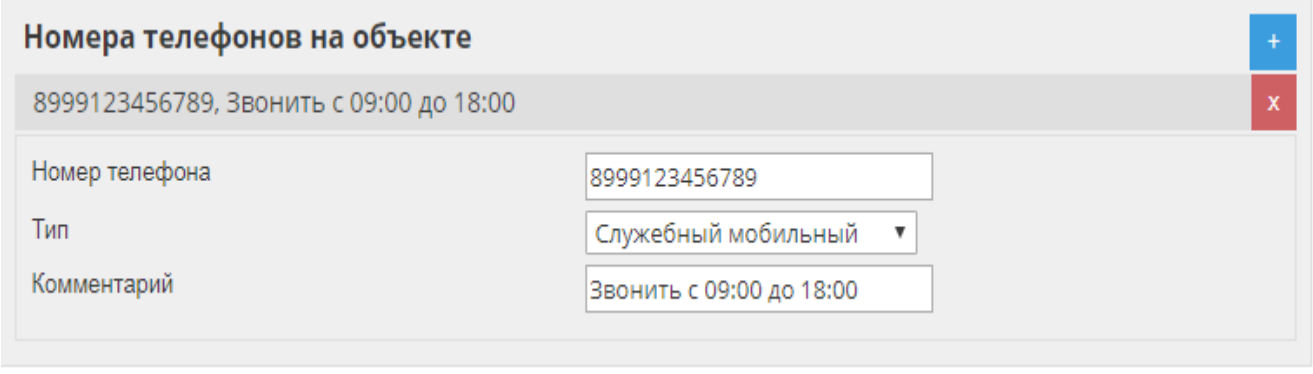


Рисунок 6.8 Номера телефонов

6.2.2.5 Описание объекта

В данном поле указывается описание объекта. Оно отображается в АРМ в поле информации по объекту.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.3 Вкладка «Карта»

Если адрес был указан во вкладке "Основная", то метка на карте устанавливается автоматически согласно указанному адресу. Однако может понабиться вручную выставить метку для уточнения расположения объекта, для этого:

1. Перейти на вкладку «Карта».

2. Переместить метку (указывает текущее положение объекта) в нужное место.

3. Нажать «Сохранить» (рисунок 6.9).

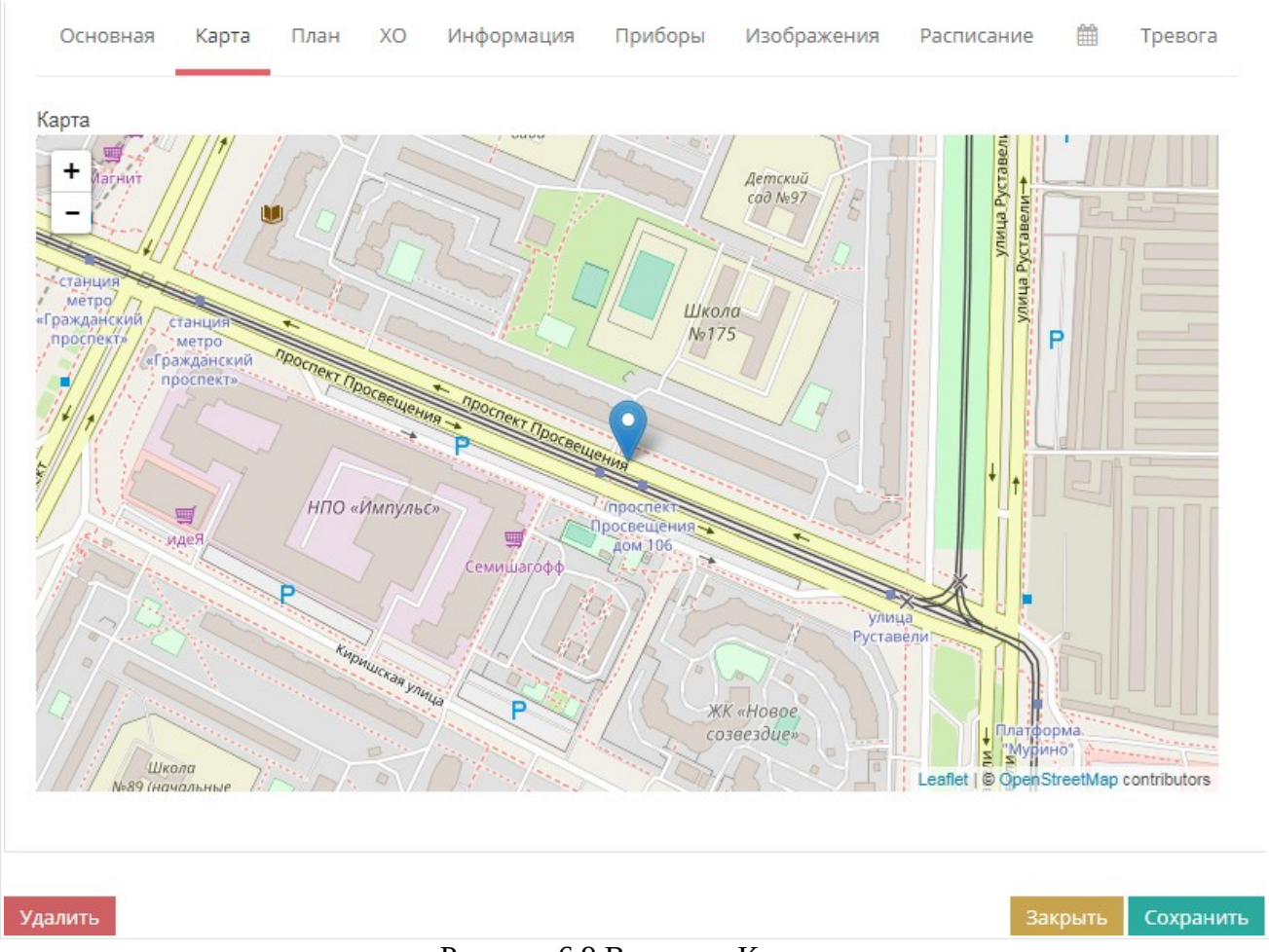


Рисунок 6.9 Вкладка «Карта»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.4 Вкладка «План»

Встроены:

1. редактор зон.
2. редактор плана.

Возможности:

- Привязать приборы к объекту (шлейфа привязанных приборов отобразятся в редакторе зон).
- Начертить план или загрузить изображение плана.
- Зайти в редактор зон.
- Перенести шлейфа на нужные места.
- Сохранить.

Рисунок 6.9.1 План объекта

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.5 Вкладка «ХО (хозорганы)»

В данной вкладке настраиваются и отображаются ответственные лица, которые относятся к выбранному объекту (рисунок 6.10).

Для добавления ответственного лица:

Нажать на +

1. Ввести данные ответственного лица.
2. Добавить порядковые номера ключей, введенные в приборе для данного отв.лица.
3. Записать уникальный Логин и Пароль для доступа в личный кабинет.
4. Сохранить.

Ответственным лицам, указанным в этой вкладке, необходимо указать номер мобильного телефона и логин/пароль, после чего они могут получить доступ к:

- Управлению личным кабинетом.
- Получению SMS-оповещений.
- Мобильному приложению "Тревожная кнопка".
- Мобильному устройству "Умка".

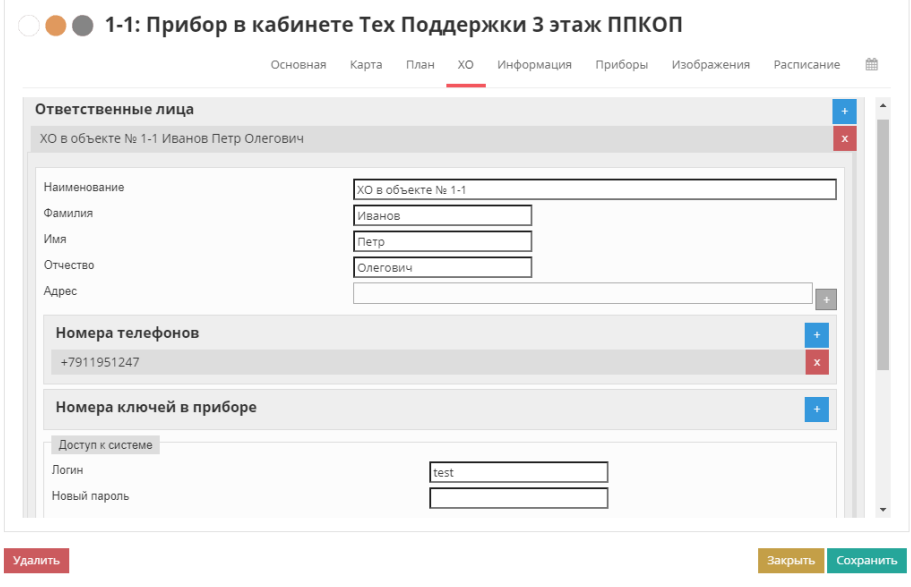


Рисунок 6.10 Вкладка "Хозорганы"

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.6 Вкладка «Информация»

В данной вкладке заполняются поля с информацией об объекте охраны (рисунок 6.11).

- Обслуживание:

  Здесь содержится информация по договору обслуживания.

- Категории объекта:

  Здесь можно указать категорию охраняемого объекта. Данная информация также будет отображена в АРМ в поле информации по объекту.

- Информация по объекту:

  Здесь можно указать дополнительную информацию по объекту, такую как:

  1. Отделение полиции
  2. Охраняемые помещения
  3. Расположение объекта
  4. Уязвимые места
  5. Пути подъезда
  6. Дислокация экипажа
  7. Вход в здание
  8. Примечания

Данная информация также будет отображена в АРМ в поле информации по объекту.

SEC.RU | Короткий путь к информации Скачано с sec.ru

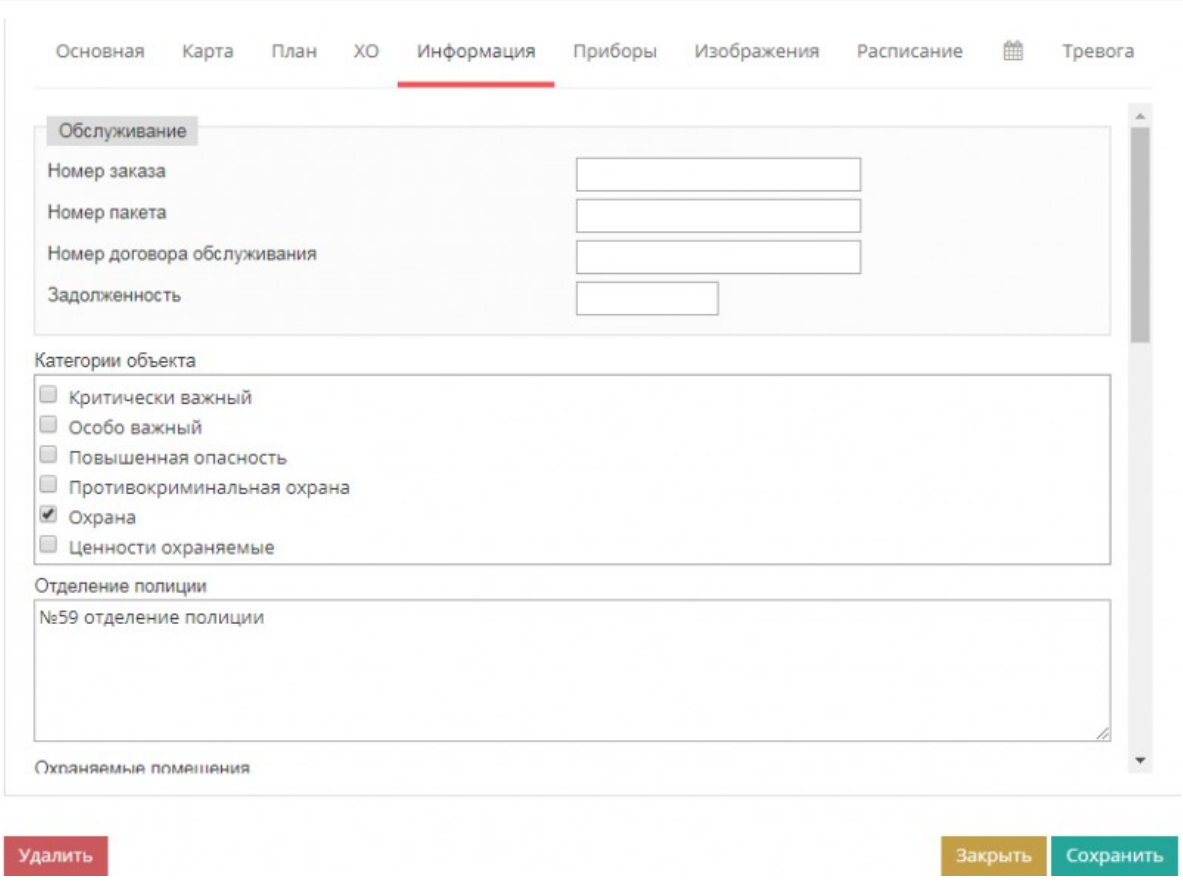


Рисунок 6.11 Вкладка "Информация"

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.7 Вкладка «Приборы»

Во вкладке «Приборы» (рисунок 6.12) отображаются доступные приборы и разделы приборов для подключения к данному объекту охраны. Для привязки прибора к объекту нужно поставить флаг у названия прибора.

Также здесь указан канал передачи данных и версия прошивки прибора.

Разделы приборов отображаются по принципу: <прибор>,<номер раздела>.

Для привязки раздела к объекту охраны, нужно поставить флаг у названия раздела прибора. Для каждого раздела можно установить задержку на выход и задать описание раздела.

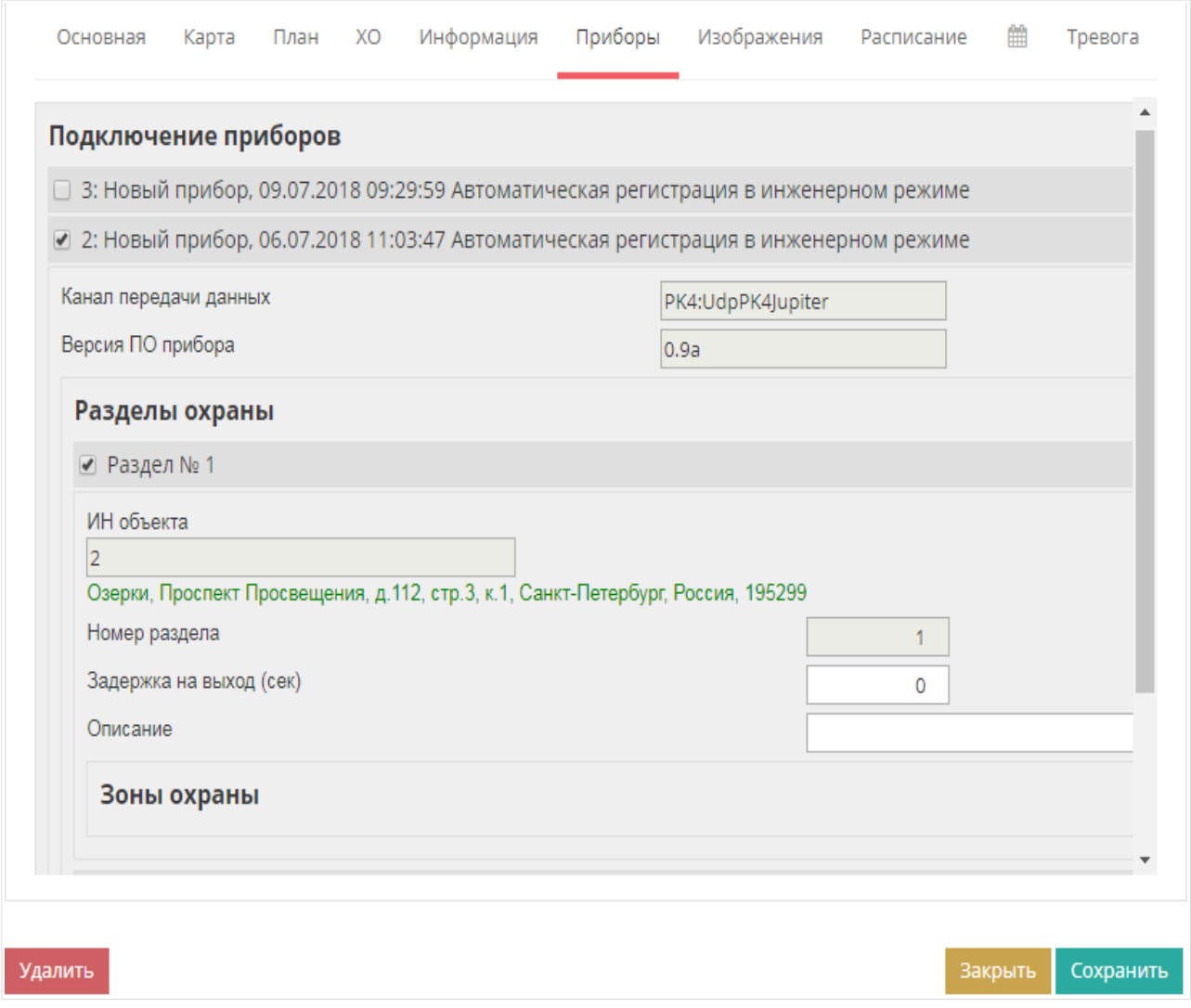


Рисунок 6.12 Вкладка «Приборы»»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.8 Вкладка «Изображения»

Во вкладке «Изображения» (рисунок 6.13) отображаются загруженные фотографии объекта охраны.

Для того чтобы добавить новое изображение необходимо:

1. Нажать на кнопку «Выберите файл».

2. Выбрать файл.

3. Ввести комментарий для изображения в поле «Комментарий».

4. Нажать на кнопку «Загрузить».

После загрузки изображение автоматически загрузится в данное окно.

Чтобы увидеть комментарий указанный при загрузке изображения, нужно навести курсор на изображение.

Для изменения комментария, нажмите на кнопку (редактирование комментария).

Для отображения изображения во весь размер, нажмите на кнопку (развернуть).

Для удаления изображения, нажмите на кнопку (удалить)

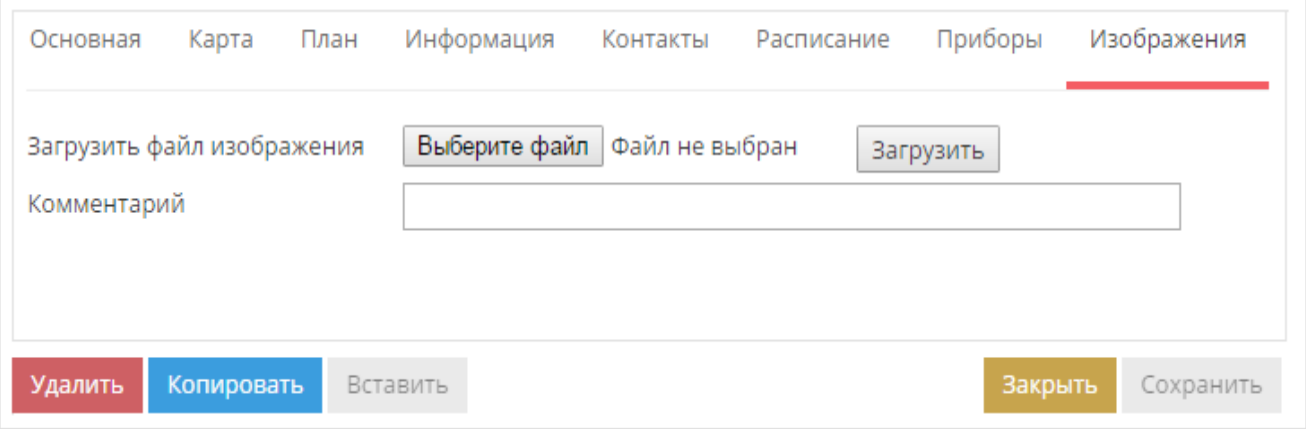


Рисунок 6.13 Вкладка «Изображения»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.9 Вкладка «Расписание»

Вкладка «Расписание» (рисунок 6.14) служит для гибкой настройки графика охраны. От этой настройки зависит логика обработки АРМ'ом тревожных извещений с охраняемых объектов.

«Метки» - Позволяют применить текущее расписание ко ВСЕМ объектам выбранной метки. Необходимо ввести название существующей метки и нажать на кнопку "Сохранить" и изменение применится

Рисунок 6.14 Вкладка "Расписание”

SEC.RU | Короткий путь к информации Скачано с sec.ru

Для изменения часов охраны определенного дня необходимо:

1. Кликнуть по одной из ячеек строки дня недели.

2. В открывшемся окне «График охраны (день) (рисунок 6.15)» по умолчанию заданы три периода охраны. Для добавления нового периода охраны нажать на кнопку (добавить).

3. Подтвердить добавление нового периода охраны.

4. Ввести время начала охраны. Окончанием одного периода считается начало следующего. Выбрать вид охраны и нажать «Сохранить».

Внимание!

Нельзя оставлять пустым окно расписания, извещения от приборов будут приходить некорректно. Всегда должен быть установлен хотя бы один период охраны на каждый из дней!

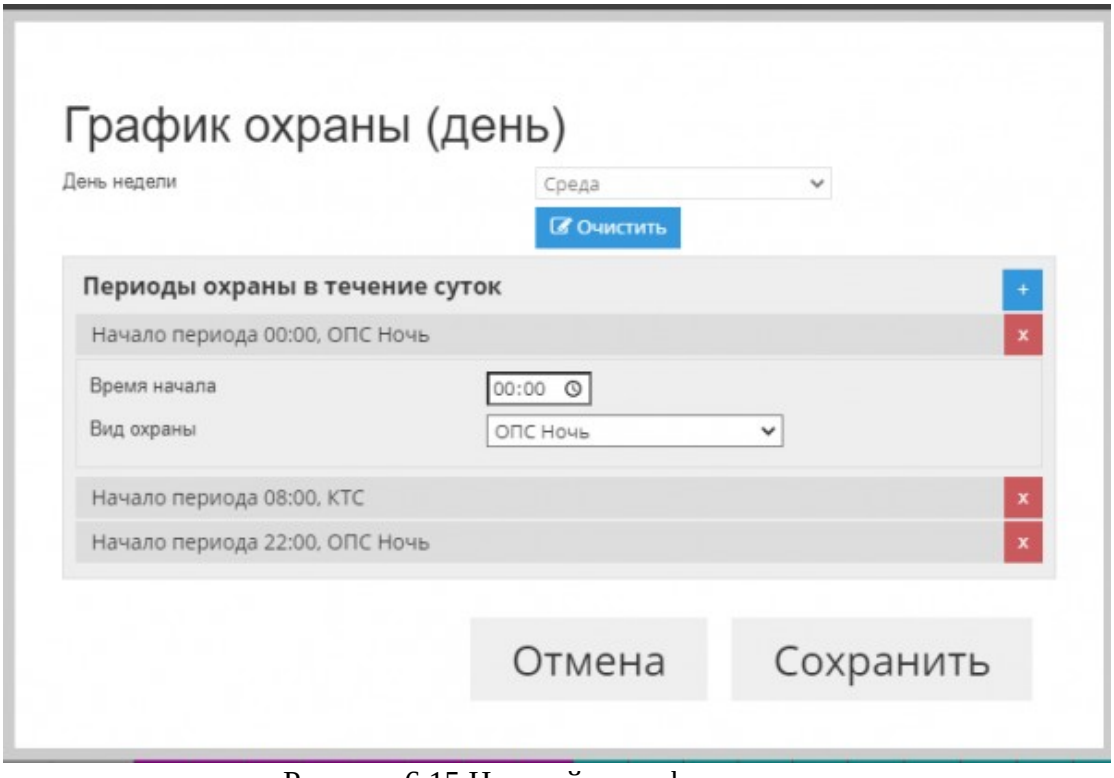


Рисунок 6.15 Настройка графика охраны

SEC.RU | Короткий путь к информации Скачано с sec.ru

Виды охраны:

- **КТС**— режим, во время которого тревожные сообщения будут обрабатываться без задержки.
- **ОПС День**— режим, во время которого тревожные сообщения будут задерживаться на время задаваемое параметром «Время на вход, день», по истечении времени будут формироваться сообщения о тревоге. Постановка на охрану будет выполняться с отсчетом времени на выход.
- **ОПС НОЧЬ** — режим, во время которого тревожные сообщения будут задерживаться на время задаваемое параметром «Время на вход, ночь», по истечении времени будут формироваться сообщения о тревоге. Постановка на охрану будет выполняться с отсчетом времени на выход.
- **ОПС БЕЗ СНЯТИЯ**— режим, во время которого тревожные сообщения будут обрабатываться без задержки, а постановка объекта на охрану проводится с отсчетом времени на выход.
- **КОМБИНИРОВАННЫЙ**— режим, во время которого реакция на сообщение о нарушении шлейфа будет задаваться оператором при постановке объекта на охрану, данный режим рекомендуется устанавливать на то время в течение которого нет точного определения режима охраны (смена режима, открытие объекта).

  При взятии объекта на охрану в режиме ОПС тревожные сообщения будут задерживаться на время задаваемое параметром «На вход, день».

  Для того чтобы удалить период охраны, нужно нажать на кнопку (удалить) в строке периода охраны.
- **«Уехали до:»**- установка данного флага переводит объект в режим "Без снятия", а также включает контроль расписания для объекта.

  С установленной галочкой любое снятие объекта с охраны до указанной даты будет генерировать тревожное сообщение "Снятие вне графика охраны".

  Данное поле рекомендуется использовать для отметки объектов с длительным отсутствием клиентов.

  Важный момент - в настройках охранной организации должна быть установлена галочка "Обрабатывать тревоги от снятых объектов", иначе тревога будет попадать только в протокол событий как информационное сообщение, но не создавать новую тревогу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

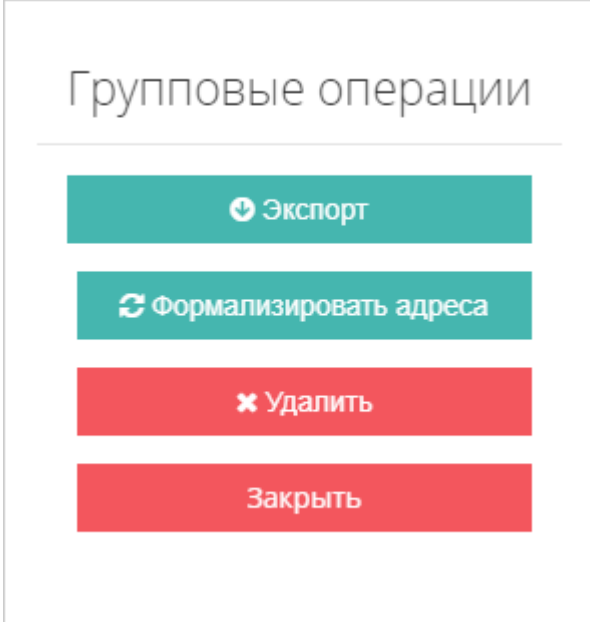
6.2.10 Групповые операции с объектами охраны

Для проведения групповых операций с объектами охраны необходимо:

1. Выбрать объекты охраны, с которыми должны быть выполнены операции поставив галочки.
2. Выбрать необходимую групповую операцию.

В групповых операциях доступны следующие действия:

1. Экспорт карточек объектов в xml-файл.
2. Формализировать адреса в карточках объектов, приведя их к общему виду.
3. Удалить объекты охраны.



SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3 Приборы

Вверху окна «Приборы» (меню «Клиенты» → «Приборы») (рисунок 6.16) отображается количество приборов, поле для поиска приборов и переключение режима отображения приборов.

К окну «Приборы» по-молчанию имеют доступ **Администратор и Инженер.**

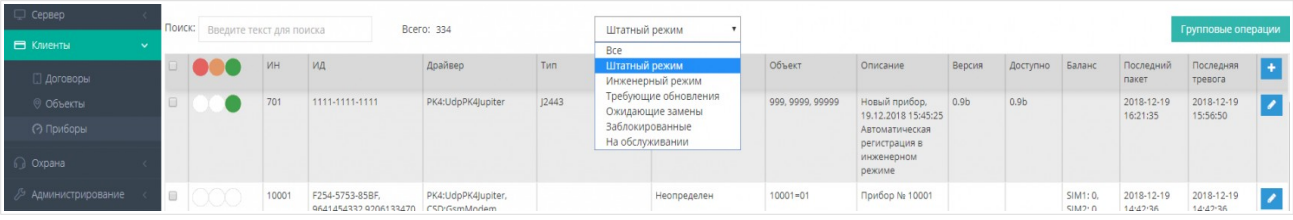


Рисунок 6.16 Окно «Приборы»

Режимы:

- **Все** - во время работы в данном режиме в таблице выводятся все приборы, независимо от их состояния и режима работы.
- **Штатный режим** - во время работы в данном режиме в таблице выводятся только те приборы, которые привязаны к объектам охраны. Данный режим создан для штатного режима работы.
- **Инженерный режим** - во время работы в данном режиме в таблице выводятся только те приборы, которые не связаны ни с одним из объектов охраны. Данный режим создан для тестирования/настройки прибора.

Примечание:
Прибор будет отображаться одновременно во вкладках "Инженерный режим" и "Штатный режим" при условии, что не все существующие разделы прибора привязаны к одному или нескольким объектам.
Как только каждый существующий раздел прибора будет привязан к одному или нескольким объектам, прибор пропадет из вкладки "Инженерный режим", и станет отображаться только во вкладке "Штатный режим".

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Требующие обновления** - во время работы в данном режиме в таблице выводятся только те приборы, для которых доступна новая версия прошивки.
- **Ожидающие замены** — во время работы в данном режиме в таблице выводятся только те приборы, для которых доступна подмена.
- **Заблокированные** - во время работы в данном режиме в таблице выводятся только те приборы, для которых установлен флаг " Блокировка работы прибора (запрет на подключение)"
- **На обслуживании**- во время работы в данном режиме в таблице выводятся только те приборы, для которых установлен флаг "Передача на сервисное обслуживание (приостановка)"

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.1 Добавление, редактирование и удаление нового прибора

6.3.1.1 Добавление нового прибора

Добавление нового прибора происходит в автоматическом режиме.

Для автоматического добавления прибора в список инженерных приборов необходимо зайти в конфигуратор и указать:

- IP/DNS адрес сервера.
- UDP порт сервера.
- Сбросить ключ шифрации по умолчанию.

После выполения этих действий прибор появится во вкладке Клиенты – Приборы.
Примечание: Если у вас в списке приборов-кандидатов на подключение находится больше определенного числа приборов или разделов (по умолчанию 100), то при попытке привязать прибор к объекту вы увидите следующее сообщение (рисунок 6.17):

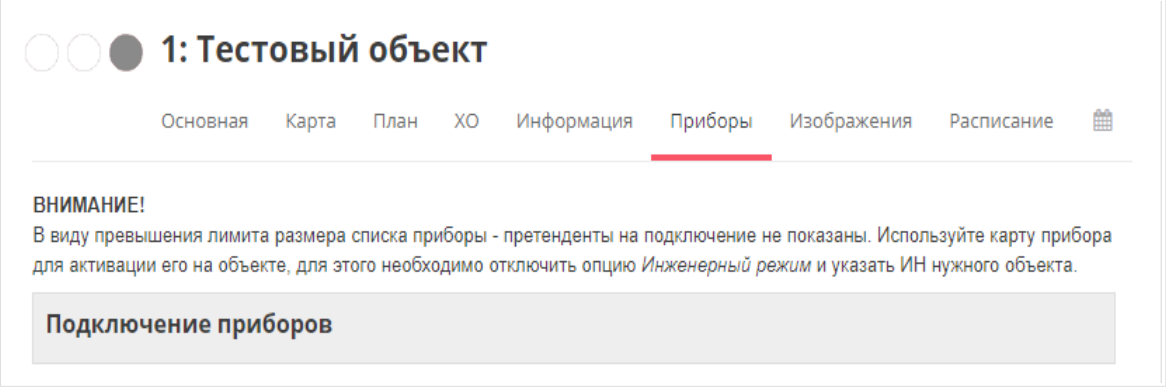


Рисунок 6.17 Окно подключения приборов

Тогда для привязки прибора требуется выполнить следующее:

1. Узнать идентификационный номер объекта, к которому вы хотите привязать прибор.
2. Перейти в карточку прибора, который требуется привязать.
3. Во вкладке "Основные" снять галочку с пункта "Инженерный режим".
4. У вас появится окно, в которое будет предложено внести идентификационный номер объекта, к которому вы хотите привязать прибор.
5. Вписать идентификационный номер объекта и нажать "ОК", прибор привяжется к объекту.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.1.2 Редактирование прибора

Для редактирования настроек прибора необходимо:

1. Нажать на кнопку "Редактировать прибор" (белый карандаш в синем квадрате).

2. Внести изменения в прибор.

3. Нажать кнопку «Сохранить» в окне «Прибор».

Чтобы закрыть окно прибора без сохранения, нажать «Закрыть» в окне «Прибор».

6.3.1.3 Удаление прибора

Чтобы удалить прибор нужно:

1. Нажать на кнопку "Редактировать прибор" (белый карандаш в синем квадрате).

2. Нажать кнопку «Удалить» в окне «Прибор» (нижний левый угол).

Внимание!

Если удалить прибор, предварительно не переведя все его разделы в инженерный режим (тем самым сбросив ключ шифрации на «по умолчанию»), то прибор больше не сможет подключиться к серверу. Для исправления ситуации необходимо будет подключиться к прибору по USB и вручную сбросить ключ шифрации на «по умолчанию».

6.3.2 Вкладка «Основные»

Во вкладке «Основные» (рисунок 6.18) необходимо заполнить краткое описание и информацию по произведенному монтажу прибора, для того чтобы в дальнейшем можно было его идентифицировать.

Обслуживание:

- Перевести прибор в инженерный режим (ключ шифрации сброситься на "по умолчанию" и прибор отвяжется от объекта).
- Блокировать смену ключа шифрования (при отвязывании прибора от одного объекта и привязывания его к другому объекту ключ шифрования остается прежним).

  При конвертации данных из Юпитер 7 в КРОС эта галочка установлена по умолчанию, что позволяет избежать сброса ключа шифрования.
- Отключить контроль неисправности каналов связи (если галочка установлена, то прибор не будет информировать сервер о потери связи по любому из каналов)

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Отключить контроль взлома корпуса (если галочка установлена, то прибор не будет информировать сервер, о вскрытии корпуса прибора).
- Поддержка безопасного взятия. При установленной галочке на прибор не будет приходить команды взятия\снятия, если любой шлейф прибора находится в тревоге\КЗ.
- Постановка на прогон (на сервер будут доходить пакеты данных, но АРМ не будет реагировать на изменения состояний прибора).
- Заблокировать работу прибора (сервер перестает принимать данные от прибора, прибор информирует пользователя об отсутствии связи с ПЦН).

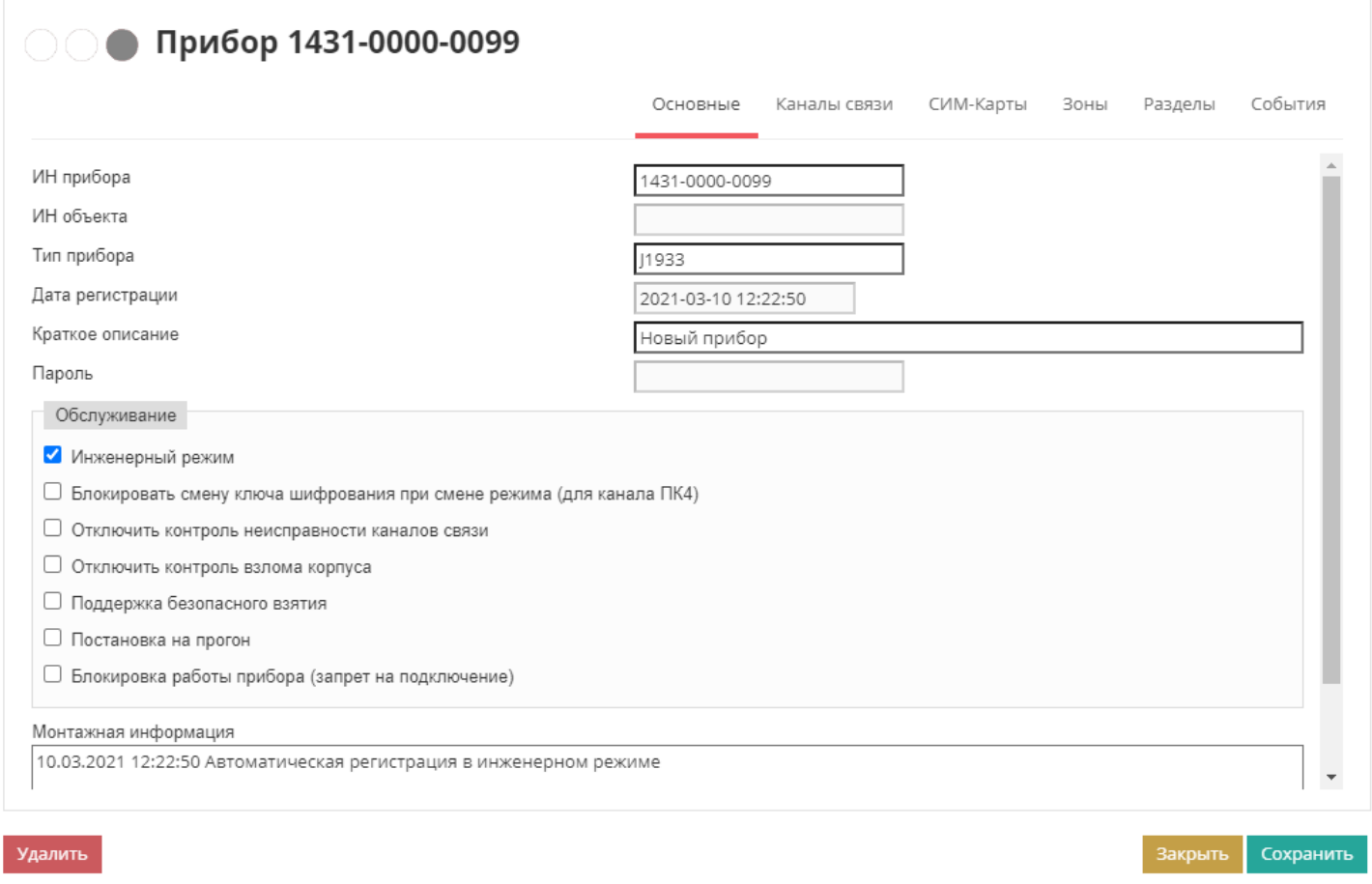


Рисунок 6.18 Вкладка «Основные»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.3 Вкладка «Каналы связи»

Каждый прибор должен иметь хотя бы один канал передачи данных. Один прибор может иметь несколько каналов передачи данных разных типов.

Все вновь подключаемые к КРОС приборы будут автоматически регистрироваться в т.н. “песочнице” в Инженерном режиме (если это разрешено в блоке параметров Охранной Организации). При этом для прибора автоматически будет создан канал передачи данных, связанный с драйвером, с помощью которого прибор соединился с сервером. Для созданного канала будут заполнены необходимые параметры, такие как идентификационные данные прибора, определяемые типом канала (например для ПК4 - это ID6 + SN6, для SurGard это OID, итд), номер порта, по которому прибор может быть отнесен к определенной охранной организации, итд.

Кроме того каналы передачи данных автоматически создаются для некоторых трансляций, например при создании трансляций SurGard и EPPS. Это необходимо для определенной идентификации прибора определяемой типом протокола. Например трансляция SurGard использует в исходящих пакетах параметр OID канала CID (ContactID) прибора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

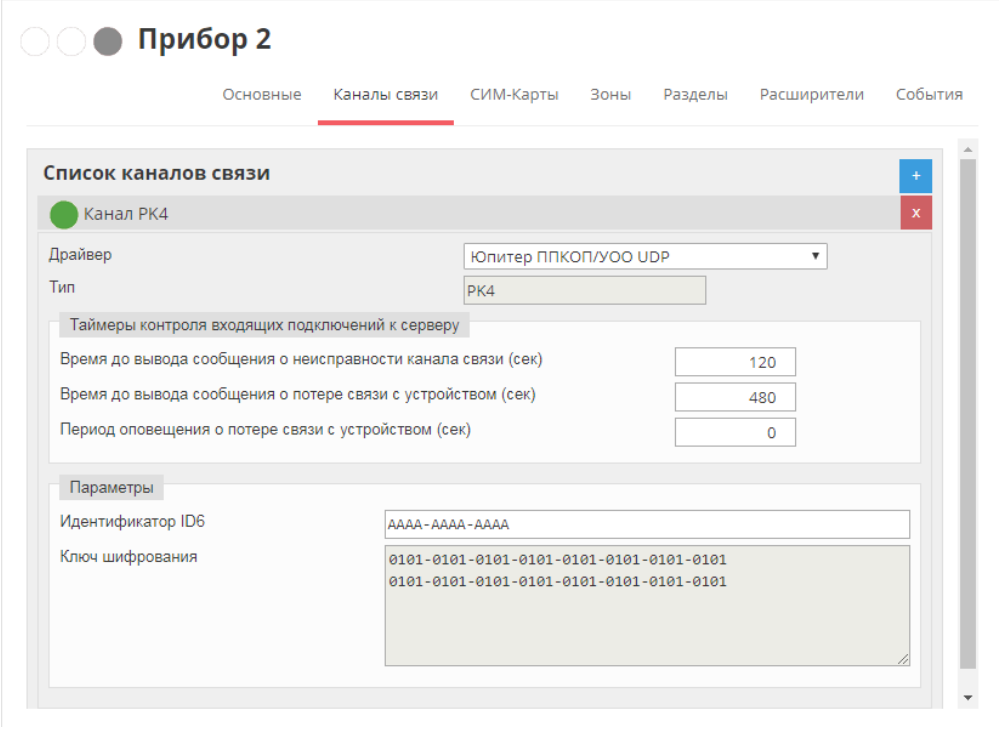


Рисунок 6.19 Вкладка «Каналы связи»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.3.1 Общие параметры для всех каналов

- **Драйвер**

Выбор драйвера для трансляции из списка доступных драйверов передатчиков. В зависимости от выбранного драйвера будет установлено содержимое блока Параметры.

- **Тип**

Тип канала передачи данных. Устанавливается автоматически, в зависимости от выбранного драйвера. Возможные значения типа:

  - PK4 - Транспортный протокол ПК4.
  - CID - Прием данных по протоколу SurGard..
  - CSD - Прием CSD сообщений или дозвон без соединения
  - EPPS - Протокол ЕППС.

- **Таймеры контроля входящих подключений к серверу**

Величины для контроля состояния канала связи прибора соответствующего каналу передачи данных.

- **Время до вывода сообщения о неисправности канала связи (сек)**

Если время, прошедшее с момента получения последнего пакета или соединения от прибора по текущему каналу передачи данных превышает установленную здесь величину, то состояние неисправности канала связи устанавливается в Неисправно .

- **Время до вывода сообщения о потере связи с устройством (сек)**

Период, по истечение которого с момента получения последнего пакета или соединения от прибора будет сформировано сообщение о потере связи с прибором.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Период оповещения о потере связи с устройством (сек)**

Если значение этого параметра отлично от нуля, то сообщение о потере связи с прибором будет формироваться в системе периодически, с указанным здесьинтервалом в секундах.

6.3.3.2 Индивидуальные параметры для канала PK4

- **Идентификатор ID6**

6-байтный основной идентификатор прибора в протоколе ПК4. Может быть изменен.

ВНИМАНИЕ! Изменения параметров канала сохраняются в только базе данных. Чтобы изменить параметры в приборе используйте Конфигуратор.

- **Ключ шифрования**

Текущий 32-байтный ключ шифрования ПК4. Поле только для чтения. По умолчанию устанавливается значение по умолчанию : 01, 01, 01 … 01. Новый ключ генерируется автоматически, при закреплении прибора за объектом и выходе из инженерного режима. Ключ автоматически сбрасывается на значение по умолчанию при переводе прибора в инженерный режим.

6.3.3.2 Индивидуальные параметры для канала EPPS

- **Таблица перекодировки**

Индивидуальная таблица перекодировки, используемая для нормализации входящих сообщений. По умолчанию используется Базовая таблица.

6.3.3.3 Индивидуальные параметры для канала CID

- **Идентификатор Contact ID**

OID прибора - основной идентификатор пакета протокола SurGard.

- **Порт**

Порт, по которому принимаются пакеты протокола SurGard. Служит для идентификации Охранной Организации, для которой предназначен пакет.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **IMEI**

IMEI прибора - основной идентификатор пакета протокола SurGard V4.

- **Таблица перекодировки**

Индивидуальная таблица перекодировки, используемая для преобразования входящих SurGard сообщений во внутренний формат КРОС. По умолчанию используется Базовая таблица.

6.3.3.4 Индивидуальные параметры для канала CSD

- **Код удаленного управления**

Код, устанавливаемый в конфигурации прибора, для управления посредством СМС. В настоящее время не используется.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.4 Вкладка «Номера телефонов»

Во вкладке «Сим-карты» (рисунок 6.20) выводится список телефонов, которые используются для каналов связи.

- Чтобы добавить новый телефонный номер, нужно нажать на кнопку "добавить", заполнить поля «Номер телефона», «Номер СИМ-карты» и поставить флаг «Активный номер», если данный номер используется в данный момент.
- Чтобы удалить телефонный номер, нужно нажать на кнопку "удалить" (белый крест в красном квадрате).

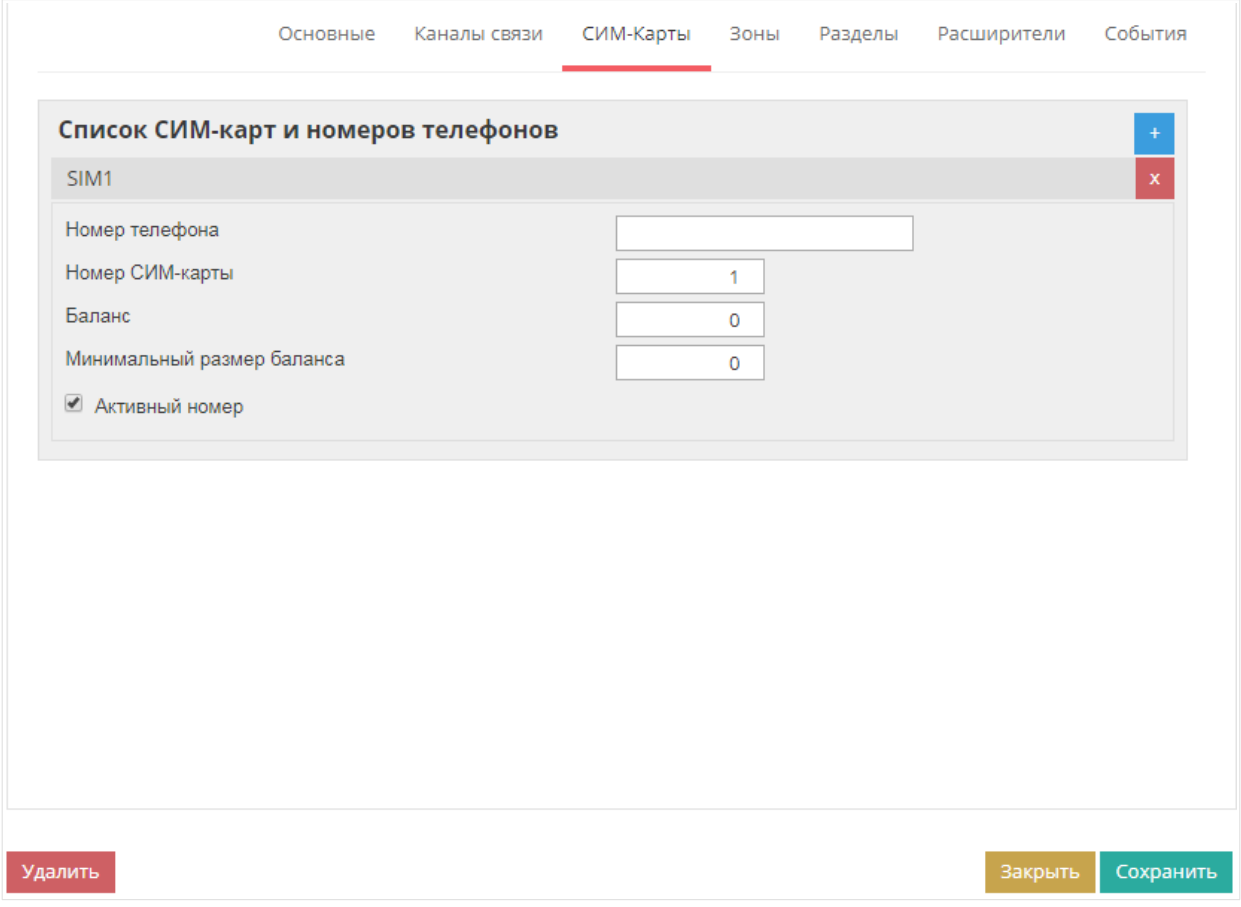


Рисунок 6.20 Вкладка «Сим-карты»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.5 Вкладка «Зоны охраны»

Во вкладку «Зоны охраны» (рисунок 6.21) выводится список зон охраны.

Добавлять новые или редактировать уже существующие зоны из данного меню нельзя, это должно быть сделано из программы-конфигуратора. В данном меню можно установить только описание раздела, а также задержку на выход.

Также можно заблокировать зону (поставить на прогон).

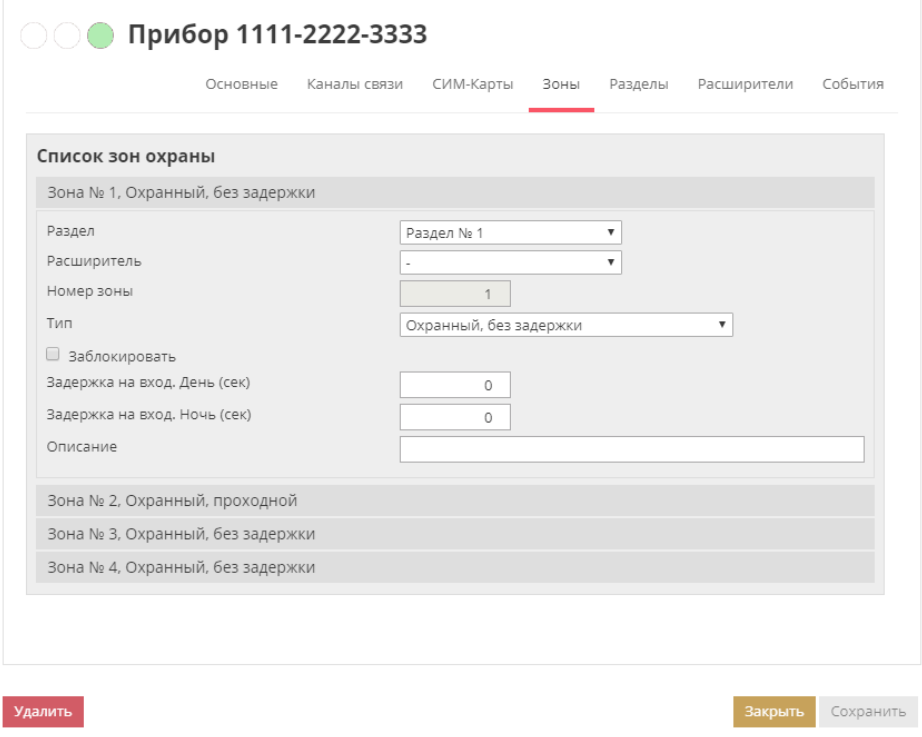


Рисунок 6.21 Вкладка «Зоны охраны»

От типа зоны охраны зависит наличие дополнительных полей для ввода задержки на вход и выход.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.6 Вкладка «Разделы»

Во вкладку «Разделы» (рисунок 6.22) выводится список разделов охраны, текущее состояние раздела (взят\снят\в тревоге), а также ИН объекта, к которому подключен данный раздел охраны.

Добавлять новые или редактировать уже существующие разделы из данного меню нельзя, это должно быть сделано из:

- Программы конфигуратора на приборе
- Онлайн конфигуратора

В данном меню можно установить только описание раздела.

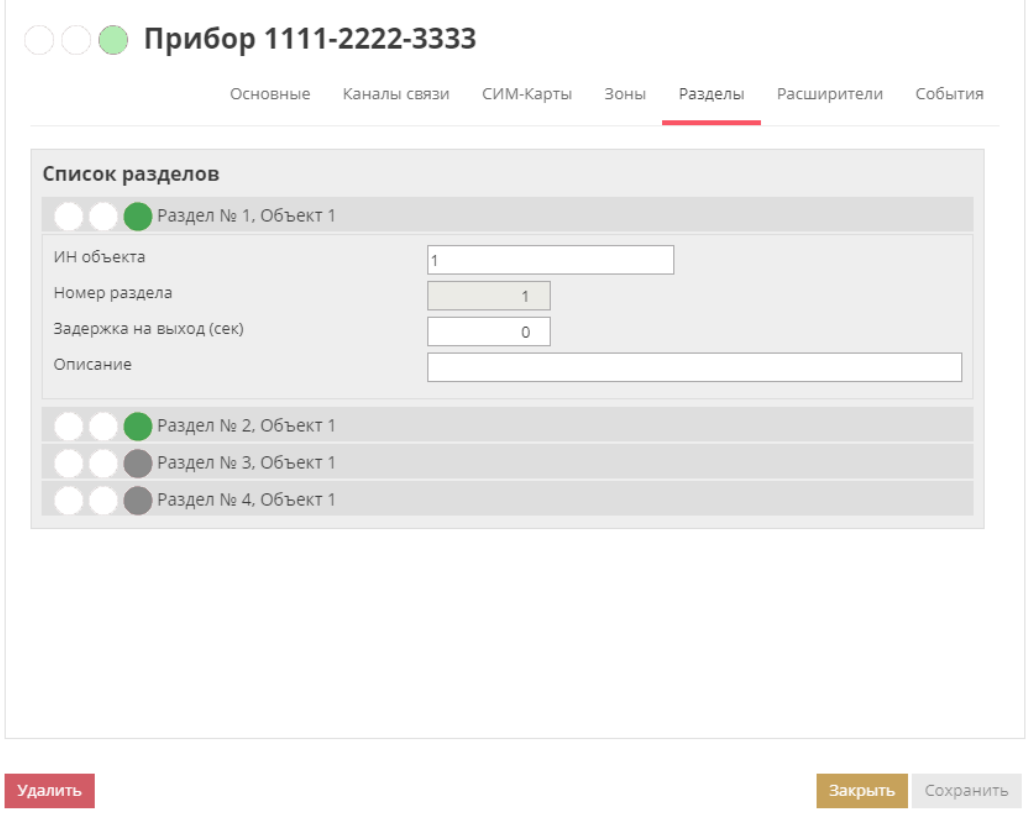


Рисунок 6.22 Вкладка «Разделы»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.7 Вкладка «Расширители»

В данном меню отображается список подключенных к прибору расширителей.
Здесь можно добавить краткое описание и пользовательское наименование, а также посмотреть список зон охраны данного расширителя (рисунок 6.23).
Конфигурировать зоны расширителя в этом меню нельзя, это должно быть сделано из программы конфигуратора.

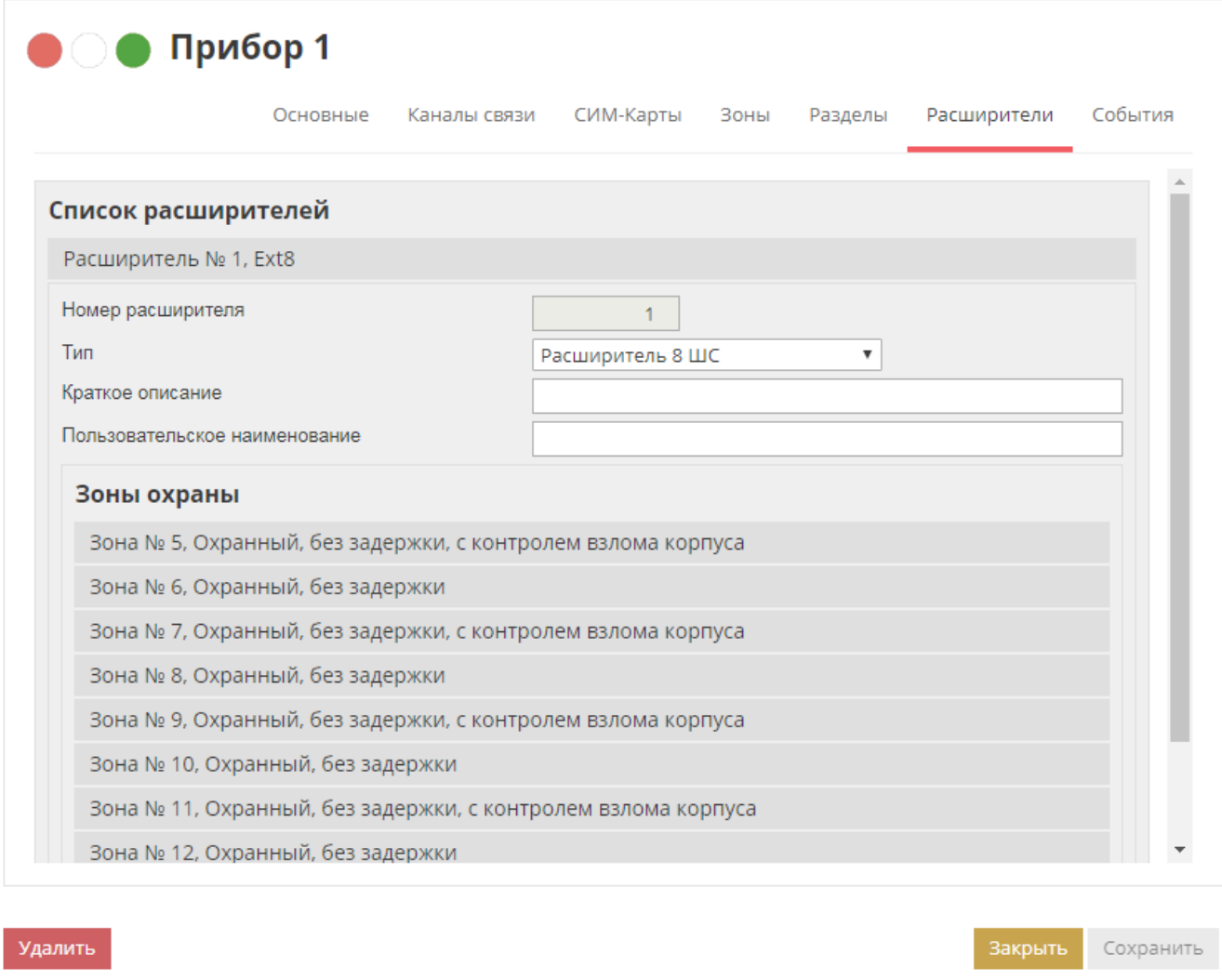


Рисунок 6.23 Вкладка «Расширители»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.8 Вкладка «События»

Во вкладке «События» (рисунок 6.24) выводятся кнопки базовых команд для прибора и поле для ввода команд.

Команды:

Выполнить — возможность отправки на прибор команды, введенной в поле «Команда», например, для конфигурации или перезагрузки прибора удаленно

Взять — взятие всех разделов прибора под охрану.

Снять — снятие всех разделов прибора с охраны

Конфигуратор - запуск удаленного конфигуратора приборов.

Конфигуратор поддерживает асинхронную загрузку данных. До первого запуска конфигуратора кнопка будет гореть красным. Это означает, что при нажатии на кнопку будет загружена полная конфигурация прибора,

и сохранена в базу данных. После первой загрузки, кнопка сменит цвет на синий. Каждый последующий раз конфигуратор будет загружаться гораздо быстрее, так как информация будет браться из базы данных.

Руководство по эксплуатации конфигуратора доступно по ссылке: Конфигуратор

По умолчанию отображение и функционал кнопок "Взять", "Снять", "Выполнить", "Конфигуратор" отключено. Для включения отображения и функционала данных кнопок необходимо:

1. Зайти на сервер под учетной записью "Администратор сервера" (superadmin-логин и пароль по умолчанию).

2. Перейти во вкладку Администрирование--->Безопасность--->Роли.

3. Открыть на редактирование необходимую роль (например Администратор), и поставить галочку в пункте "Клиенты: Разрешение взятия/снятия" и галочку в пункте "Клиенты: Отправка команд на прибор через АПИ".

4. У всех пользователей с ролью "Администратор" появится возможность брать и снимать приборы с охраны, заходить в удаленный конфигуратор и выполнять команды на приборе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Конфигурация — получение от прибора его текущей конфигурации

Состояние — получение текущего состояния разделов прибора

По умолчанию кнопки "Конфигурация" и "Состояние" доступны только если прибор заведен на сервер напрямую. Если, например, используется зеркалирование, то на "принимающем" сервере эти кнопки будут отсутствовать.

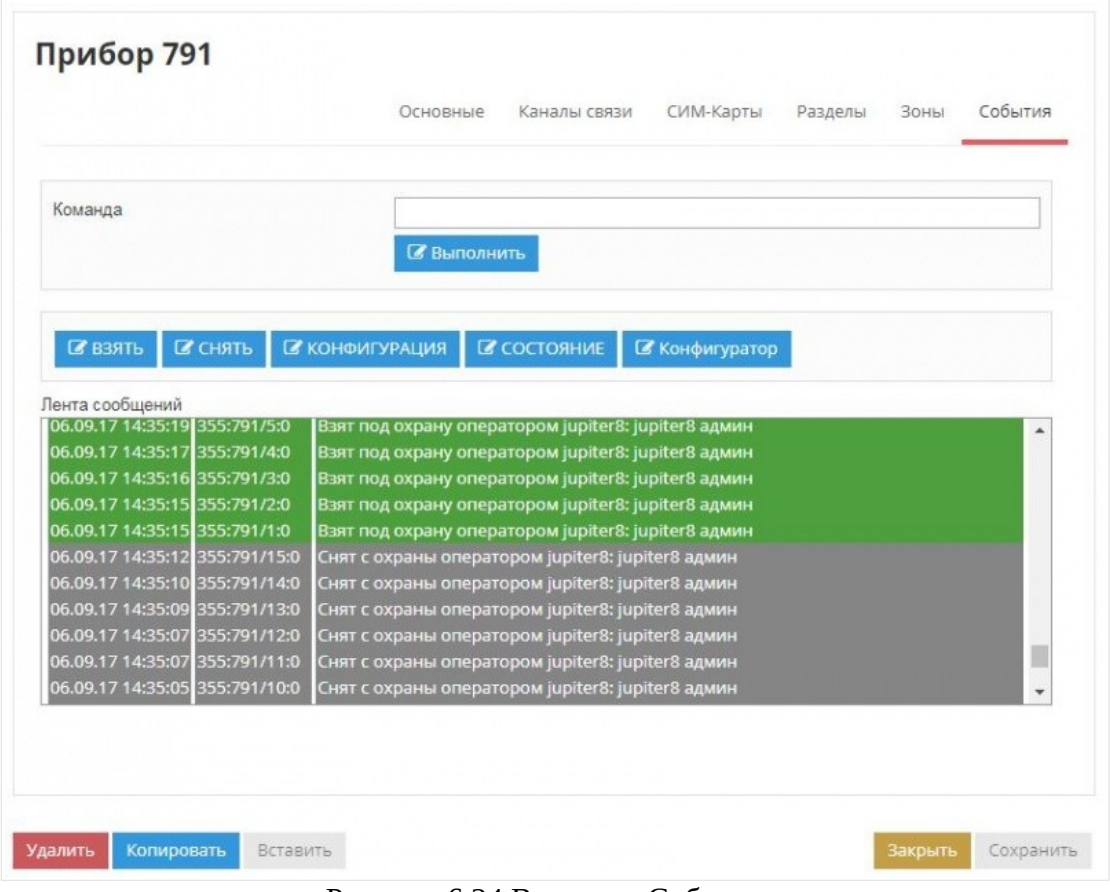


Рисунок 6.24 Вкладка «События»

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.9 Групповые операции с приборами охраны

Для проведения групповых операций с приборами охраны необходимо:

Выбрать приборы охраны, с которыми должны быть выполнены операции поставив галочки.

Выбрать необходимую групповую операцию.

В групповых операциях доступны следующие действия:

1. Блокировать смену ключа шифрования при смене режима (Для канала ПК4)
2. Отключить контроль неисправности канала.
3. Отключить контроль взлома корпуса.
4. Поддержка безопасного взятия.
5. Постановка на прогон.
6. Блокировка работы прибора (запрет на подключение).

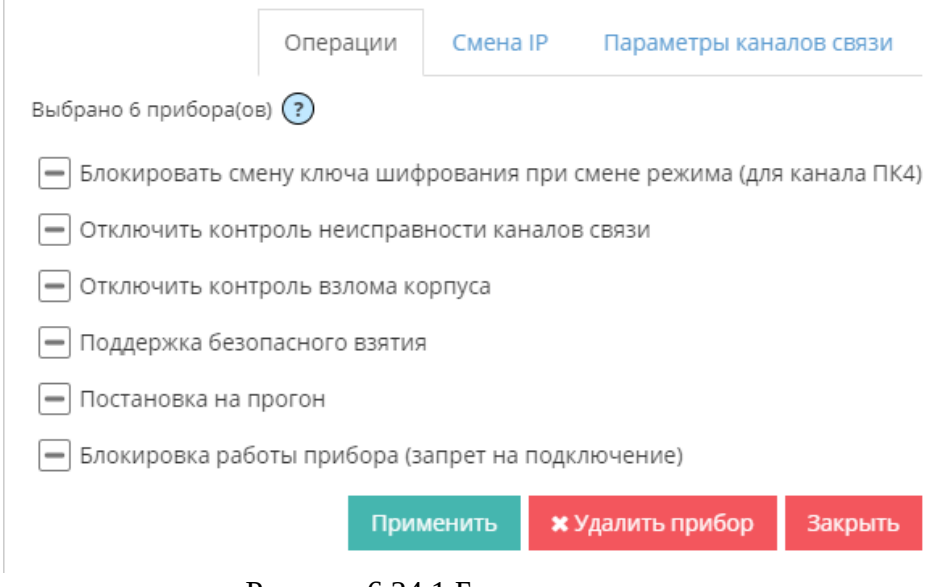


Рисунок 6.24.1 Безопасное взятие

SEC.RU | Короткий путь к информации Скачано с sec.ru

Смена IP-адресов для подключения приборов (рисунок 6.24.2). Прибор должен быть в снятом состоянии, чтобы принимать команды на изменение ip-адресов для подключения.

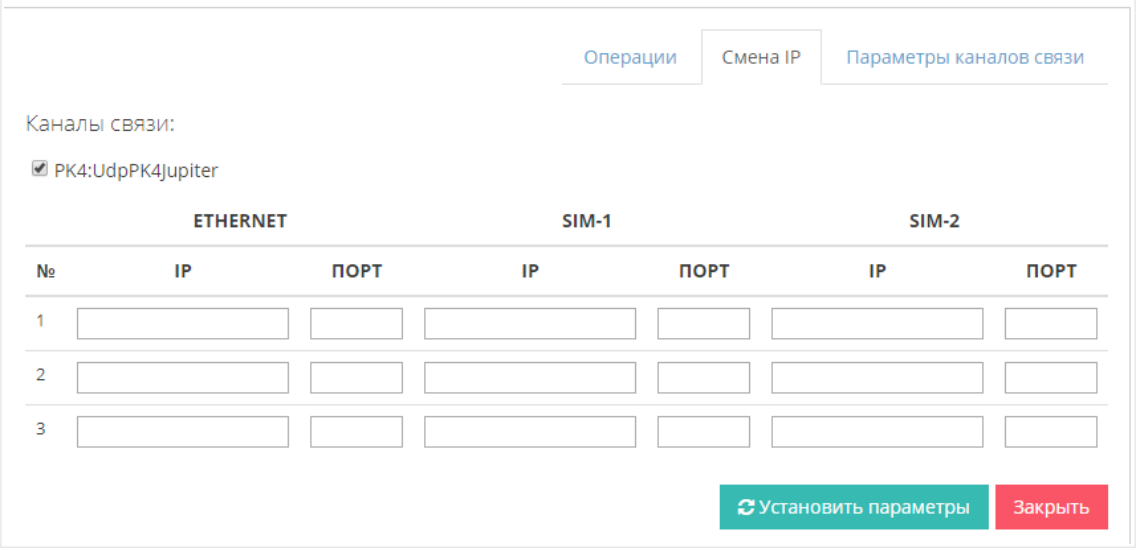


Рисунок 6.24.2 Сменя ip-адресов

Изменение параметров каналов связи (оповещения о потере связи с приборами)(рисунок 6.24.3).

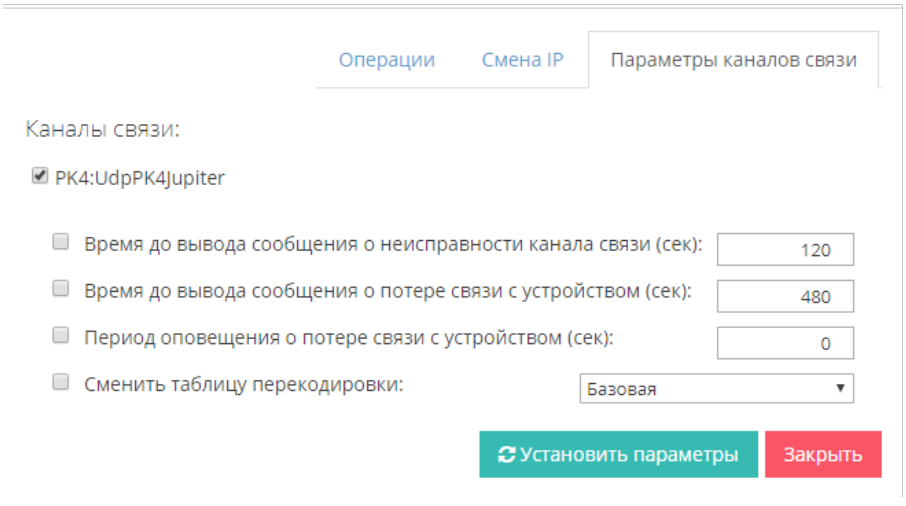


Рисунок 6.24.3 Параметры каналов связи

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.3.10 Удаленное обновление прошивки

Можно обновить только приборы не находящиеся под охраной.

Для удаленного обновления прошивки требуется:

1. Перейти во вкладку Клиенты-Приборы

2. С помощью фильтра выбрать приборы, у которых возможно обновление прошивки (Фильтр - требующие обновления)

Будет выведен список приборов (рисунок 6.3.10), в котором:

- Зеленый - прошивка загружается
- Синий - прошивка загружена на 100%
- Красный - ошибка обновления (прибор не на связи или ошибка при обновлении)

		792	2443-2443-2443,	PK4:UdpPK4Jupiter, CID:TcpSurgardDecID	УОО 4 IP/GPRS (2443)	GPRS SIM1	522	УОО	0.8a	0.8c	SIM1: 0p	05.03.2018 09:58:40	26.02.2018 16:59:24	
		5453	1933-1933-1991	PK4:UdpPK4Jupiter	ППКОП 16 IP/GPRS (1933)	Ethernet	896	ППКОП стенд (левый прибор)	2.0b	2.0c	SIM2: 0p, SIM1: 0p	05.03.2018 09:58:30	28.02.2018 18:06:44	
		5495	2222-1933-1937	PK4:UdpPK4Jupiter	ППКОП 16 IP/GPRS (1933)	Ethernet		Новый прибор, 19.02.2018 10:59:30 Автоматическая регистрация в инженерном режиме	2.0e	2.0c		19.02.2018 15:02:27	19.02.2018 10:59:30	

Рисунок 6.3.10 Удаленное обновление прибора

3. Выбрать прибор и далее нажать на Обновить прошивку в Групповых операциях. В ленте прибора появляется сообщение от прибора:

Например, для УОО:

"UOO " HM10 0

Это означает, что процесс загрузки начался, скачено 0%

Если отправить команду hp, то в ответ придет процесс загрузки ПО.

4. После загрузки обновления прибор самостоятельно перезагрузится и будет работать в штатном режиме.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.4 Подмена прибора

Система имитостойкости СПИ «Юпитер» построена на передаче в каждом пакете протокола ПК4 серийного номера устройства. Серийный номер уникален для каждого экземпляра устройства и не может быть изменен пользователем.

Идентификатор устройства добавляется в конфигурацию при выполнении процедуры регистрации устройства.

Для корректного осуществления процедуры "Подмены прибора" необходимо:

В конфигураторе нового прибора указать идентификатор идентичный текущему заменяемому прибору (идентификаторы должны быть одинаковые).

Для корректной подмены оба прибора должны находиться в снятом состоянии.

1. Настроить новый прибор и подключить к серверу, он появится во вкладке Клиенты-Приборы выделенный красным цветом (рисунок 6.25).

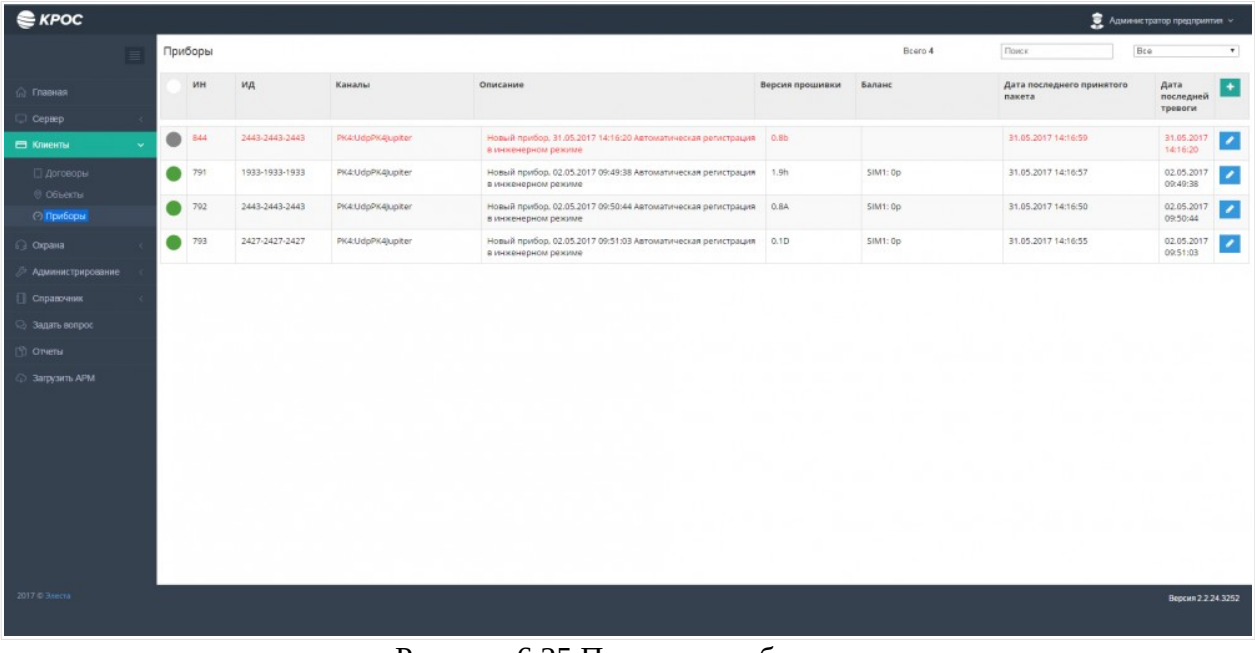


Рисунок 6.25 Подмена прибора

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Нажать "редактирование прибора", откроется окно представленное ниже (рисунок 6.26).

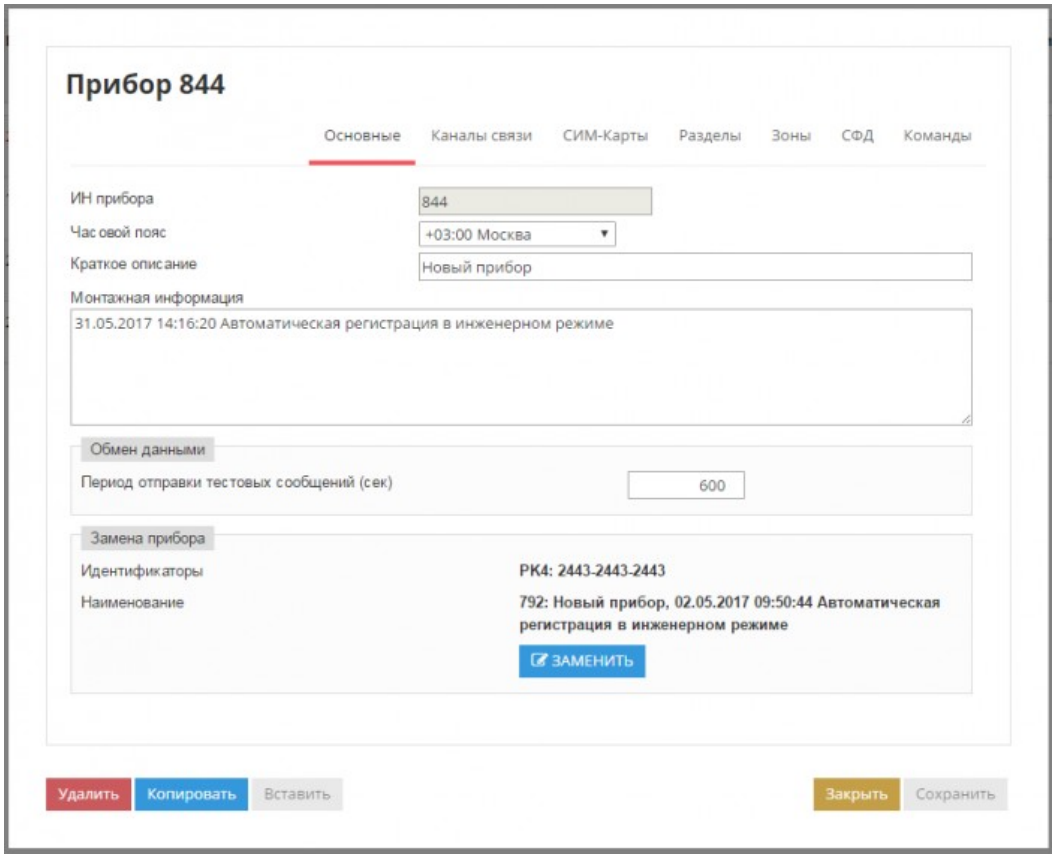


Рисунок 6.26 Окно подмены прибора

3. В окне "Замена прибора" выводятся данные прибора, который необходимо заменить на новый (рисунок 6.27).

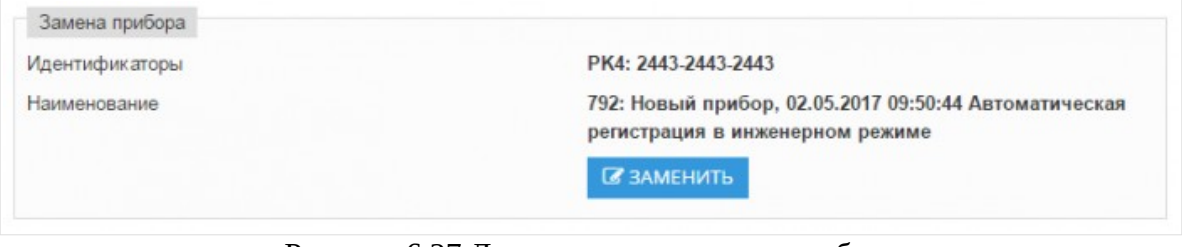


Рисунок 6.27 Данные подменяемого прибора

4. Нажать "Заменить", вследствии чего начинает работать новый прибор.
5. Сохранить.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.5 Пошаговая инструкция по подключению прибора к серверу-КРОС

В данном пункте пошагово рассматривается процесс заведения прибора на сервер КРОС. Предполагается, что установка сервера прошла корректно, все настройки установлены «по умолчанию» и сервер КРОС полностью готов к работе.

6.5.1 Настройка портов

Сервер принимает данные от приборов по протоколу UDP, ожидая соединения на портах, задаваемых в настройках.
По умолчанию после установки сервера для приборов выделены порты 10093-10095, но, вероятнее всего, возникнет необходимость поменять эти порты.
Для установки необходимых вам портов требуется:

1. Определить какой порт вы хотите использовать для соединения приборов с сервером.

   Это могут быть любые порты в диапазоне 10000-19999.

2. После определения порта необходимо сделать проброс выбранного вами порта на вашем маршрутизаторе, а также добавить выбранный порт в исключения антивируса или сетевого экрана, чтобы они не блокировали входящие от прибора пакеты.

3. Войти в систему администрирования КРОС.

4. Ввести в адресной строке браузера адрес вашего сервера КРОС, например:

   http://localhost:9900

   или

   http://192.168.1.13:9900

   192.168.1.13 - IP компьютера, на котором установлен сервер.

5. Появится приглашение ввести логин и пароль пользователя. Требуется зайти как **Администратор сервера**. Использовать установленные по умолчанию:

   Логин: superadmin

   Пароль: superadmin

SEC.RU | Короткий путь к информации Скачано с sec.ru

6. Зайти в меню Охрана ---> Реквизиты. Далее выбрать охранную организацию, зайти в Параметры (рисунок 5.28).
7. Под номером 5 на картинке ниже располагается поле, в которое нужно ввести выбранный вами порт или диапазон портов, после чего нажать кнопку "Сохранить"(рисунок 6.29).

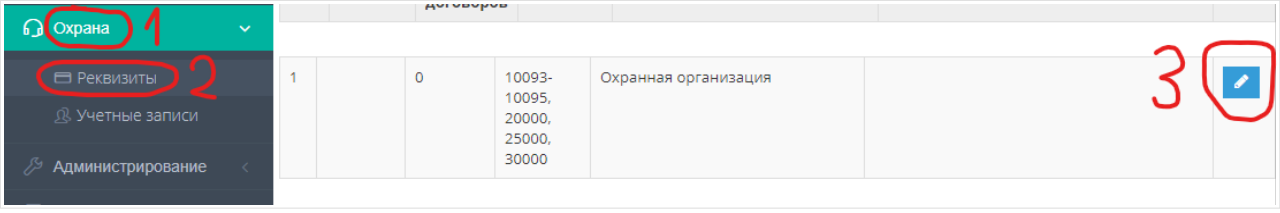


Рисунок 6.28 Выбор охранной организации для редактирования

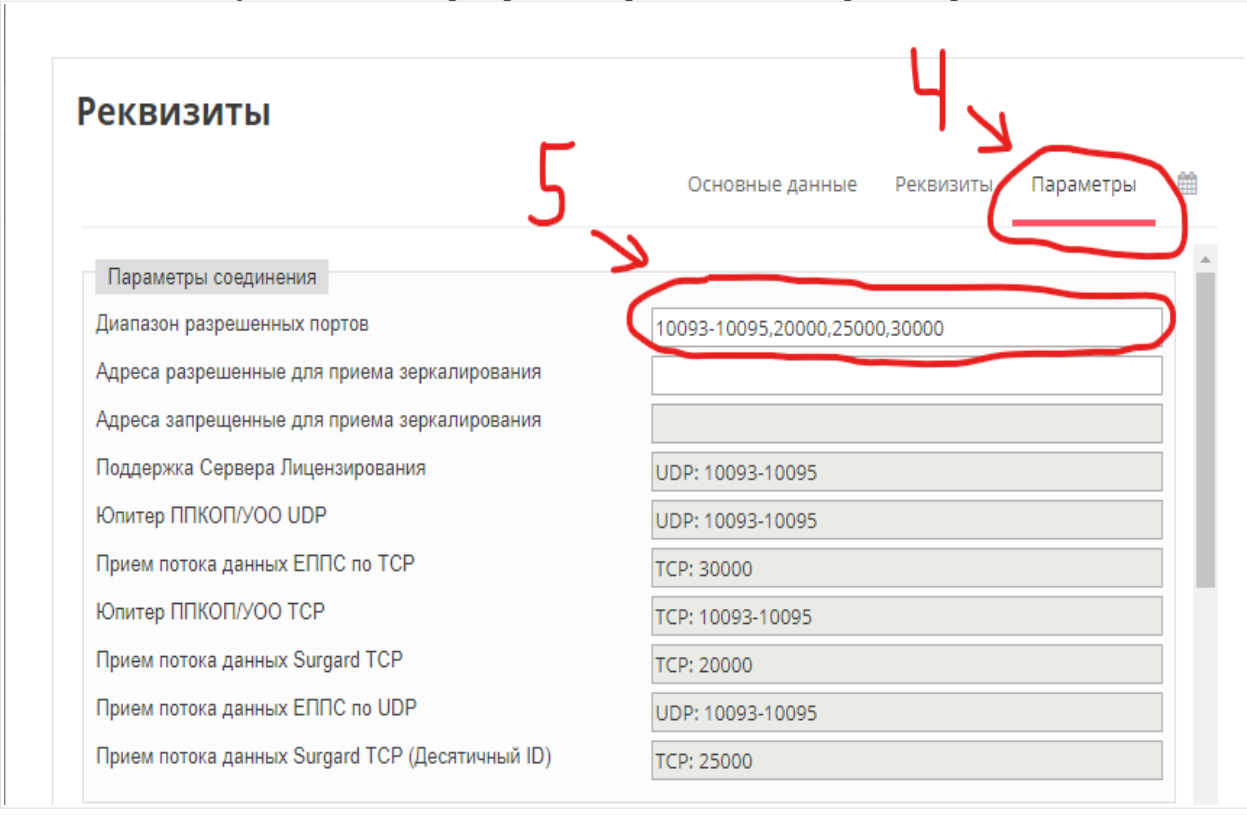


Рисунок 6.29 Редактирование данных для охранной огранизации

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.5.2 Добавление договора

На охрану объекта или нескольких объектов заключается договор охраны. Под договором охраны подразумеваются договор с физическими или юридическими лицами, подключенными на пульт централизованного наблюдения.
Для добавления договора необходимо:

1. Войти в систему администрирования КРОС под учетной записью **администратора охранного предприятия**.

Установленные по умолчанию:

Логин: admin

Пароль: admin

2.Зайти в меню Клиенты ---> Договоры ---> Создать новый договор (рисунок 6.30).

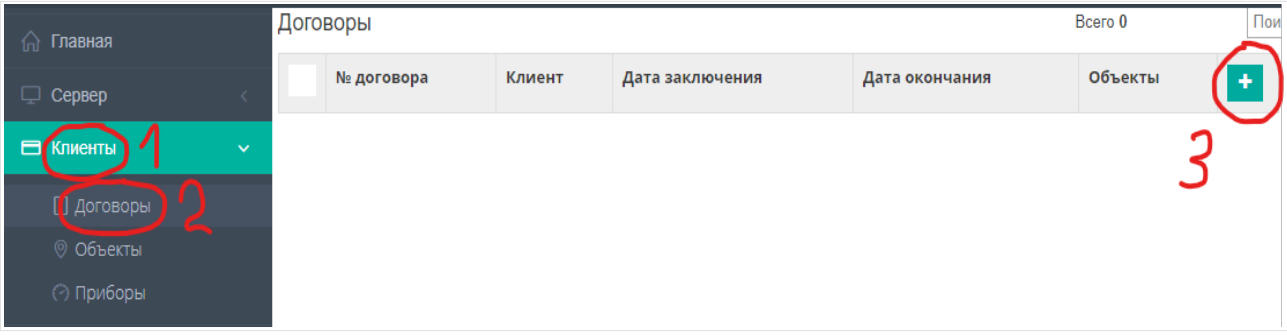


Рисунок 6.30 Создание нового договора

3.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Заполнить поля договора. Обязательными являются поля "Номер договора", а также поле "Состояние" должно стоять "Активен" (рисунок 6.31).

Остальные поля заполняются по необходимости. После ввода всех необходимых данных нажать кнопку "Сохранить".

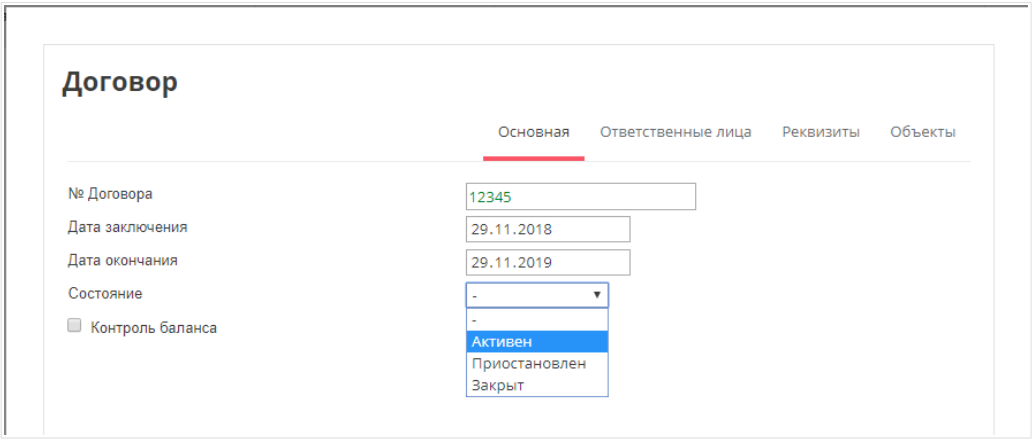


Рисунок 6.31 Заполнение договора

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.5.3 Добавление объекта

Для добавления объекта охраны необходимо:

1. Войти в систему администрирования КРОС под учетной записью администратора охранного предприятия.

Установленные по умолчанию:

Логин: admin

Пароль: admin

2. Зайти в меню Клиенты ---> Объекты ---> Создать новый объект (рисунок 6.32).

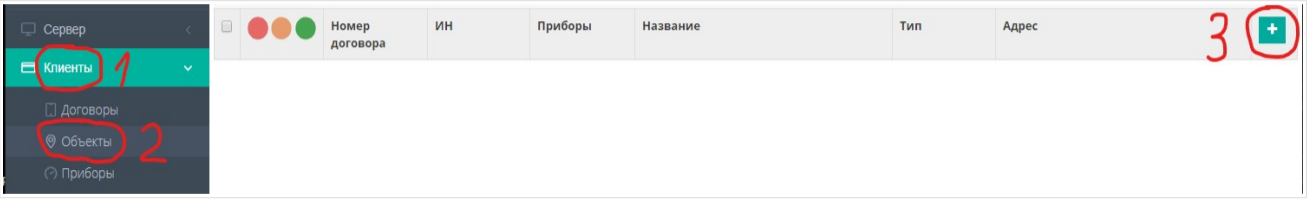


Рисунок 6.32 Создание нового объекта

3. Заполнить поля объекта. Обязательным является только поле "Номер договора".

Остальные поля заполняются по необходимости. После ввода всех необходимых данных нажать кнопку "Сохранить" (рисунок 6.33).

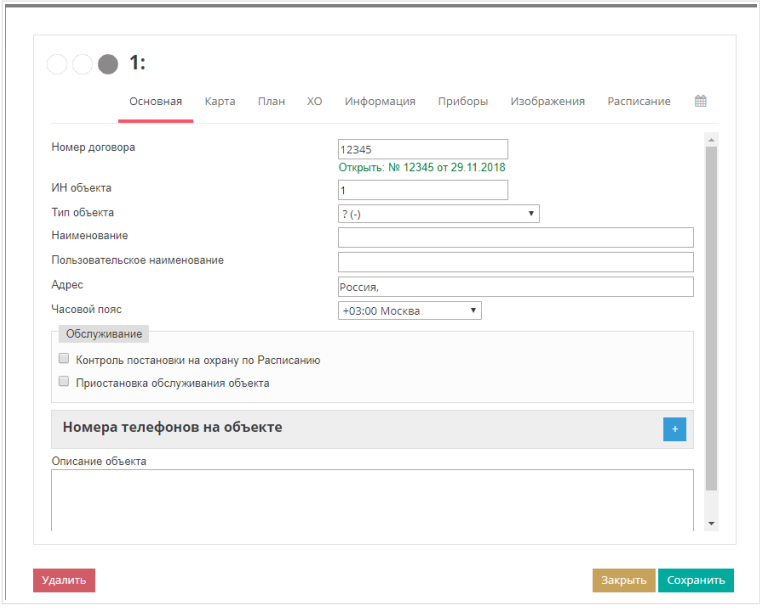


Рисунок 6.33 Заполнение нового договора

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.5.4 Добавление прибора

Добавление нового прибора на сервер происходит в автоматическом режиме, но требует правильной конфигурации самого прибора, чтобы прибор знал на какой сервер ему подключаться.

Для конфигурации прибора требуется:

1. Подключить прибор USB кабелем к компьютеру (рисунок 6.34), зайти на накопитель прибора и запустить конфигуратор(рисунок 6.35).

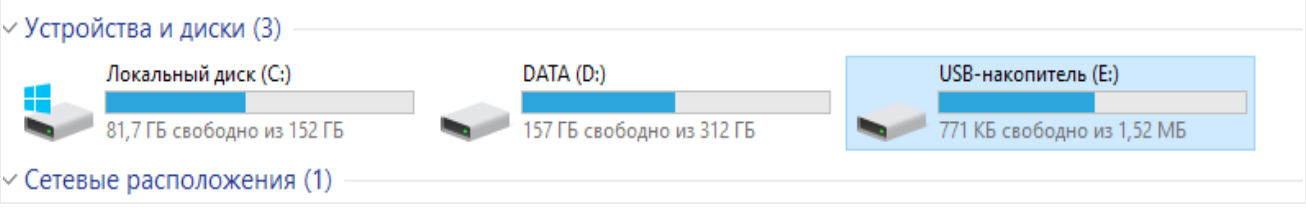


Рисунок 6.34 Подключение прибора к компьютеру

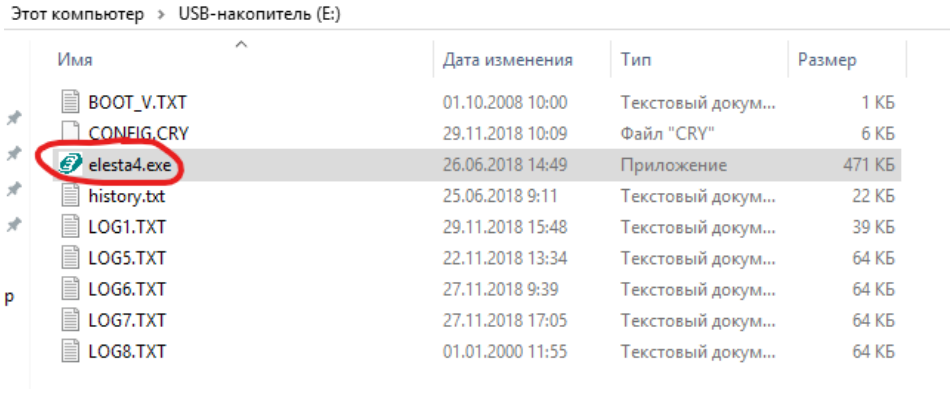


Рисунок 6.35 Запуск конфигуратора

2. В конфигураторе выбрать пункт IP/UDP, задать идентификатор прибора и очистить ключ шифрации на "по умолчанию" (рисунок 6.36).

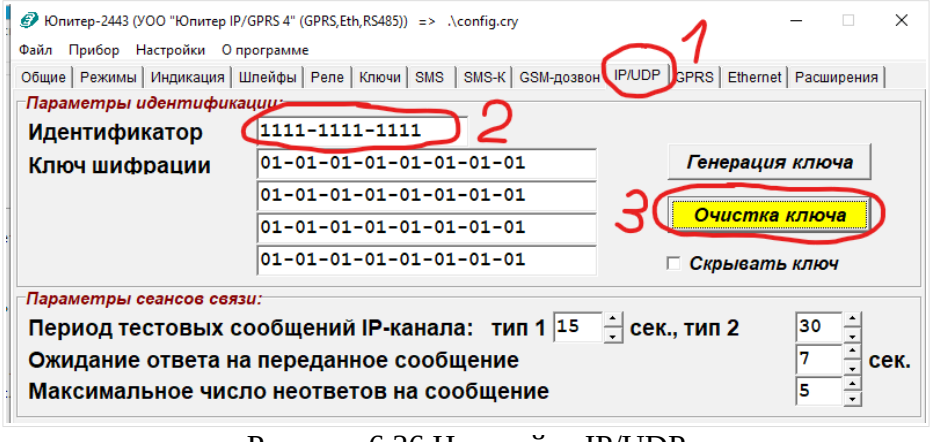


Рисунок 6.36 Настройка IP/UDP

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Далее настройка прибора немного различается в зависимости от возможностей вашего прибора.

3.1 На картинке ниже показан вариант настройки прибора по Ethernet (рисунок 6.37).

- Если прибор с сервером находятся в одной сети, то в поле "Параметры серверов сообщений" требуется написать внутренний IP-адрес компьютера, на котором установлен сервер КРОС, например 192.168.1.27 и порт, который вы выбрали для соединения с КРОС.
- Если прибор с сервером находятся в разных сетях, то в поле "Параметры серверов сообщений" требуется написать внешний белый IP-адрес компьютера, на котором установлен сервер КРОС, например 32.13.32.23 и порт, который вы выбрали для соединения с КРОС.

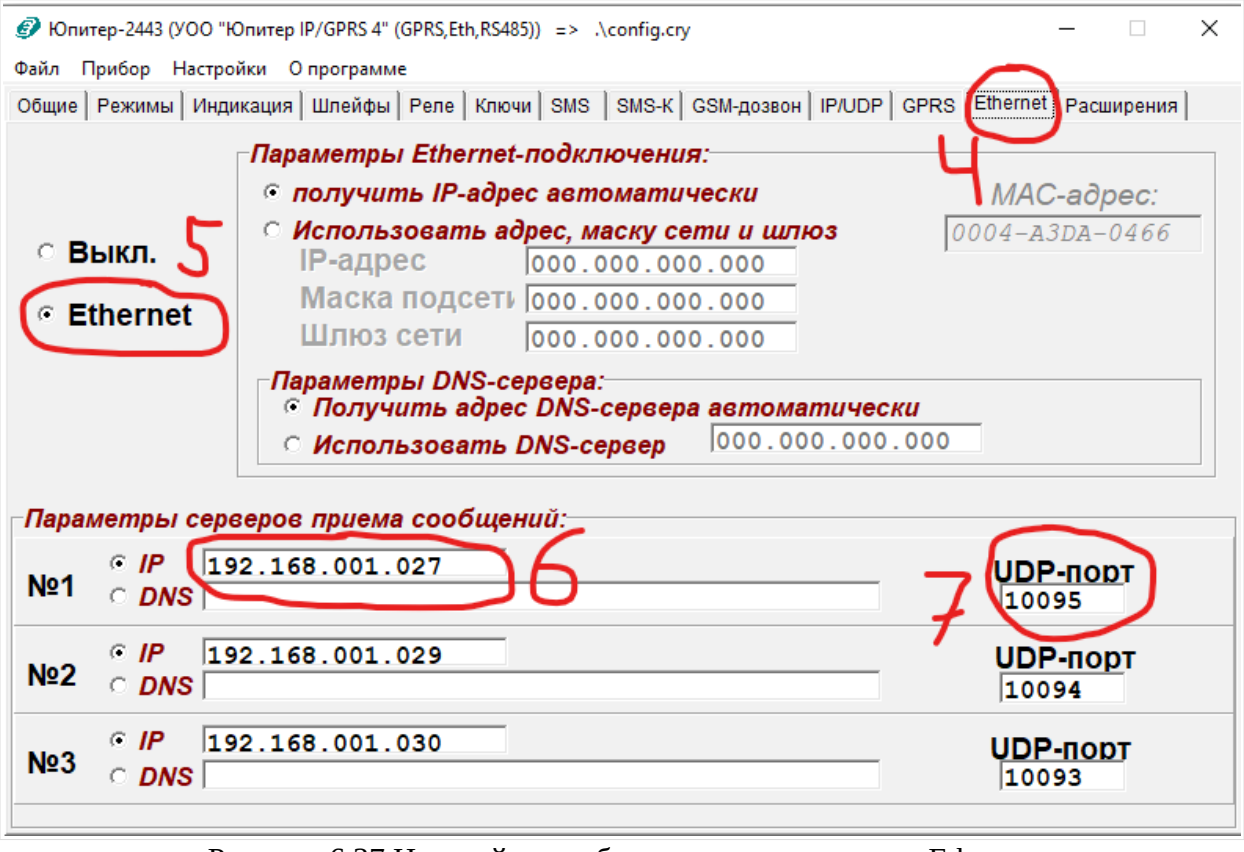


Рисунок 6.37 Настройка прибора для соединения по Ethernet

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.2 На картинке ниже показан вариант настройки прибора по GPRS (рисунок 6.38).

- В поле "Параметры GPRS SIM-карты" требуется написать информацию об APN-сервере, которая отличается в зависимости от используемого оператора мобильной свези
- В поле "Серверы приема сообщений" требуется написать внешний белый IP-адрес компьютера, на котором установлен сервер КРОС, и порт, который вы выбрали для соединения с КРОС

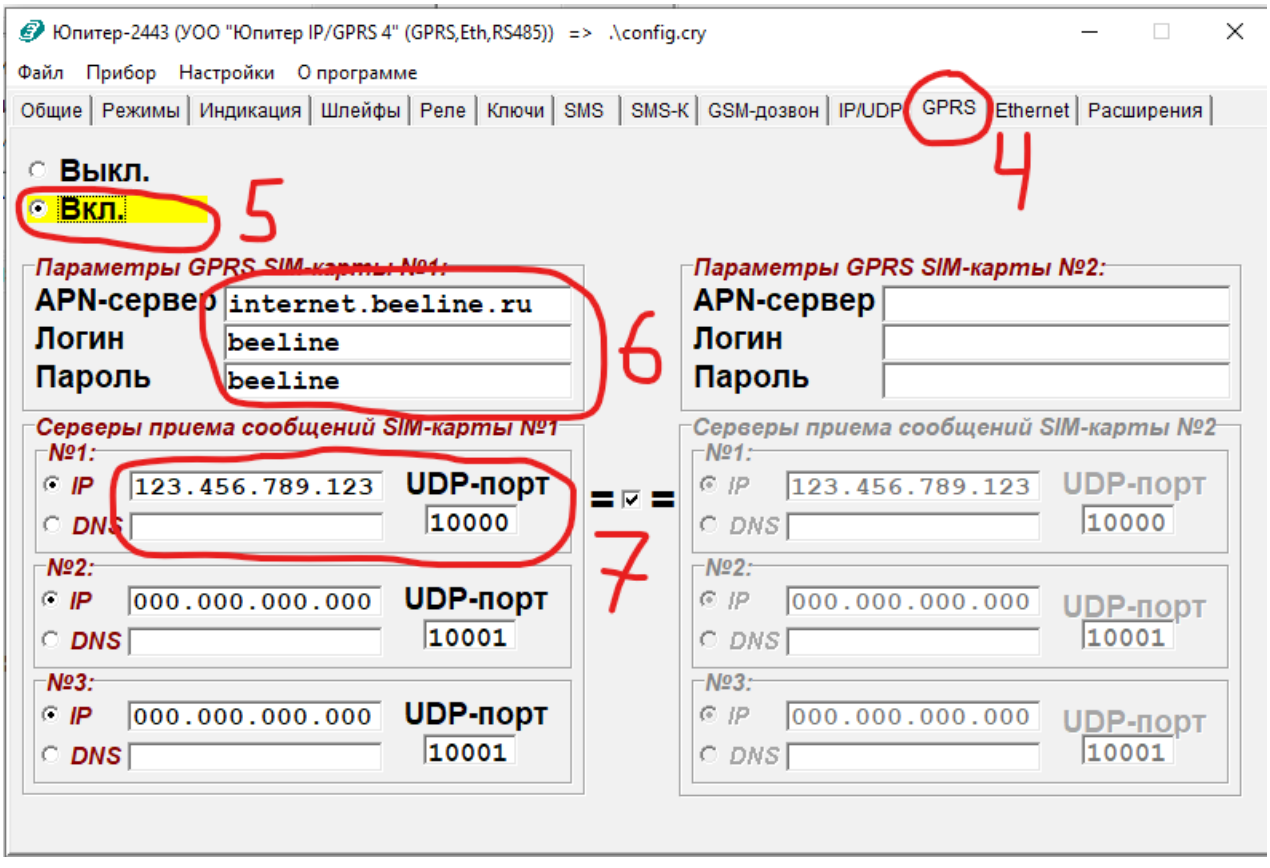


Рисунок 6.38 Настройка прибора для работы по GPRS

4. После ввода необходимых для соединения данных требуется нажать в конфигураторе кнопку "В устройство", чтобы записать данные на прибор.

После записи данных необходимо извлечь USB-кабель с помощью безопасного извлечения, после чего выключить и включить прибор. После этого изменения вступят в силу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Войти в систему администрирования КРОС под учетной записью **администратора охранного предприятия**.

Используйте установленные по умолчанию:

Логин: admin

Пароль: admin

6. Зайти в меню Клиенты ---> Приборы

Если настройка прибора была проведена корректно, то прибор автоматически появится в списке (рисунок 6.39).

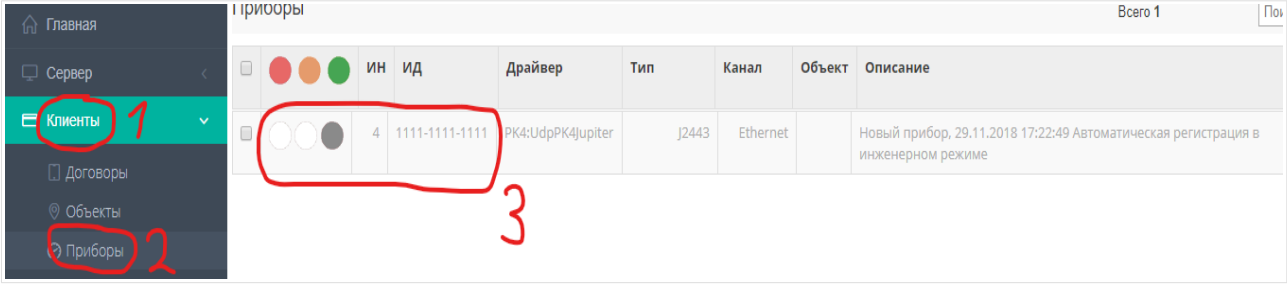


Рисунок 6.39 Появление прибора в списке

7. Для подключения прибора к объекту требуется:

7.1 Зайти в меню Клиенты ---> Объекты ---> Редактирование объекта

7.2 Зайти в раздел "Приборы" и поставить галочку на приборе, который хотите подключить к данному объекту, и нажать кнопку "Сохранить" (рисунок 6.40).

После этого прибор будет подключен к объекту.

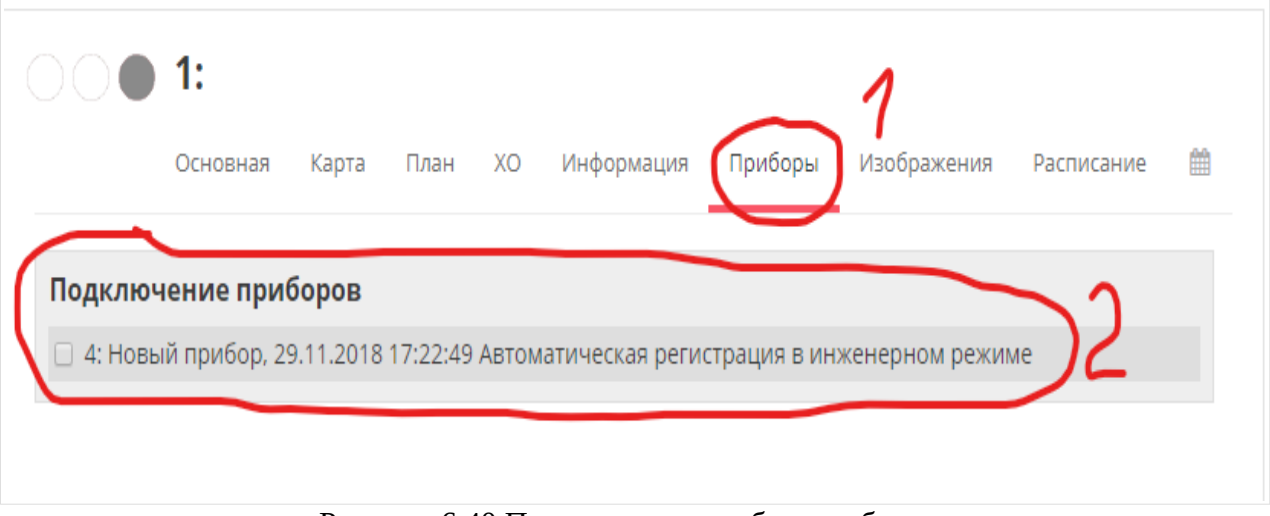


Рисунок 6.40 Подключение прибора к объекту

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.6 Ответственные лица

В меню Ответственные лица (меню Клиенты → Ответственные лица) (рисунок 6.41) отображаются, настраиваются и удаляются ответственные лица.
Меню Ответственные лица по умолчанию доступно Администратору.

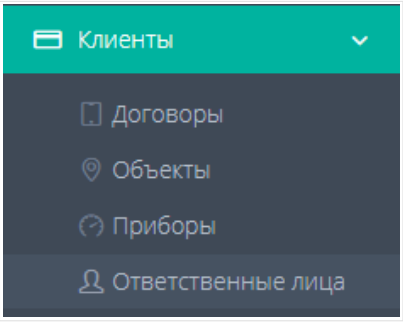


Рисунок 6.41 Меню «Ответственные лица»

В верхней части таблицы располагается:

1. Окно поиска.
2. Общее количество ответственных лиц в данной охранной организации.
3. Фильтр ответственных лиц по различным критериям:
   - Все (общий список)
   - Ответственные лица с личным кабинетом
   - Ответственные лица с тревожной кнопкой
   - Ответственные лица с часами "Умка"
   - Ответственные лица с подключенным СМС-оповещением

В основной таблице отображается сводная информация по каждому ответственному лицу. Для каждого ответственного лица доступно окно редактирования, в котором можно изменить личные данные, дать доступ в личный кабинет, к тревожной кнопке и другим опциям.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Ответственные лица

Поиск: Введите текст для поис Всего: 24

Все
- Все
- С личным кабинетом
- С тревожной кнопкой
- С умкой
- С SMS оповещением
- Инкассаторы

ИН	НАИМЕНОВАНИЕ	НОМЕР ДОГОВОРА	ФИО	ЛОГИН	НОМЕР УМКИ	ТЕЛЕФОНЫ
5	Бережная Анна Семеновна	12s1833e		33g817n1w561		8911223422354
6	Семен Петрович Бережной	12s1833e		23j01i7iv8dc		89214432277
7	Объемный Даниил Кондратьевич	12s1833e		1st635yojj211		89134435567
8	Бережная Анна Семеновна	12s1833e		dgx2o6211w86		8911223422354
9	Семен Петрович Бережной	12s1833e		i395mpm7cqgw		89214432277
10	Объемный Даниил Кондратьевич	12s1833e		2v0me3m5us9c		89134435567
11	Бережная Анна Семеновна	12s1833e		j952f1ose7p5		8911223422354
12	Семен Петрович Бережной	12s1833e		6exsr3ny861b		89214432277
13	Объемный Даниил Кондратьевич	12s1833e		09oau8ae0573		89134435567
14	Демилова Ольга Петровна	10_4GSMg		vp72ypo2440d		4438854
15	Солодов Эбрагим Власович	10_4GSMg		tm210wclnt28		7164532
16	Ситников Андрей Борисович	10_4GSMg		gzz0mqv77g83		77233244
17	Серов Сергей Валентинович	14s2444e		wet9z51u0m5n		4434433
18	Дарья Павловна Ульянова	14s2444e		8y260doqeihe		8843345
19	Тимур Андреевич Толстокожий	14s2444e		3agp6z2r3874		54334442
20	Код принуждения, общий для всех собственников	14s2444e		568gn36s7g6j		

Рисунок 6.42 Таблица ответственных лиц

SEC.RU | Короткий путь к информации Скачано с sec.ru

7. Меню «Охрана»

7.1 Реквизиты

В окне «Реквизиты» (меню «Охрана» → «Реквизиты») (рисунок 7.1) **Администратор сервера** создает структуры подразделений охранных организаций внутри основного сервера.

Один сервер КРОС может работать с неограниченным количеством охранных организаций. Количество может ограничиваться только системными ресурсами и параметрами тарифа. Каждой охранной организации выделяется отдельная область в базе данных и собственный пул портов для входящих соединений. Кроме того для каждой организации могут быть определены индивидуальные параметры.

К окну «Реквизиты» по-умолчанию имеют доступ **Администратор сервера** и **Администратор**. **Администратор** не может добавлять новые реквизиты или удалять существующие, только редактировать относящийся к его организации.

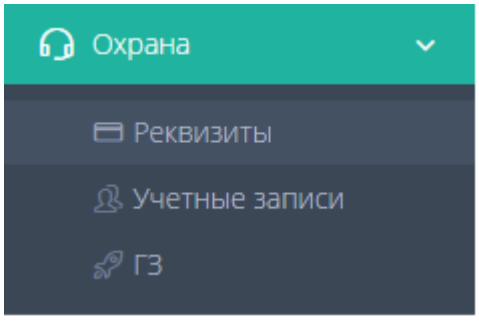


Рисунок 7.1 Меню «Реквизиты»

При создании записи охранной организации для нее может быть указан достаточный набор реквизитов, таких как ИНН, КПП, Краткое и полное наименование, ФИО директора и главного бухгалтера, номера телефонов, итд.

SEC.RU | Короткий путь к информации Скачано с sec.ru

В случае наличия доступа в интернет возможен поиск по ИНН и автоматическое заполнение реквизитов. Кроме того при корректном вводе БИК в случае наличия доступа в интернет происходит автоматический поиск актуальных реквизитов банка. Также при заполнении юридического и фактического адреса автоматически определяется почтовый индекс.

Для каждой охранной организации может быть индивидуально установлен календарь праздничных дней. Этот календарь будет использован для временных расчетов, в том числе для графика охраны объектов. Для объекта можно определить индивидуальный календарь, в этом случае календарь объекта будет иметь более высокий приоритет.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.1 Параметры охранной организации

Внимание!

При создании дополнительных охранных организаций каждая новая созданная организация должна иметь УНИКАЛЬНЫЙ набор портов!

В случае наличия повторяющихся в разных организациях портов сохранение целостности оперативных данных НЕ ГАРАНТИРУЕТСЯ!

Параметры охранной организации добавляются и редактируются во вкладке «Параметры». Доступ к вкладке параметры - Охрана→ Реквизиты → Редактировать охранную организацию → “Параметры” (рисунок 7.2).

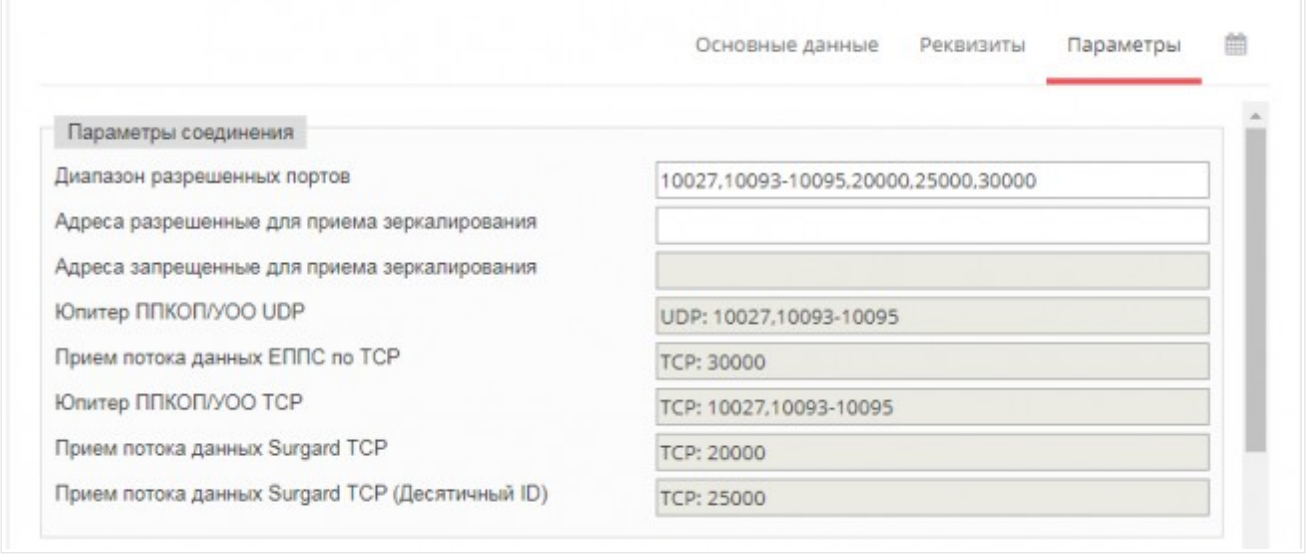


Рисунок 7.2 Вкладка параметров охранной организации

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.1.1 Параметры соединения

- **Диапазон разрешенных портов**

Список портов, выделенных охранной организации. Порты выделяются независимо от протокола. Например, если выделен порт 10095 то он будет работать и на UDP и на TCP протоколах, и во всех случаях будет связан с охранной организацией. Обычно при создании организации выделяется по одному свободному порту для каждого активного НЕ-служебного драйвера. Порты служебных драйверов общие для всех охранных организаций.

Поскольку распределение портов является критически важным для правильной работы приборов - редактирование списка портов доступно только в режиме Администратора сервера. При этом Администратор сервера берет на себя ответственность за уникальность набора портов для каждой организации. В противном случае могут возникнуть коллизии с отправкой данных прибором в другую охранную организацию.

- **Адреса разрешенные для зеркалирования**

В случае работы КРОС в режиме многосерверной конфигурации с “горячим” резервированием со стороны принимающего сервера требуется разрешение со всеми остальными зеркалируемыми серверами. Перечислить IP адресов можно в этом поле. IP адреса перечисляются через запятую.

- **Адреса запрещенные для зеркалирования**

В случае работы КРОС в режиме многосерверной конфигурации с “горячим” резервированием при попытке соединения от сервера, не внесенного в список разрешенных, его IP адрес фиксируется в этом поле. После переноса зафиксированного адреса в список разрешенных и после первого удачного соединения адрес удаляется из списка запрещенных.

- **Перечень драйверов приемников с привязкой к портам и протоколам**

Отображается информационная таблица, с перечислением используемых в системе

SEC.RU | Короткий путь к информации Скачано с sec.ru

драйверов, указанием протокола и списка портов индивидуально для каждого драйвера.

7.1.1.2 Активность GSM-модема

Определение соответствия набора функций “Дозвон без соединения” с номерами телефона GSM модема. В случае использования одного модема для нескольких охранных организаций этот раздел заполнять не нужно - будет использован базовый список, определенный для драйвера GSM модема.

- Номер телефона - номер телефона канала GSM модема.
- Действие - действие, инициируемое КРОС, в случае получения звонка на указанный канал модема. Возможные варианты:
  - Дежурный режим
  - Тревога
  - Взять
  - Снять

7.1.1.3 Каналы IP-модема

Настройки для IP модема. Позволяют добавить соответствие:

- Номер телефона
- IP адрес модема
- Номер порта

7.1.1.4 Инженерный режим

Если ни один раздел прибора не прикреплен к какому-либо объекту - считается что прибор работает в Инженерном Режиме. Если хотя бы один раздел прибора связан с объектом - прибор работает в Штатном режиме. Данные и события инженерных приборы не передаются в АРМ ДПУ/ДО/СК работающие в штатном режиме, также для трансляции данных с таких

SEC.RU | Короткий путь к информации Скачано с sec.ru

приборов необходимо явно установить в трансляции параметр Инженерный режим.

- **Разрешить автоматическую регистрацию приборов в инженерном режиме**

Если параметр включен - все вновь подключаемые к КРОС приборы будут автоматически регистрироваться в т.н. “песочнице” в инженерном режиме. Если выключен - автоматическая регистрация новых приборов будет запрещена.

- **Автоматически устанавливать пароль на изменение настроек подключения в инженерном режиме для приборов Сатурн**

Параметр работает только для приборов Сатурн, в которых есть возможность установить блокировку на изменение настроек подключения. Если параметр отключен - блокировка будет автоматически установлена если прибор работает в Штатном режиме, и отключена если прибор переведен в Инженерный режим. Если параметр включен - блокировка будет автоматически установлена в любом случае.

- **Удалять неактивные приборы в инженерном режиме**

Если прибор, зарегистрированный в инженерном режиме, не проявляет активности в течение указанного времени - он будет удален из базы данных. Отключить удаление можно с помощью этого параметра.

- **Период неактивности инженерных приборов до удаления (сек)**

Время в секундах, после которого будут удалены приборы в инженерном режиме, в случае если это разрешено предыдущим параметром.

7.1.1.5 Режим работы

- **Автоматически создавать канал Contact-ID для новых приборов**

При регистрации нового прибора, подключившегося с использованием протокола ПК4 (Сатурн/Юпитер) для него, кроме канала ПК4 будет также создан канал CID с драйвером TcpSurgard, что обеспечит возможность для этого прибора принимать и транслировать данные по протоколу SurGard. Для создаваемого канала в качестве OID и IMEI используется десятичное значение параметра ID6 канала ПК4.

- **Автоматически включать режим поддержки безопасного взятия для новых**

SEC.RU | Короткий путь к информации Скачано с sec.ru

приборов
Параметр имеет значение для HTTP/JSON API, которое поддерживает два режима взятия для приборов. Безопасное взятие контролирует состояние всех зон, и будет отвергнуто если хотя бы одна зона не в состоянии “НОРМА”. При этом формируется тревожное сообщение с причиной отказа. Второй режим взятия устанавливает все разделы во взятое состояние без проверок.
По умолчанию поддержка безопасного взятия не включена. Этот параметр устанавливается в свойствах конкретного прибора и может быть установлен для группы приборов. Однако если требуется автоматически включать этот параметр для всех вновь подключающихся приборов - нужно использовать описываемый параметр.

- **Устанавливать разделы не содержащие зон во взятое состояние**

Устанавливается, если необходимо работать с логическими приборами, содержащими разделы, но не содержащими зон. Например с мобильным телефоном, заведенным вручную в базу данных КРОС в качестве прибора с СИМ картой и используемого в качестве тревожной кнопки в сочетании с GSM модемом.

- **Устанавливать разделы содержащие только КТС во взятое состояние**

Если раздел содержит только КТС то логически он всегда находится под охраной. Однако, например, конфигуратор для работы с прибором требует, чтобы прибор был полностью снят, с этой целью прибор позволяет перевести такой раздел в снятое состояние. Описываемый параметр принудительно устанавливает такой раздел во взятое состояние.

- **Автоматически создавать отсутствующие разделы**

В случае получения сообщения от раздела отсутствующего в конфигурации прибора, зарегистрированной в базе данных - этот раздел будет автоматически создан.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Автоматически создавать отсутствующие зоны**

В случае получения сообщения от зоны отсутствующей в конфигурации прибора, зарегистрированной в базе данных - эта зона будет автоматически создана.

- **Контроль неисправности каналов связи для каналов CSD (Дозвон)**

Включает \ отключает контроль неисправности для приборов, работающих по каналу CSD (модем).

7.1.1.6 Обработка тревог

- **Обрабатывать тревоги от снятых объектов**

Если этот параметр установлен то в случае получения тревожного сообщения от снятого раздела будет создан дескриптор тревоги и пересчитано состояние прибора и объекта. Если этот параметр не установлен - в системе появится тревожное сообщение, но дескриптор тревоги создан не будет.

- **Разрешать отбой тревог от взятых приборов и объектов с неисправностью канала связи**

Установка параметра позволяет отбивать тревоги в случае если прибор, связанный с объектом:

a) взят под охрану,

b) находится в тревожном состоянии,

c) потерял связь с системой,например отключен инженером для проведения ремонта.

- **Всегда обрабатывать тревоги Взлом, Движение корпуса, Сбои питания, Перегрев, Переохлаждение**

Любое из перечисленных сообщений будет инициировать создание дескриптора тревоги и пересчет состояния прибора и объекта, независимо от состояния охраны прибора.

- **Всегда обрабатывать тревоги КТС, Пожарные, Газ, Затопление**

Любое тревожное сообщение от шлейфа одного из перечисленных типов будет инициировать создание дескриптора тревоги и пересчет состояния прибора и объекта, независимо от состояния охраны прибора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Разрешать взятие тревожных разделов**

По умолчанию отправка команд взятия разделам, находящимся в тревожном состоянии запрещена. Этот параметр позволяет разрешить отправку команд взятия тревожным разделам.

- **Генерировать тревогу по событию потери связи с прибором**

Установленная галочка отвечает за генерацию тревожного сообщения при потере связи прибора с пультом охраны.

- **Генерировать тревогу при потере связи с приложением ТК**

Установленная галочка отвечает за генерацию тревожного сообщения при потере связи приложения «Тревожная кнопка V.2.0.» с пультом охраны.

7.1.1.7 Режим работы АРМ

- **Запрет работы в нескольких АРМ под одним именем**

К одному серверу КРОС может быть подключено неограниченное количество АРМ. Каждый оператор АРМ регистрируется в системе и получает индивидуальные аутентификационные данные. Параметр запрещает множественный вход под одним логином и паролем на разных АРМ одновременно.

- **Время ожидания подтверждения принятия тревоги от ДО (сек)**

При передаче тревоги от АРМ ДПУ на АРМ ДО в ручном режиме происходит ожидание подтверждения принятия тревоги в работу. Если в течение указанного времени ни один ДО не принял тревогу в обработку она возвращается на АРМ ДПУ.

7.1.1.8 Контроль резервного питания

- **Генерировать тревогу при переходе прибора на резервное питание**

По умолчанию переход прибора на резервное питание не является тревогой. Если же этот параметр включен - при пропадании основного питания КРОС включает таймер, и если после истечения заданного тайм-аута состояние питания остается прежним - генерирует тревожное сообщение.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.1.9 Параметры учета состояния договора

КРОС может контролировать состояние договора обслуживания, и прекращать обработку событий от объектов, относящихся к договору, в случае неактивности, приостановки или истечения. Для управления эти контролем служат следующие параметры:

- **Блокировать сообщения от объектов с неактивными договорами**

Объекты будут отключены в случае если действие договора еще не началось, либо состояние договора не определено. КРОС периодически проверяет даты начала и окончания договоров, и если их текущее состояние не определено - устанавливает состояние Активен , в случае актуальности указанного периода действия договора, либо Закрыт - в случае если период договора истек.

- **Блокировать сообщения от объектов с приостановленными договорами**

Объекты будут отключены в случае если для договора установлено состояние Приостановлен . Это состояние может быть установлено или снято только вручную.

- **Блокировать сообщения от объектов с закрытыми договорами**

Объекты будут отключены если срок договора истек либо состояние договора установлено в Закрыт . КРОС периодически проверяет даты начала и окончания договоров, и если их текущее состояние не определено - устанавливает состояние Активен , в случае актуальности указанного периода действия договора, либо Закрыт - в случае если период договора истек.

Чтобы сохранить реквизиты, после заполнения вкладок, необходимо нажать на кнопку «Сохранить» в нижней части окна «Реквизиты».

Чтобы закрыть окно «Реквизиты» без сохранения, нужно нажать на кнопку «Закрыть» или «Удалить» в окне «Реквизиты».

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.2 SMPP сервер

Отправка SMS сообщений осуществляется через интернет на SMS сервер провайдера услуги, который, в свою очередь отправляет SMS сообщение адресату.

Данную услугу Вы можете заказать у любого провайдера (предоставляющего услугу) независимо от его территориального расположения.

Провайдер должен предоставить Вам все необходимые настройки:

- Логин
- Пароль
- Номер порта
- Сетевой адрес SMPP сервера

Внимание!

В первую очередь перед настройкой SMPP сервера необходимо убедиться, что в личном кабинете поставщика услуги SMPP все корректно настроено!

Часто бывает так, что поставщики услуги блокируют некоторых операторов связи, требуется специальный тариф, либо не разрешен доступ к API поставщика услуг с вашего ip-адреса.

Обязательно убедитесь в корректности всех настроек.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Настройки доступа с SMPP серверу:

Осуществляется **Администратором охранной организации**. Для этого требуется:

1. Перейти Охрана - Реквизиты – Параметры (рисунок 7.4).

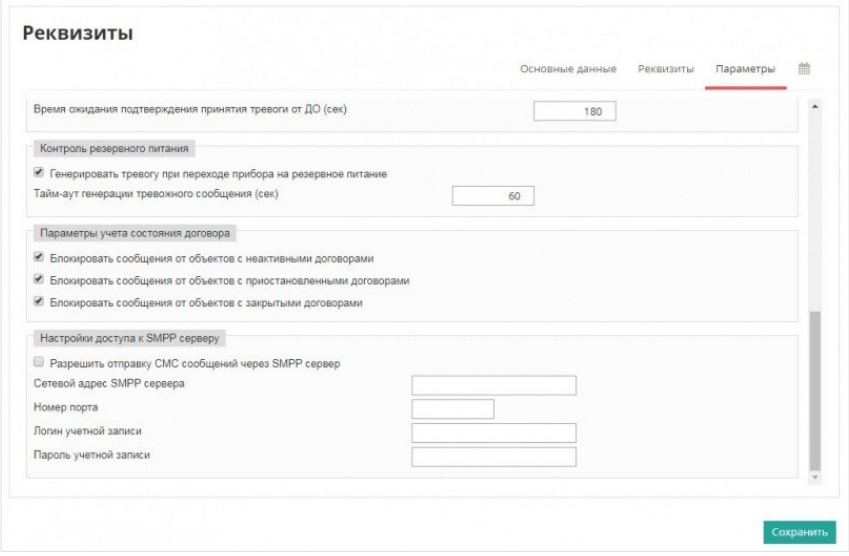


Рисунок 7.4 Настройки SMPP сервера

2. Ввести параметры SMPP сервера:
   - Сетевой адрес SMPP сервера
   - Номер порта
   - Логин учетной записи, выданной провайдером
   - Пароль учетной записи, выданной провайдером
3. Сохранить введенные данные.

Для уменьшения затрат на sms-сообщения необходимо создать отдельную таблицу перекодировки сообщений, в которой будут прописаны только необходимые вам сообщения. Для этого:

1) Зайти на сервер КРОС под учетной записью superadmin

2) Перейти во вкладку Сервер - Таблицы

3) Нажать кнопку "Добавить таблицу"

SEC.RU | Короткий путь к информации Скачано с sec.ru

4) Ввести название новой таблицы

5) Установить галочки (Блок сообщений) на те сообщения, которые НЕ будут включены в СМС пакет.

Для включения СМС информирования для Ответственного лица или Хозоргана требуется:

1) Зайти в настройки ответственного лица.

2) Установить галочку "Включить SMS оповещения" и выбрать созданную вами специальную таблицу для SMS.

3) Сохранить.

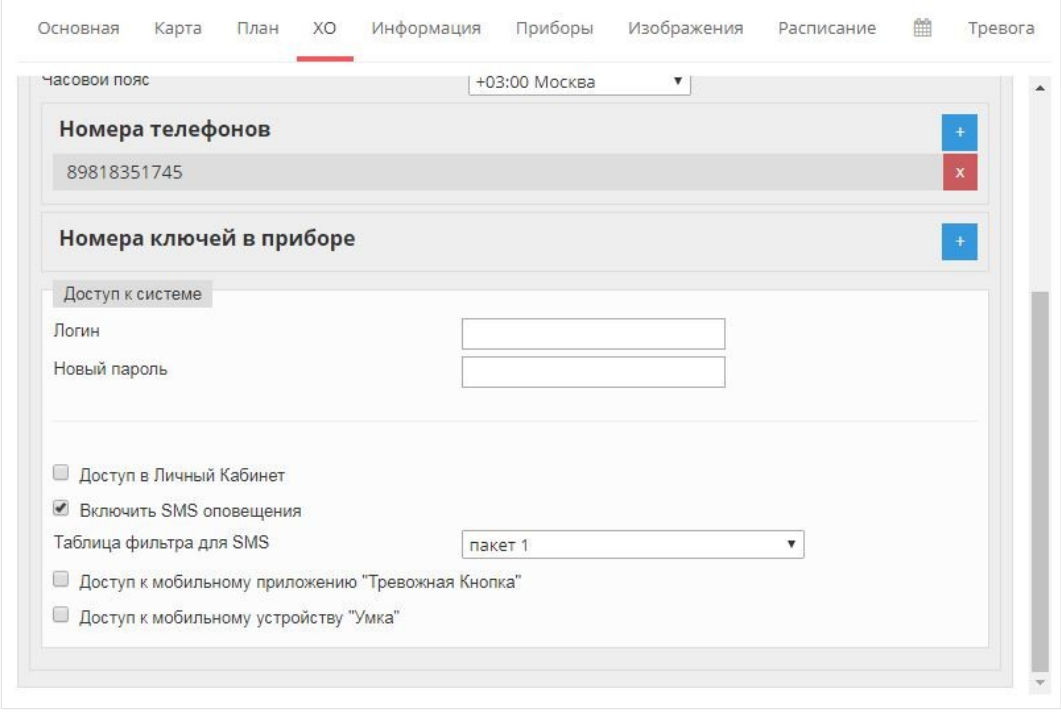


Рисунок 7.5 Включение СМС-оповещений для SMPP сервера

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.3 Редактирование реквизитов

Для редактирования реквизитов нужно:

1. Нажать на кнопку (редактировать) реквизиты.
2. Внести изменения в реквизиты.
3. Нажать кнопку «Сохранить» в окне «Реквизиты».

Чтобы закрыть окно реквизитов без сохранения, нажать «Закрыть» в окне «Реквизиты».

7.1.4 Удаление реквизитов

Для удаления реквизитов нужно:

1. Нажать на кнопку (редактировать) реквизиты.
2. Нажать кнопку «Удалить» в окне «Реквизиты».

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.2 Учетные записи

В окне «Учетные записи» (меню «Охрана»→«Учетные записи») (рисунок 6.6) создаются, редактируются и удаляются учетные записи.

Пользователь должен иметь уникальный логин и пароль в контексте всей системы КРОС, а не в рамках одной охранной организации. Это необходимо т.к. именно по идентификационным данным определяется принадлежность пользователя к той или иной охранной организации.

К окну «Учетные записи» по-умолчанию имеют доступ **Администратор сервера** и **Администратор**.

Администратор сервера не может добавлять новые учетные записи и имеет доступ только к учетным записям **Администраторов**.

Администратор имеет доступ к учетным записям сотрудников своего охранного предприятия. Учетные записи служат для разграничения прав доступа пользователей.

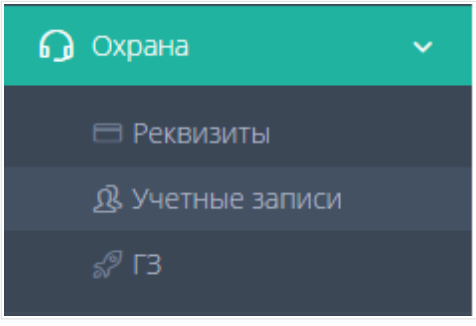


Рисунок 7.6 Меню «Учетные записи»

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.2.1 Добавление учетной записи

Чтобы добавить учетную запись нужно:

1. Нажать на кнопку (добавить).
2. В окне «Карта пользователя» на вкладке «Идентификация» ввести имя пользователя, логин и пароль (рисунок 7.7).

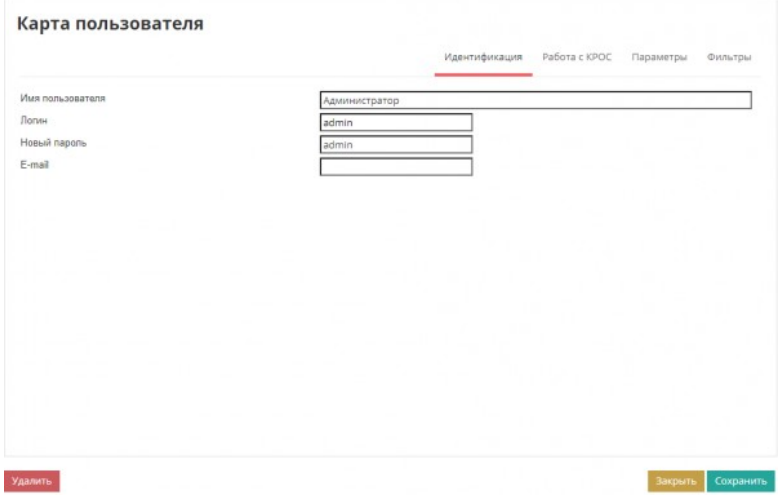


Рисунок 7.7 Вкладка ввода логина и пароля нового пользователя

Примечание: Логин не должен совпадать с уже существующим, если введенный логин будет красного цвета - это значит что данный логин уже используется в системе.

3. Перейти на вкладку «Работа с КРОС» (рисунок 7.8).

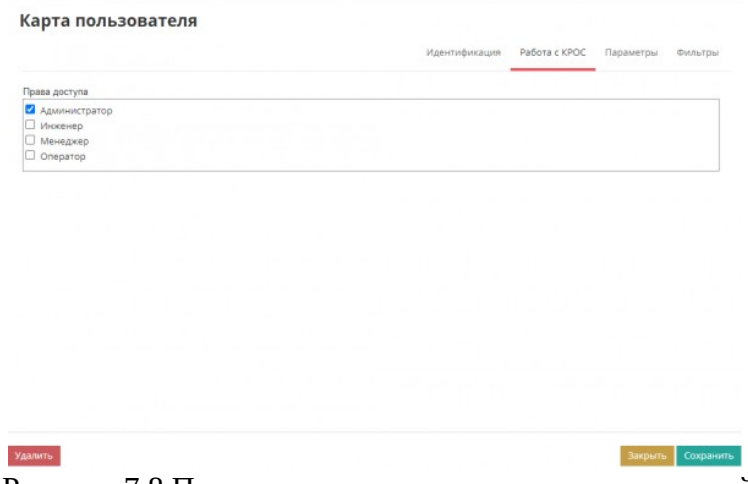


Рисунок 7.8 Права доступа для новых учетных записей

SEC.RU | Короткий путь к информации Скачано с sec.ru

Здесь отображается список всех ролей, активных в системе КРОС. Для пользователя можно активировать одну или несколько ролей.

- **Администратор** - Назначается пользователям имеющим право на изменение и создание учетных записей организации. Имеет доступ к созданию, редактированию и удалению договоров, объектов и проборов.
- **Инженер** - При работе на рабочем месте "АРМ" инженер может работать с приборами находящимися в режиме "инженерный".
- **Менеджер** - Имеет доступ для просмотра статистики, изменение, просмотр договоров, объектов и справочников.
- **Оператор** – назначается пользователям, не имеющим доступа к серверу организации, работающих только с АРМ Юпитер-Крос.

4. Для учетной записи выбрать роль учетной записи. Каждая из ролей имеет определенный набор прав доступа. Изначально существует 4 роли пользователей.

Примечание: Добавление новой роли учетной записи или изменение уже существующей осуществляется в окне «Безопасность» под учетной записью Администратора сервера.

5. Перейти на вкладку «Параметры» (рисунок 7.9).

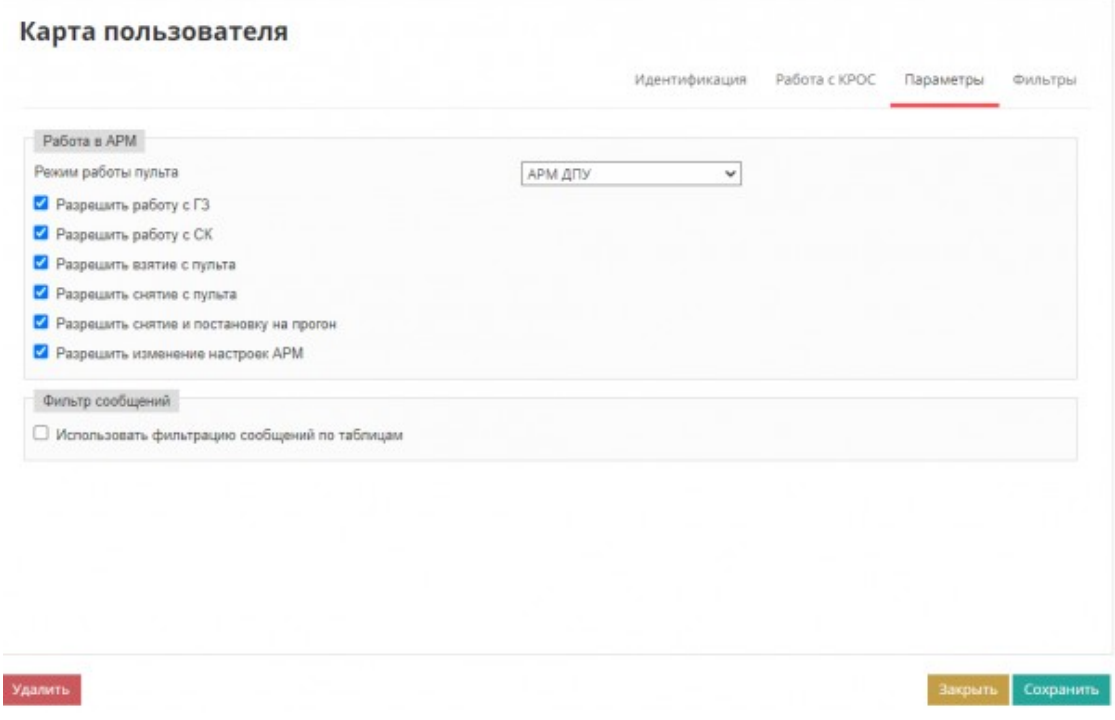


Рисунок 7.9 Параметры новых учетных записей

SEC.RU | Короткий путь к информации Скачано с sec.ru

6. Выбрать «Режим работы пульта». Возможные варианты:

- **Доступ запрещен**
  Полный запрет доступа в АРМ.
- **Инженерный**
  АРМ будет работать в инженерном режиме, т.е. получать и управлять приборами, находящимися в инженерном режиме, доступ к объектам и охранным функциям будет отключен.
- **АРМ ДПУ**
  АРМ в режиме Дежурный Пульта Управления.
- **АРМ ДО**
  АРМ в режиме Дежурный Офицер.
- **АРМ СК**
  АРМ в режиме Ситуационная карта.

7. Задать необходимые разрешения. Возможные варианты:

- **Разрешить работу с ГЗ**
  Для оператора АРМ ДПУ и ДО - дополнительно можно запретить или разрешить работать с Группами Задержания (ГЗ).
- **Разрешить работу с СК**
  Для оператора АРМ ДПУ и ДО - дополнительно можно запретить или разрешить работать с Ситуационной Картой (СК).
- **Разрешить взятие/снятие с пульта**
  Дополнительно определяет право пользователя ставить под охрану и снимать с охраны объекты средствами АРМ.
- **Разрешить снятие и постановку на прогон**
  Определяет право пользователя ставить на прогон и снимать с прогона объекты средствами АРМ.
- **Разрешить изменение настроек АРМ**
  Пользователь будет иметь право изменять настройки интерфейса и режимов работы АРМ средствами АРМ.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8. Выбрать таблицу перекодировки, если необходимо, либо оставить таблицу по умолчанию.

Для каждого пользователя можно индивидуально настроить таблицу перекодировки, которая будет использоваться для преобразования и фильтрации потока сообщений, видимых пользователю.

- **Использовать фильтрацию сообщений по таблицам**

Разрешение использования индивидуальной таблицы. Если параметр не включен - будет использоваться базовая таблица.

- **Таблица перекодировки**

Выбор таблицы перекодировки из списка имеющихся в системе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

9. Перейти на вкладку «Фильтры» (рис 7.9.1).

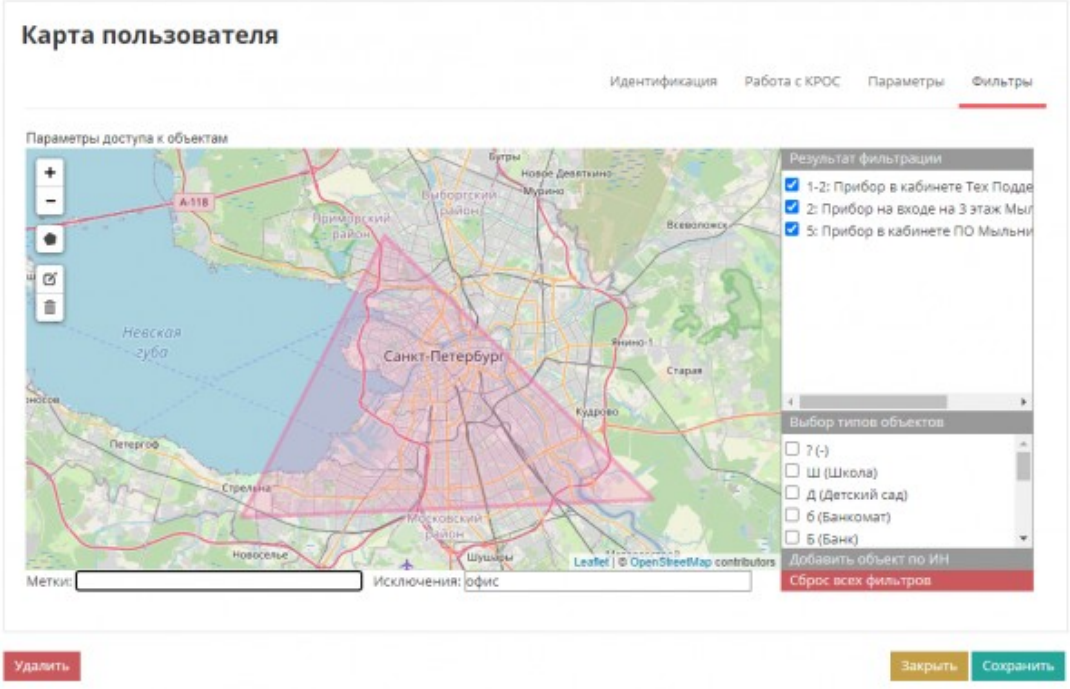


Рисунок 7.9.1 Фильтр учетной записи

10. Закрепить объекты охраны за учетной записью. По умолчанию, созданная запись видит все объекты.

Примечание: Для того что бы отобразить список объектов охраны, которые расположены на определенной территории, необходимо создать зону обслуживания.
Для того чтобы создать зону обслуживания, нужно кликнуть по инструменту (добавить зону обслуживания) и отметить территорию на карте.

В правой части окна располагаются те объекты охраны, которые проходят фильтрацию по геозоне.

9. Нажать на кнопку «Сохранить» в окне «Карта пользователя».
Чтобы закрыть окно «Карта пользователя» без сохранения, нужно щелкнуть по кнопке «Закрыть» или «Удалить» в окне «Карта пользователя».

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.2.2 Редактирование учетной записи

Чтобы отредактировать учетную запись нужно:

1. Нажать на кнопку (редактировать) учетную запись.
2. Внести изменения в учетную запись.
3. Нажать кнопку «Сохранить» в окне «Карта пользователя».

Чтобы закрыть окно учетной записи без сохранения, нажать «Закрыть» в окне «Карта пользователя».

7.2.3 Удаление учетной записи

Чтобы удалить учетную запись нужно:

1. Нажать на кнопку (редактировать) учетную запись.
2. Нажать кнопку «Удалить» в окне «Карта пользователя».

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.2.4 Фильтр объектов

Окно фильтра объектов состоит из редактора геозон (карта), списка индивидуальной фильтрации, списка фильтра типов и кнопки сброса всех фильтров (рисунок 7.10).

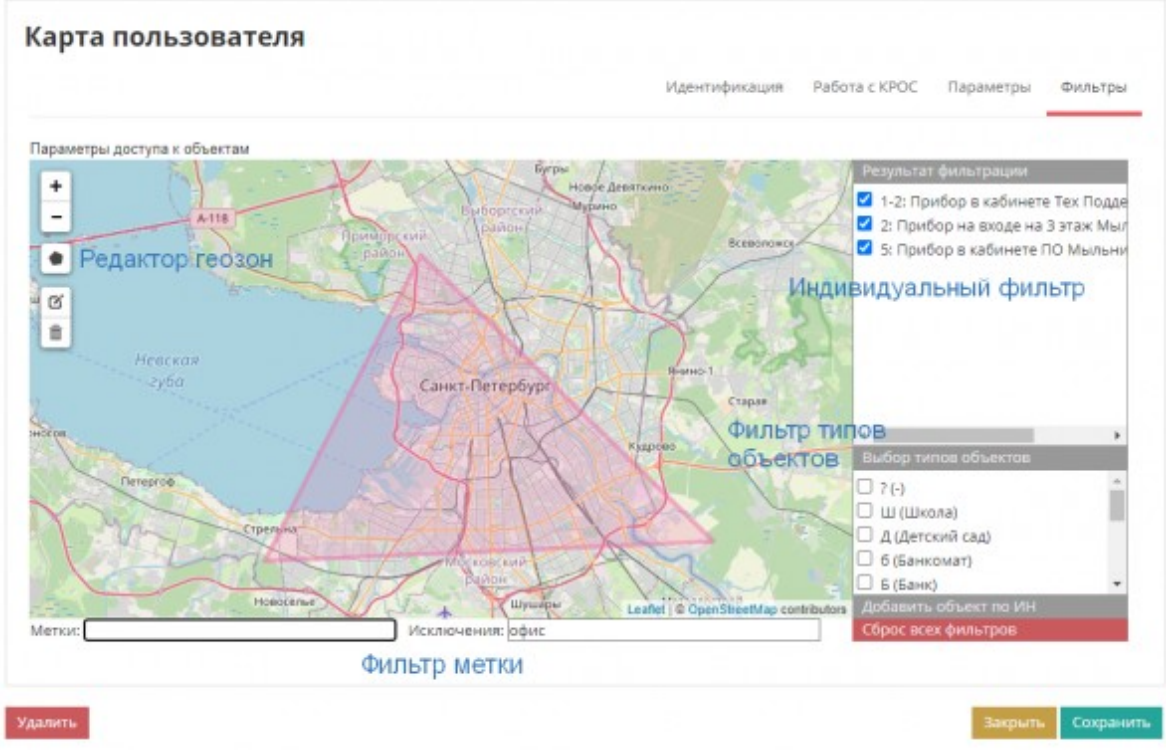


Рисунок 7.10 Окно фильтра объектов

Наивысший приоритет имеют геозоны, определяемые редактором геозон.
Все остальные фильтры накладываются на множество объектов, полученных после отсечения объектов не входящих в геозоны (рисунок 7.11).

SEC.RU | Короткий путь к информации Скачано с sec.ru

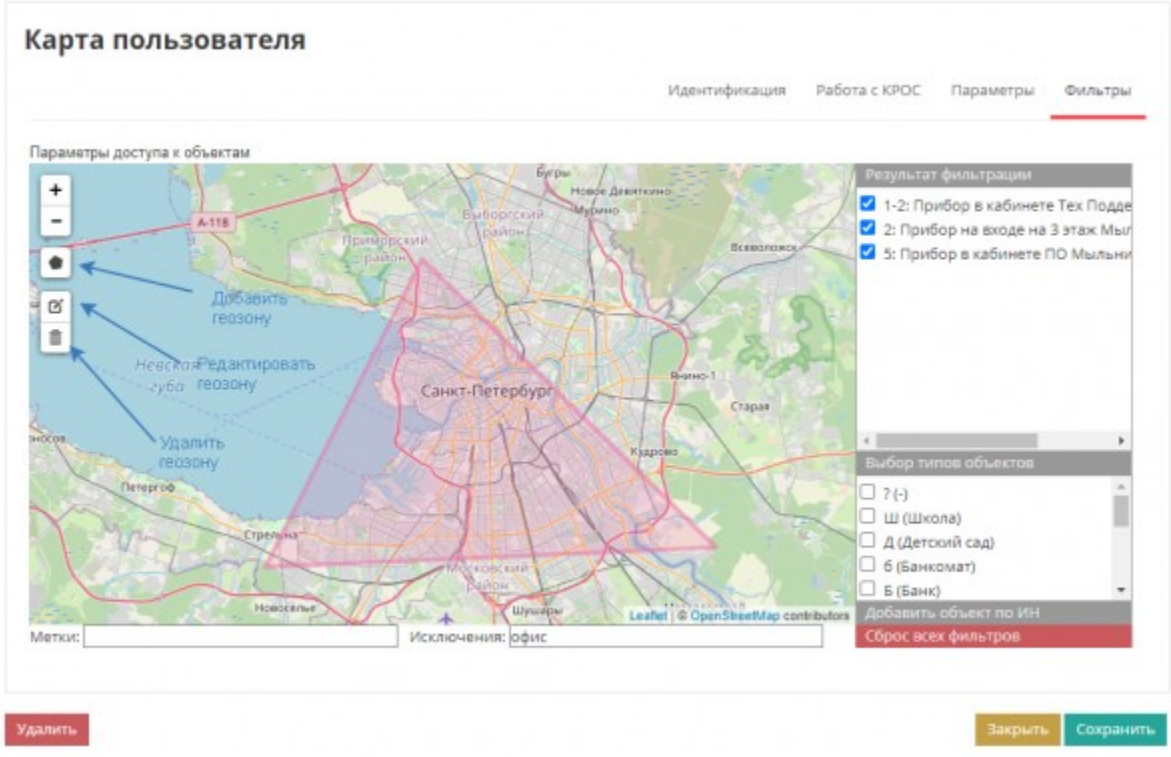


Рисунок 7.11 Редактор геозон

Существует возможность фильтрации объектов с помощью меток. Имеется возможность либо добавить фильтр по одной или нескольким одинаковым меткам, либо наоборот добавить исключения к фильтруемым объектам.

Может быть определено несколько геозон, при этом множества входящих в них объектов суммируются.

Возможен вариант без указания геозон. При этом остальные фильтры накладываются на первоначально доступное множество объектов.
После определения геозон, которые задают зону ответственности для фильтра, с правой стороны появляется список объектов, попавших в заданную геозону (рисунок 7.12).

SEC.RU | Короткий путь к информации Скачано с sec.ru

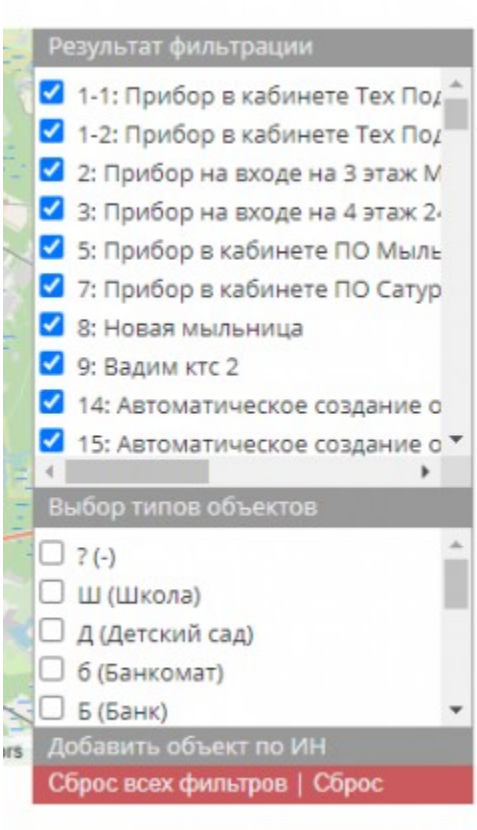


Рисунок 7.12 Фильтр объектов

Каждый объект в списке выделен, что означает его активность.
Объекты в списке могут быть отключены вручную.
В список может быть добавлен индивидуальный объект, не попадающий в общие условия фильтра.
Для этого нужно нажать кнопку “Добавить объект по ИН”, ввести идентификационный номер объекта, и подтвердить добавление. После этого выбранный объект появится в списке индивидуального фильтра.
Фильтр типа объекта, в случае если выбран хотя бы один тип из списка типов, исключит из списка индивидуальной фильтрации объекты, не совпадающие с выбранными типами.
Если ни один тип не выбран - фильтр типов объектов неактивен.

Можно отменить все уровни фильтрации если нажать кнопку “Сброс всех фильтров”. После этого доступным становится все первоначальное множество объектов.

Кнопка "Сброс" снимает выделение со всех объектов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.3 Группы задержания

В окне «ГЗ» (меню «Охрана»→«ГЗ») (рисунок 7.13) создаются, редактируются, удаляются ГЗ , и организуется их подключение к приложению «Юпитер-ГЗ».
К окну «ГЗ» по-умолчанию имеет доступ **Администратор.**

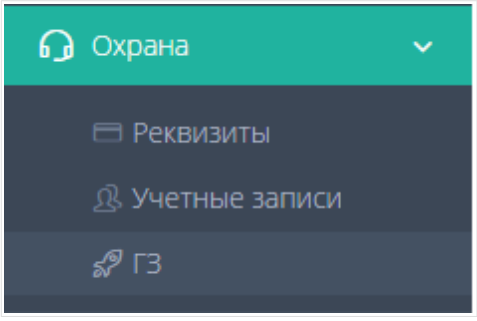


Рисунок 7.13 Меню «ГЗ»

7.3.1 Добавление ГЗ

Чтобы добавить ГЗ нужно:

1. Нажать на кнопку Добавить (белый плюс на зеленом фоне).

2. В открывшемся окне ввести идентификационный номер группы задержания. Заполнить поле - «Краткое описание» и ввести\создать пароль для «Юпитер-ГЗ» (рисунок 7.14).

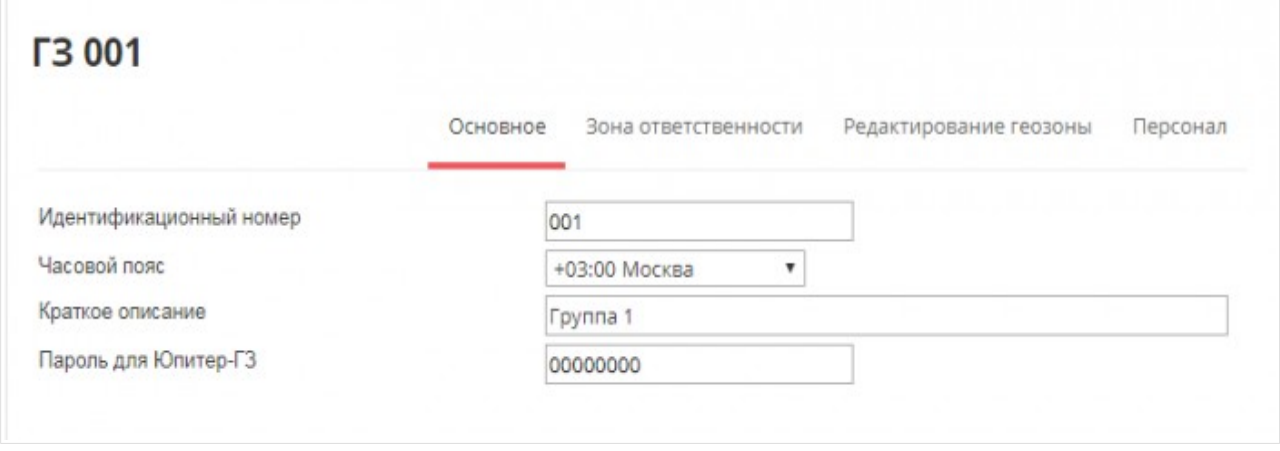


Рисунок 7.14 Создание новой ГЗ

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Во вкладке «Зона ответственности» можно настроить геозону, за которой закреплена группа быстрого реагирования, и объекты охраны в этой зоне расположенные.

Существует возможность закрепить конкретные ГЗ за конкретными объектами (рисунок 7.15).

Примечание: Для того чтобы отобразить список объектов охраны, которые расположены на определенной территории, необходимо создать зону ответственности. Для этого нужно кликнуть по инструменту (добавить зону обслуживания) и отметить территорию на карте. После нанесения на карту зоны обслуживания, в списке справа отобразятся объекты охраны которые входят в зону ответственности.

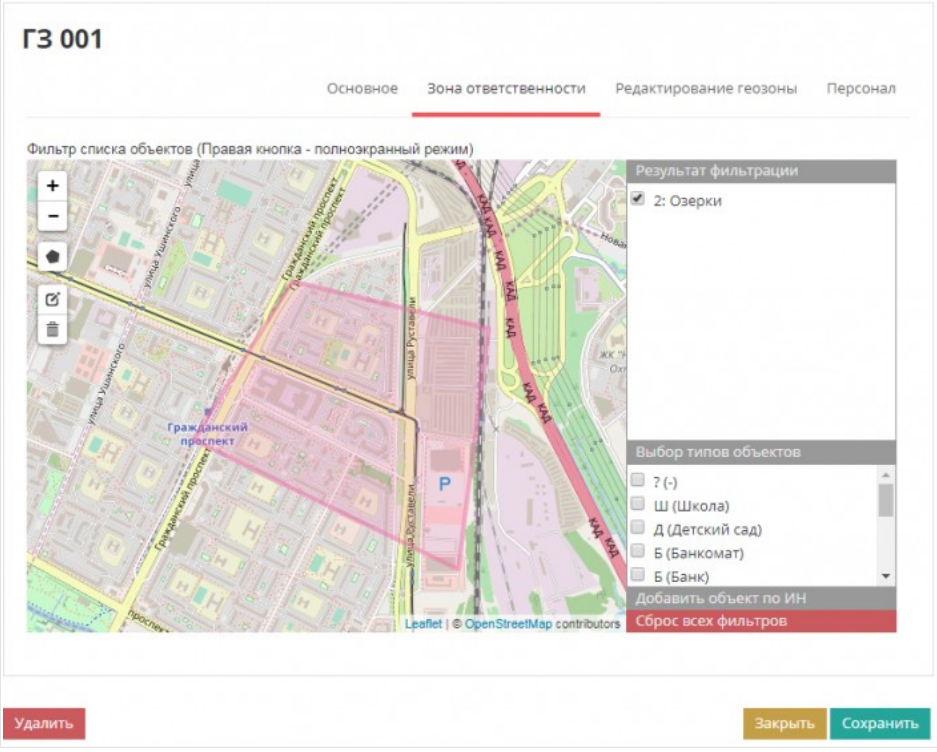


Рисунок 7.15 Зона ответственности ГЗ

4. Во вкладке "Редактирование геозоны" существует возможность установить контроль над входом и выходом ГЗ из закрепленной за ней геозоны.

Для этого необходимо отметить территорию на карте, за которой закреплена ГЗ, и установить флаги контроль входа\выхода из геозоны.

5. После настройки всех пунктов нажать «Сохранить» в нижней части окна «ГЗ». Чтобы закрыть окно «ГЗ» без сохранения, нужно щелкнуть по кнопке «Закрыть» или «Удалить» в окне «ГЗ».

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.3.2 Редактирование ГЗ

Для редактирования настроек ГЗ необходимо:

1. Нажать на кнопку (редактировать) ГЗ.
2. Внести изменения в ГЗ.
3. Нажать кнопку «Сохранить» в окне «ГЗ».

Чтобы закрыть окно учетной записи без сохранения, нажать «Закрыть» в окне «Мобильная группа».

7.3.3 Удаление ГЗ

Чтобы удалить ГЗ нужно:

1. Нажать на кнопку (редактировать) ГЗ.
2. Нажать кнопку «Удалить» в окне «ГЗ».

SEC.RU | Короткий путь к информации Скачано с sec.ru

8. Меню «Администрирование»

8.1 Система

Один сервер КРОС может работать с неограниченным количеством охранных организаций. Поэтому система администрирования логически разделена на два блока настроек - все параметры относящиеся к ядру сервера и, соответственно, работающие для всех охранных организаций, вынесены в разделы меню, доступные на уровне **Администратора сервера**, большинство из них недоступны сотрудникам отдельных организаций. Индивидуальные настройки относящиеся к охранной организации размещены в разделе параметров охранной организации и доступны сотруднику с ролью **Администратор охранной организации**.

К окну «Система» имеет доступ только **Администратор сервера**.

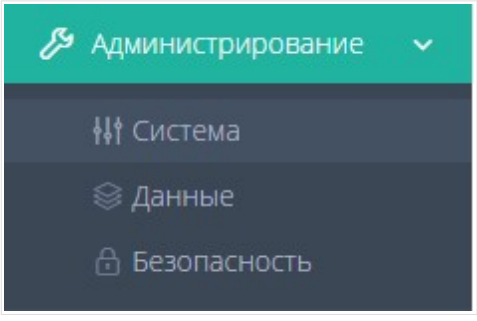


Рисунок 8.1 Меню «Система»

8.1.1 Вкладка «Сервер»

Раздел содержит основную информацию о лицензии и версии сервера КРОС.

- **Лицензия**

Информация о текущей активной лицензии, либо ее отсутствии.

- **Текущая версия сервера**

Текущая работающая версия сервера КРОС.

- **Перезагрузка**

Операция перезагрузки сервера. Эта операция перезапускает только сервис ПО КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Компьютер, на котором установлен сервер, не перезапускается.

- **Стабильная версия**

Информация о доступном обновлении стабильной версии.

- **Доступная стабильная версия**

Список доступных стабильных версий для обновления. Версию можно выбрать в списке для последующих действий.

- **Что нового**

Запрос технического списка последних изменений для выбранной версии.

- **Установить**

Запрос на обновление текущей версии сервера на выбранную. КРОС получает выбранную версию из репозитория Сервера Лицензирования, разворачивает ее и предлагает перезагрузку для активации обновлений.

ВНИМАНИЕ: При работе под ОС MS Windows обновление может пройти нестабильно, в виду того что из за особенностей файловой системы компоненты сервера, включая библиотеки и файлы ресурсов, могут быть заблокированы от записи в процессе работы КРОС.

- **Бета - версия**

Информация о доступном обновлении бета версии. Этот раздел отображается только в случае если активная лицензия КРОС имеет доступ к бета-тестированию.

- **Доступная бета версия**

Список доступных бета-версий для обновления. Версию можно выбрать в списке для последующих действий.

- **Что нового**

Запрос технического списка последних изменений для выбранной бета-версии.

- **Установить**

Запрос на обновление текущей версии сервера на выбранную. КРОС получает выбранную версию из репозитория Сервера Лицензирования, разворачивает ее и предлагает перезагрузку для активации обновлений.

SEC.RU | Короткий путь к информации Скачано с sec.ru

ВНИМАНИЕ: При работе под ОС MS Windows обновление может пройти нестабильно, в виду того что из за особенностей файловой системы компоненты сервера, включая библиотеки и файлы ресурсов, могут быть заблокированы от записи в процессе работы КРОС.

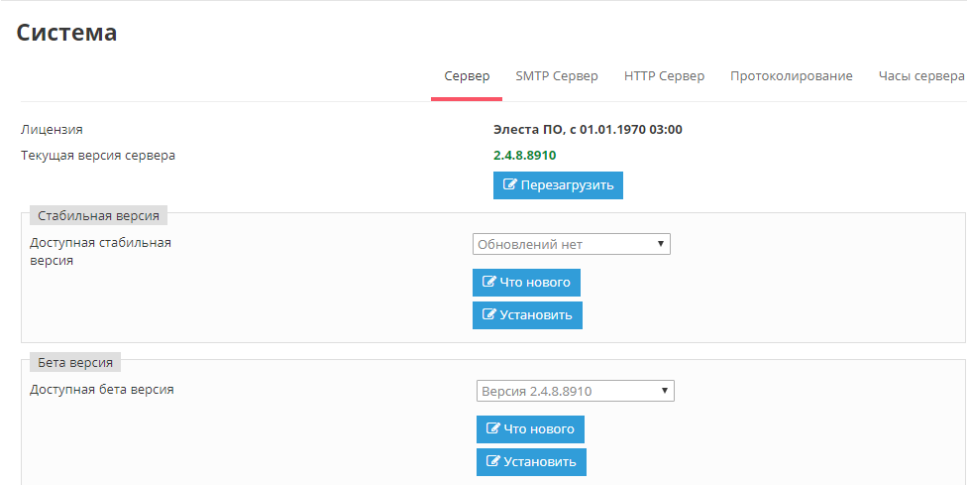


Рисунок 8.2 Вкладка «Сервер»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.1.2 Вкладка «SMTP сервер»

Во вкладке «SMTP сервер» (рисунок 8.3) производится настройка параметров для отправки сообщений через SMTP сервер.
Для настройки SMTP сервера необходимо:

1. Зайти на сервер как **Администратор сервера** (superadmin-логин и пароль по умолчанию).
2. В боковом меню выбрать Администрирование -> Система -> SMTP сервер.
3. В поле «Обратный адрес» нужно указать e-mail адрес, с которого будут приходить сообщения.
4. В поле «Кодировка сообщений» нужно указать название кодировки.
5. В поле «SMTP-сервер» указывается адрес SMTP-сервера, от которого будут приходить сообщения.

   Используйте SMTP сервер того же поставщика услуг, электронную почту которого вы указали в поле "Обратный адрес".
6. В поле «Порт» указывается порт SMTP-сервера.
7. В полях «Логин» и «Пароль» указываются логин и пароль для авторизации на SMTP-сервере.
8. Для сохранения настроек, нужно нажать кнопку «Сохранить».

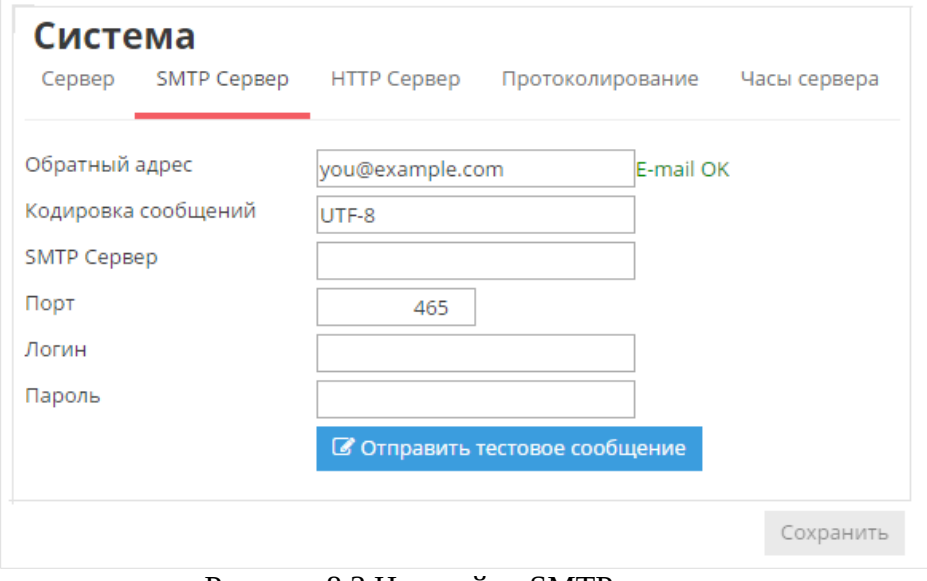


Рисунок 8.3 Настройки SMTP сервера

SEC.RU | Короткий путь к информации Скачано с sec.ru

С помощью данной функции можно получить на указанный E-mail регистрационную карту охранной организации, в которой будут указаны такие параметры, как:

- Основная информация об организации (регистрационный код, ИНН, адрес регистрации, электронная почта, номера телефонов).
- Данные о зарегистрированных пользователях (имя пользователя, роль пользователя, логин и пароль пользователя).
- Технические настройки (номера портов, необходимых для работы Юпитер-КРОС).

Для отправки регистрационной карты необходимо:

1.Зайти на сервер как Администратор сервера (superadmin-логин и пароль по умолчанию).

2.В боковом меню выбрать Охрана -> Реквизиты -> Открыть карточку охранной организации.

3.Во вкладке "Основные данные" нажать на кнопку "Отправка регистрационной карты на e-mail" (рисунок 8.4).

4.Регистрационная карта отправится на e-mail, указанный в реквизитах охранной организации.

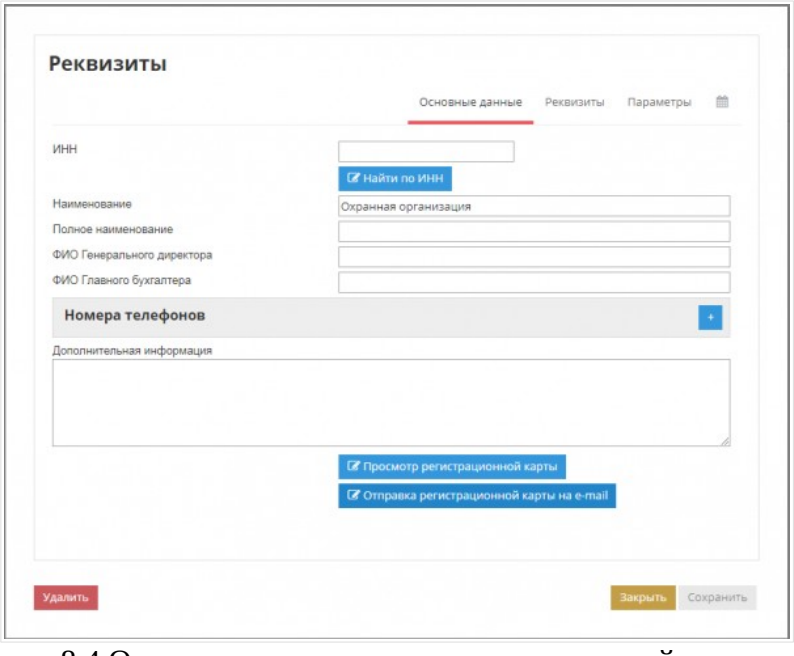


Рисунок 8.4 Основные данные в реквизитах охранной организации

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.1.3 Вкладка «HTTP сервер»

HTTP и HTTPS сервер является неотъемлемой частью сервера КРОС и используется для построения WEB-интерфейсов системы администрирования

Таким образом настройки приведенные ниже влияют на всю систему администрирования а также на функционал всех драйверов, работающих через HTTP/HTTPS.

Адресом КРОС для доступа по HTTP/HTTPS может является внешний статический IP адрес или доменное имя, либо локальный сетевой адрес. Можно получить доступ к КРОС с того же компьютера, где он установлен, используя адрес 127.0.0.1 или localhost с портом по умолчанию 9900.

Во вкладке «HTTP сервер» (рисунок 8.5) происходит настройка параметров http-сервера.

Разрешить HTTP сервер
Разрешить работу HTTP сервера как неотъемлемой части КРОС. HTTP сервер будет запущен при старте КРОС.

Разрешить HTTPS сервер
Разрешить работу HTTPS сервера как неотъемлемой части КРОС. HTTPS сервер будет запущен при старте КРОС.

В строке «HTTP Порт» указывается номер порта TCP по которому WEB интерфейс КРОС и API HTTP драйверов будет доступны по протоколу HTTP.

В строке «HTTPS Порт» указывается номер порта TCP по которому WEB интерфейс КРОС и API HTTP драйверов будет доступны по протоколу HTTPS.

Для сохранения изменений нужно нажать кнопку «Сохранить».

SEC.RU | Короткий путь к информации Скачано с sec.ru

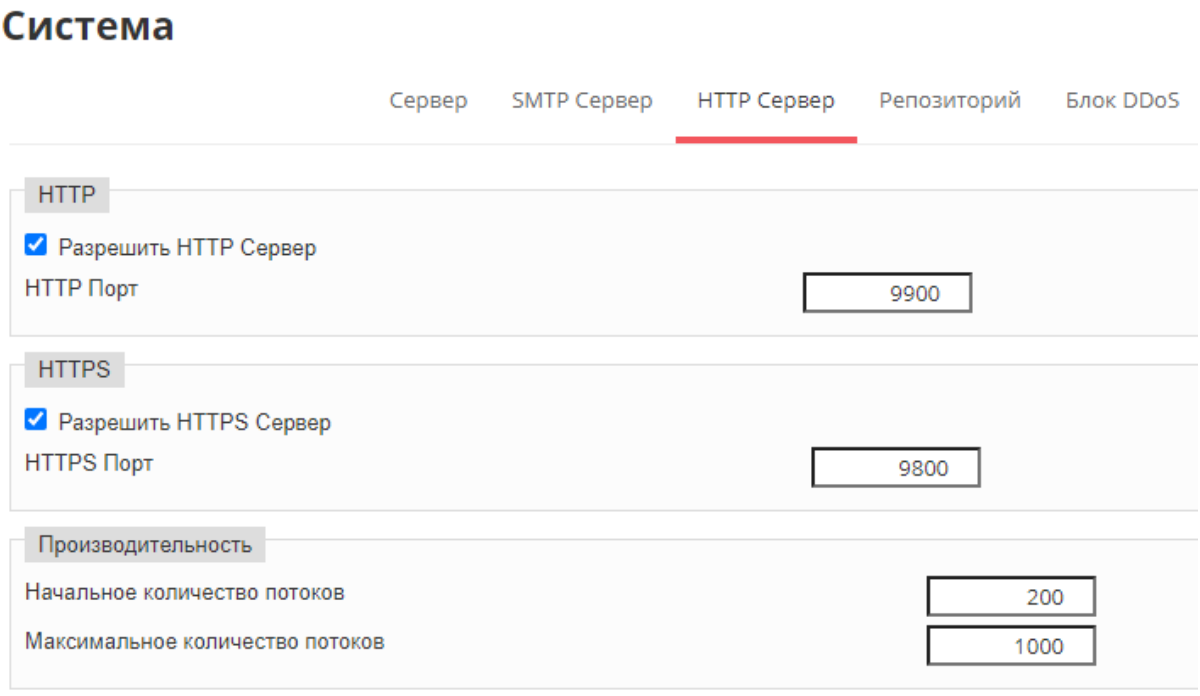


Рисунок 8.5 Вкладка «HTTP сервер»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.1.4 Вкладка «Протоколирование»

На сервере предусмотрено создание лог файлов как самого сервера, так и всех его драйверов. Во вкладке «Протоколирование» (рисунок 8.6) имеется возможность задать параметры работы с логами:

- **Разрешить протоколирование**

Если отключить этот параметр лог-файлы записываться не будут.

- Максимальный размер файла протокола (всегда записывается в байтах)

  При достижении указанного размера, лог-файл будет скопирован в текущий каталог с

  архивным именем (*.log.1, .log.2, и т.д.), текущий лог будет очищен, запись лога начнется в чистый файл.

- Ограничение количества файлов протокола

  Максимальное количество хранимых архивных файлов. При превышении указанного количества будет удален самый старый архивный лог-файл.

- **Путь для хранения файлов протокола**
  Подкаталог для хранения лог-файлов. Может быть путь в локальной сети.

- **Шаблон записи протокола**
  Формат строки лог-файла. По умолчанию - %d [%5p] %X{context}: %m %n

  - %d - дата и время
  - %5p - тип записи с выравниванием в 5 символов (INFO,DEBUG,WARN,ERROR)
  - %X{context} - контекст записи
  - %m - сообщение
  - %n - перевод строки

По умолчанию лог файлы сохраняются на сервере в папке ...\smpo-server\logs.

SEC.RU | Короткий путь к информации Скачано с sec.ru

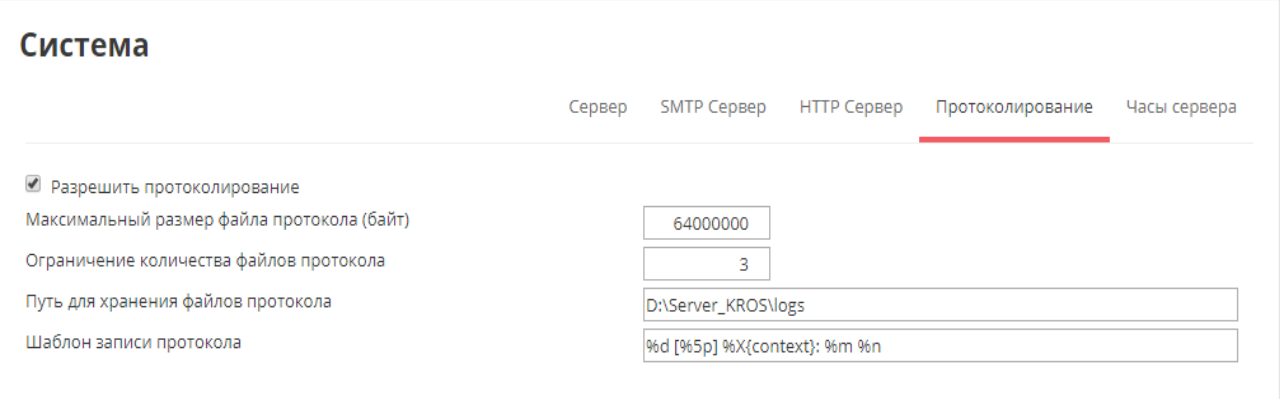


Рисунок 8.6 Вкладка «Протоколирование»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.1.5 Вкладка «Часы сервера»

Часы сервера работают в независимом от настроек базового компьютера часовом поясе UTC и, поскольку КРОС взаимодействует с множеством внешних источников, в том числе вероятно находящихся в разных часовых поясах, и в связи негарантированной точности системных часов базового компьютера, требует периодической коррекции времени с синхронизацией по “атомным” часам. Для этого используется стандартный NTP протокол.

- Разрешить синхронизацию времени

  Включить периодическую синхронизацию времени КРОС по протоколу NTP.

- **Синхронизировать часы сервера перед стартом**
  Синхронизировать внутренние часы КРОС перед началом любых взаимодействий с внешними источниками и приемниками данных.

- **Период синхронизации (сек)**
  Продолжительность периода времени между синхронизациями.

- **Список серверов времени**
  Используемые для синхронизации NTP серверы, перечисленные через запятую.

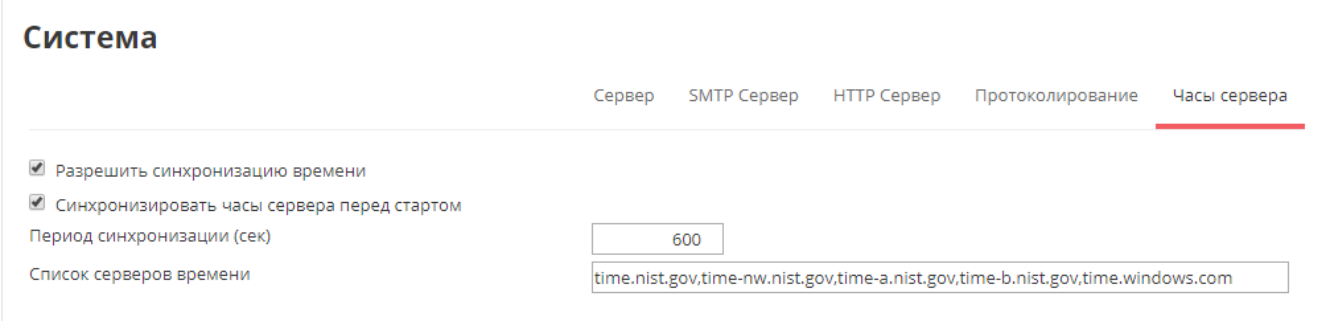


Рисунок 8.7 Часы сервера

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.1.6 Вкладка «Блок DDOS»

КРОС содержит базовый функционал для обнаружения DDoS атак и временной блокировки их источников. Система обработки входящих соединений контролирует и фиксирует для каждого адреса отправителя количество пакетов, не обработанных ни одним из драйверов-приемников. Если это количество превысит установленный лимит - данные от зафиксированного адреса перестают приниматься установленный период времени.

- **Разрешить обнаружение DDoS атак и блокировку их источников**

  Активация системы базовой защиты от DDoS атак.

- **Количество подозрительных соединений до момента блокировки адреса источника**

  Количество соединений от одного адреса не обработанных ни одним из драйверов приемников, при достижении которого адрес источника будет заблокирован.

- **Продолжительность блокировки адреса источника атаки (мин) -**

  Период времени, в течение которого все попытки соединения с заблокированного адреса будут отвергаться.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.1.7 Вкладка «Репозиторий»

В случае работы КРОС в изолированной среде для обновления прошивки приборов можно использовать локальный репозиторий. Для этого необходимо создать по указанному пути копию онлайн репозитория прошивок и убедиться что HTTP порт, указанный в настройках HTTP сервера, доступен для приборов. Копия онлайн-репозитория доступна по индивидуальному запросу к производителю оборудования.

●Использовать локальный репозиторий

По умолчанию обновление прошивки приборов происходит с использованием онлайн-репозитория, в настоящее время находящегося по адресу http://download.elesta.ru/firmware. Параметр активирует использование локального репозитория, при этом к онлайн-репозиторию обращений не происходит.

●Путь к каталогу содержащему репозиторий прошивок

Полный путь к репозиторию. По умолчанию это папка firmware автоматически создаваемая в основном каталоге установки КРОС. В случае если репозиторий расположен в другом месте - можно указать другой путь.

●IP адрес для локальных обновлений

Адрес сервера КРОС в общей с приборами сети. По этому адресу прибор будет обращаться к локальному репозиторию для запроса обновлений. Может отличаться от внешнего статического IP-адреса сервера КРОС в случае работы приборов через VPN, прокси-сервер или в локальной сети. В общем случае здесь нужно указать адрес используемый в настройках IP соединения приборов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.2 Данные

Во вкладке «Данные» (меню «Административные»→«Данные») (рисунок 8.8) производится настройка базы данных.

К окну «Базы данных» имеет доступ только **Администратор сервера**.

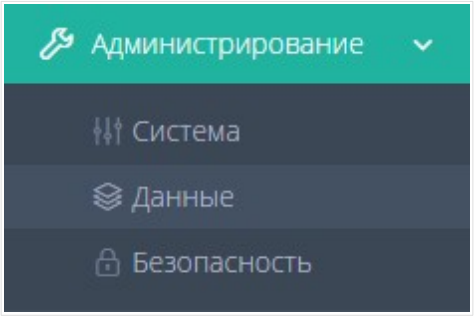


Рисунок 8.8 Меню «Данные»

8.2.1 Вкладка «SQL сервер»

Во вкладке «SQL Сервер» (рисунок 8.9) производятся настройки доступа к серверу баз данных. После изменения параметров сервер КРОС требует обязательной перезагрузки. Предполагается работа с сервером PostgreSQL.

Примечание:

По умолчанию при установке сервера данная вкладка заполнена автоматически и не требует дополнительной настройки. Настройка требуется только в частных случаях, как, например, иные имя пользователя или пароль PostgreSQL либо если вам требуется название базы данных, отличное от стандартного.

- **Адрес сервера**
  IP адрес или доменное имя сервера SQL. По умолчанию используется порт 5432. Если необходимо использовать другой порт - лг указывается через двоеточие, например localhost:5433.
- **Имя базы данных**
  Основная база данных КРОС. По умолчанию jupiter.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Имя схемы**
  Схема в контексте базы данных PostgreSQL. По умолчанию используется public,

  поэтому имя схемы можно не указывать.

- **Имя пользователя**
  Имя пользователя для доступа к базе данных в контексте SQL Сервера.

- **Пароль**
  Пароль для доступа к базе данных в контексте SQL Сервера.

  Для сохранения изменений, нужно нажать на кнопку «Сохранить».

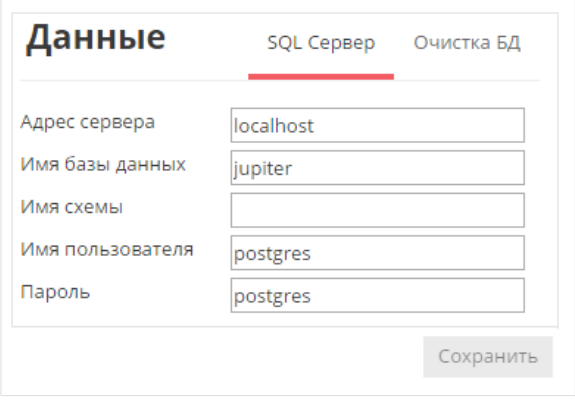


Рисунок 8.9 Вкладка SQL сервер

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.2.2 Вкладка «Резервирование»

8.2.2.1 Создание резервной копии

Данная вкладка предназначена для создания резервных копий сервера и базы данных, а также восстановления из резервных копий при аварии.

Полное резервирование базы данных КРОС осуществляется на системном уровне, для чего используются инструменты входящие в состав установленного сервера PostgreSQL - pg_dump и pg_restore.

Создание резервных копий возможно как вручную, так и в автоматическом режиме. Для создания резервной копии необходимо:

Следует различать резервную копию базы данных и версии сервера.
Резервная копия базы данных - это бэкап именно базы данных (договоров, объектов, приборов, учетных записей и т.д.). Не сохраняет версию сервера.
Резервная копия версии сервера - это бэкап исполняющих файлов, отвечающих за работу сервера КРОС в целом, в том числе и за версию сервера. Не сохраняет данные (договора, объекты, приборы и т.д).

1. Зайти на Сервер-КРОС под учетной записью Администратор сервера (по умолчанию логин и пароль superadmin).
2. Перейти в меню Администрирование ---> Данные ---> Резервирование БД (рисунок 8.10).
3. Во вкладке "Резервирование" доступно два варианта создания резервной копии.

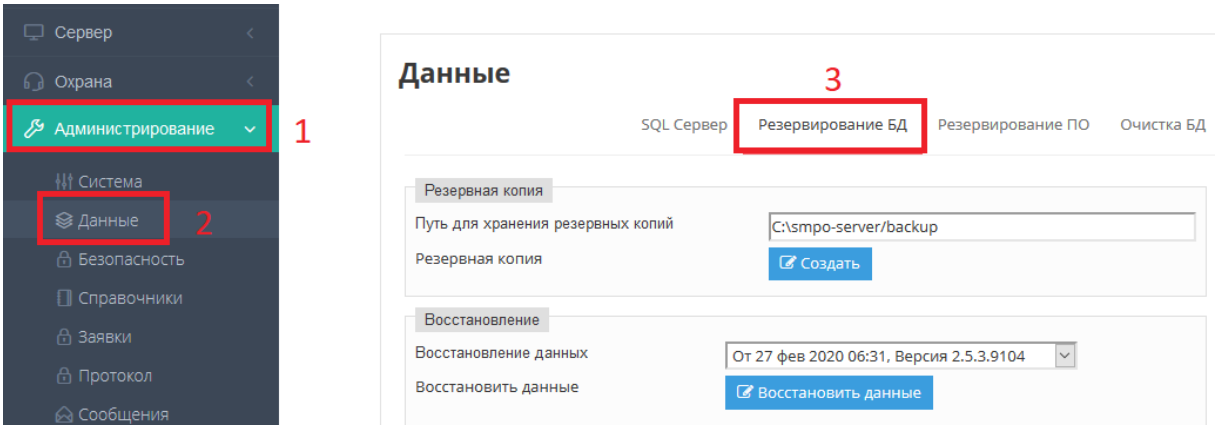


Рисунок 8.10 Вкладка «Резервирование БД»

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Создание резервной копии вручную:**

Для создания резервной копии вручную требуется:

1. Задать путь для хранения резервных копий, либо оставить установленный по умолчанию. Если задаете свой путь для хранения, то после ввода пути необходимо нажать кнопку "Сохранить".

   Здесь можно указать несколько путей на разных носителях и сетевых ресурсах, разделенные запятой, при этом резервные файлы при создании будут продублированы в каждый из указанных каталогов. Для восстановления средствами КРОС будет всегда использоваться только самый первый путь в списке.

2. Нажать кнопку "Создать" (рисунок 8.11).

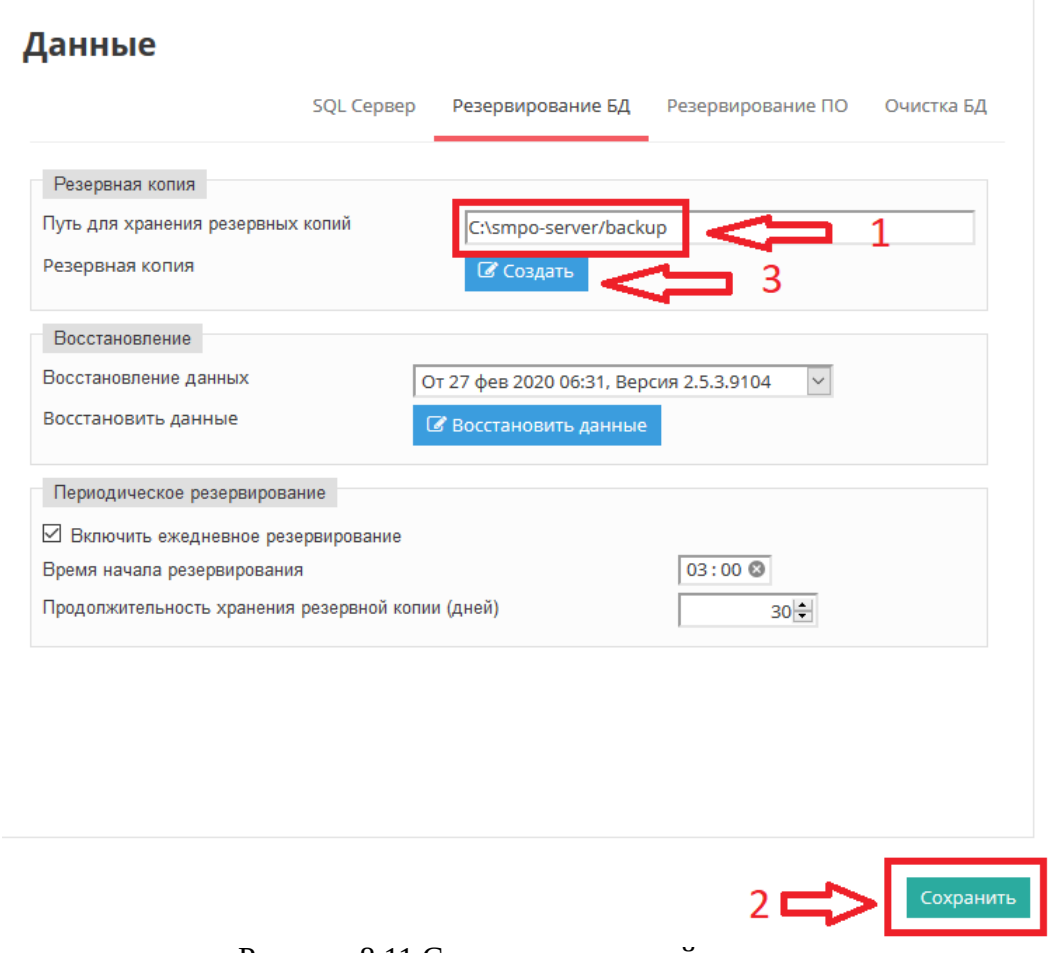


Рисунок 8.11 Создание резервной копии вручную

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Создание резервной копии в автоматическом режиме:**

Для создания резервной копии в автоматическом нужно:

1. Задать путь для хранения резервных копий, либо оставить установленный по умолчанию.
2. Установить галочку "Включить ежедневное резервирование".
3. Выбрать время начала резервирования. Рекомендуется выбрать такое время, когда нагрузка на систему минимальна.
4. Выбрать продолжительность хранения резервной копии. По умолчанию время хранения составляет 1 месяц.
5. После выставления всех настроек нажать кнопку "Сохранить". После этого резервные копии начнут создаваться согласно установленным настройкам (рисунок 8.12).

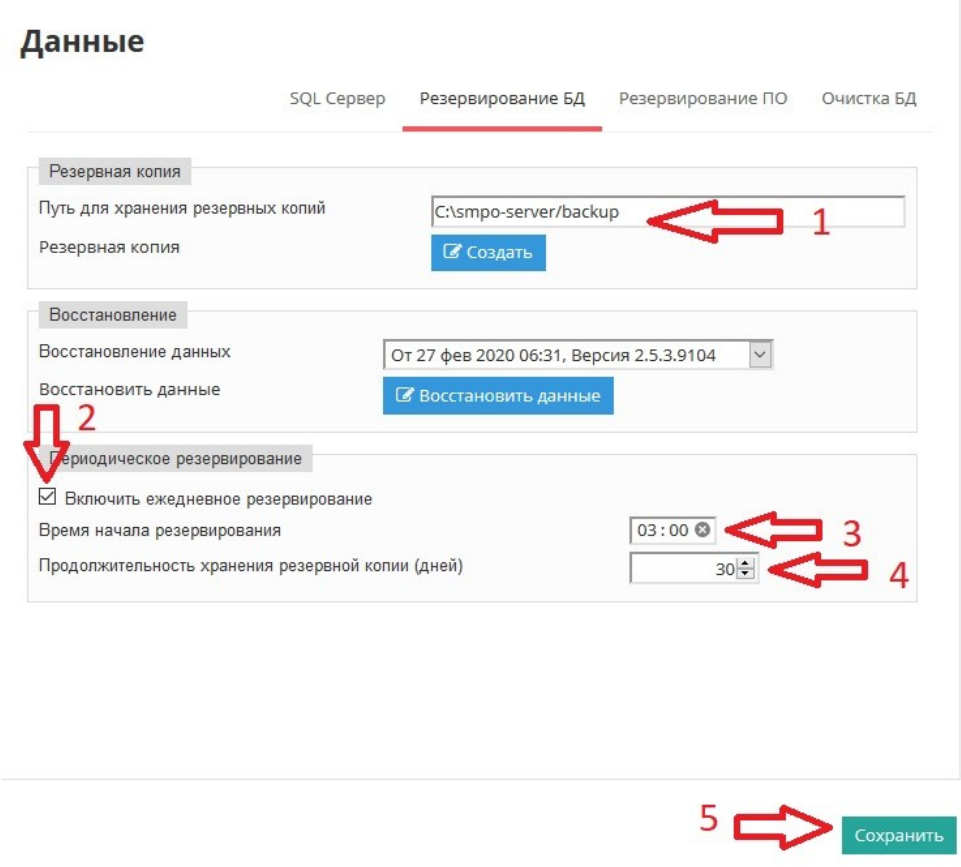


Рисунок 8.12 Создание резервной копии в автоматическом режиме

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Создание резервной копии версии сервера**

Перед обновлениями версии сервера КРОС рекомендуется делать резервную копию папки с сервером, чтобы в случае неуспешного обновления можно было подменить файлы, и запустить старую работавшую до обновления версию.

Сделать это проще всего запустив файловый менеджер от имени суперпользователя и выполнил архивирование папки по адресу /usr/local/smpo-server.

Для этого (на примере Astra Linux):

1. Необходимо открыть терминал.

2. Ввести команду sudo fly-fm . Будет открыт файловый менеджер под правами суперпользователя.

3. Проследовать в папку /usr/local/

4. В папке /usr/local/ найти папку под названием smpo-server.

5. Нажать на папку smpo-server правой кнопкой мыши, выбрать пункт "Упаковать", далее в выпадающем меню выбрать "Как архив zip". Будет создан архив smpo-server.zip

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.2.2.2 Восстановление из резервной копии

Для восстановления из резервной копии необходимо (рисунок 8.13):

1. Выбрать нужную резервную копию из списка (пункт 1 на рисунке ниже).

Внимание! Если вы, например, полностью переустановили сервер, и вам нужно восстановить резервную копию, то для того, чтобы список копий появился в меню необходимо положить архивы с копиями в папку, которая прописана у вас как путь для хранения резервных копий, и обновить страницу в браузере.

3. Нажать на кнопку "Восстановить данные". Запустится процесс восстановления. После успешного восстановления базы данных сервер будет автоматически запущен.

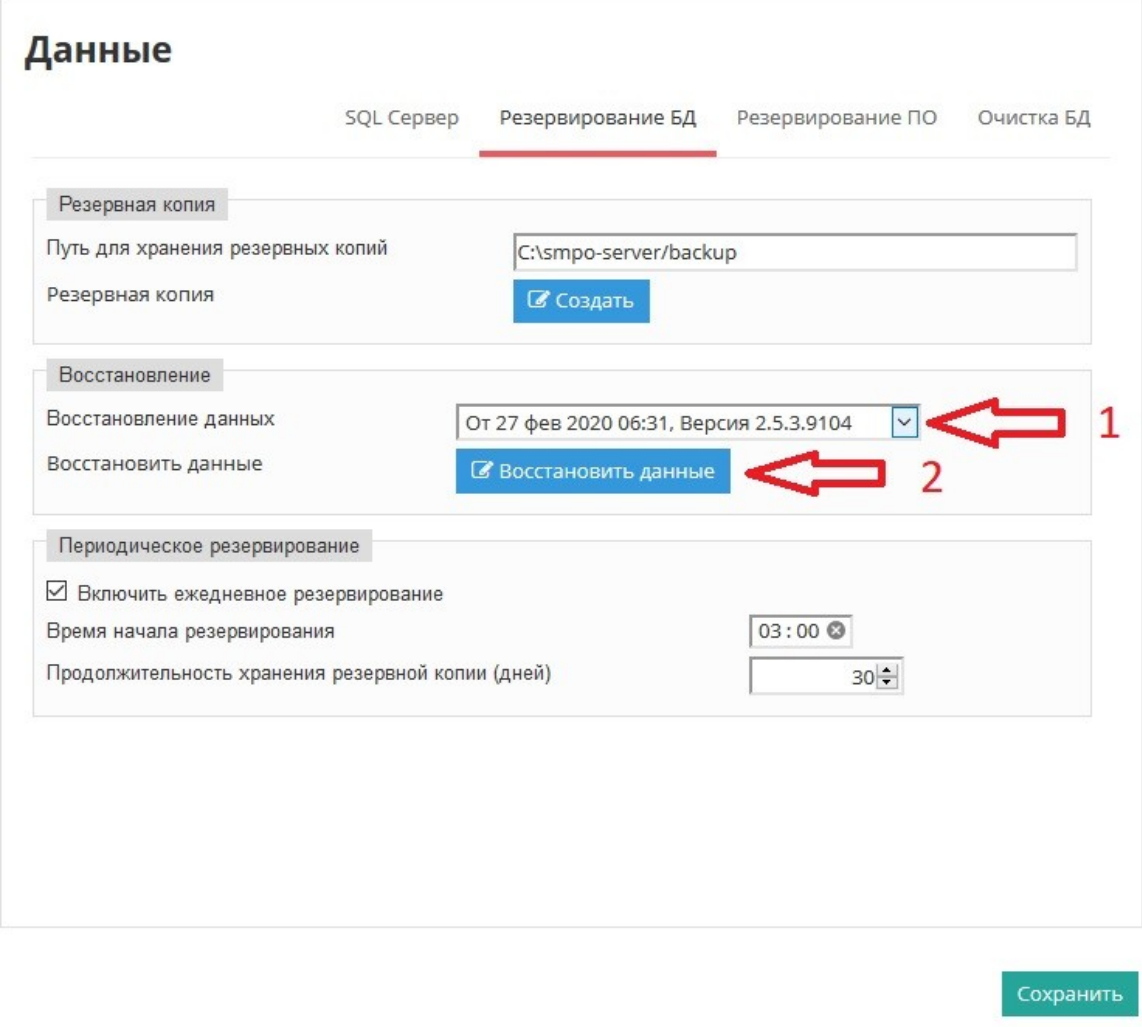


Рисунок 8.13 Восстановление из резервной копии

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Восстановление резервной версии версии сервера**

Для восстановления версии сервера из резервной копии требуется (на примере Astra Linux):

1. Необходимо открыть терминал.

2. Ввести команду sudo fly-fm . Будет открыт файловый менеджер под правами суперпользователя.

3. Проследовать в папку /usr/local/

4. В папке /usr/local/ найти архив под названием smpo-server.zip

5. Правой кнопкой мыши щелкнуть по архиву, выбрать "Распаковать", далее "Распаковать в эту папку". Файлы будут заменены.

Пути и названия папок и архивов могут отличаться в зависимости от ваших установок и предпочтений, здесь описан лишь алгоритм действий для восстановления.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.2.3 Вкладка «Очистка БД»

КРОС работает с большими объемами данных. Лента сообщений, протокол событий, очередь трансляций могут создавать большие массивы хранимых данных, которые рано или поздно могут заполнить весь носитель, на котором расположена база данных. Кроме того превышение объема оперативных данных свыше необходимого приводит к замедлению работы системы. Чтобы избежать этого в системе предусмотрено периодическое автоматическое удаление устаревших данных.

Происходит очистка обработанного архива сообщений и очереди на отправку в трансляциях. Автоматизация учитывает необходимый минимум для каждого из объектов в 1000 последних событий. Эти события остаются в БД и не удаляются несмотря на уставленную периодичность очистки системы (рисунок 8.14).

- **Разрешить периодическую очистку данных**
  Dключение и отключение системы автоматической очистки.
- **Период хранения оперативных данных (минут)**
  Оперативными данными считается лента событий по всем объектам. В независимости от настройки периодичности очистки БД оперативные данные будут оставлены.
- **Периодичность запуска системы очистки**
  Возможность задать период (1 час, 3 часа, 12 часов, ежедневно, раз в три дня, еженедельно). Для еженедельной очистки устанавливается день недели, в который производится очистка данных.
- **Время запуска (ЧЧ:ММ)**
  Системное время на сервере для начала процесса удаления данных.

Примечание: Важно учитывать время не только удаления данных, но и создания резервных копий. Настоятельно не рекомендуется совмещать их по времени или задавать им близкий временной интервал.

SEC.RU | Короткий путь к информации Скачано с sec.ru

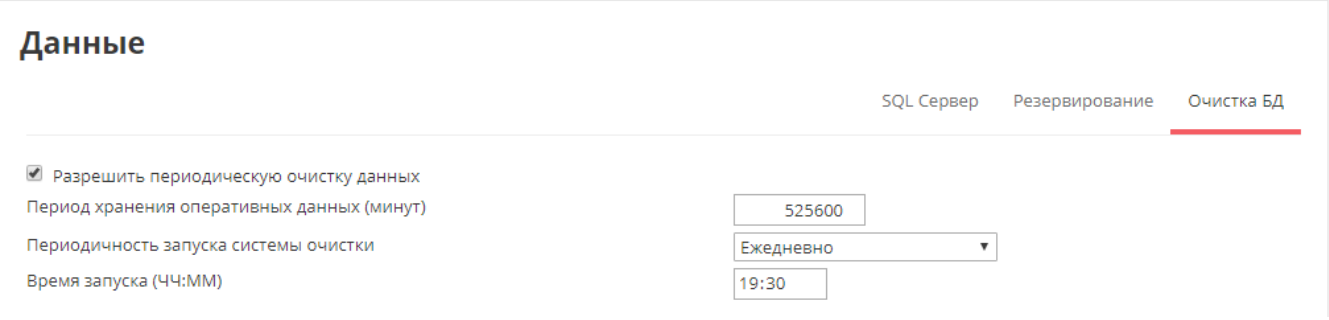


Рисунок 8.14 Настройка очистки базы данных

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3 Безопасность

Доступ к ресурсам системы КРОС определяются параметрами учетной записи. Учетная запись по сути является фактом регистрации в системе сотрудника организации. Для каждой охранной организации может быть зарегистрировано неограниченное количество учетных записей.

В системе может быть только одна учетная запись Администратора сервера, определяемая на уровне системных настроек. Администратор сервера имеет доступ ко всем системным ресурсам сервера. Администратор сервера не имеет доступа к оперативным данным охранной организации. Ему доступен только список пользователей, имеющих роль Администратора охранной организации.

Для определения прав доступа в КРОС существует система Ролей . Каждая роль может содержать определенный набор прав доступа. Каждый пользователь охранной организации может иметь одну или несколько ролей. Новые роли могут быть введены в системе КРОС только Администратором сервера.

К окну «Безопасность» (рисунок 8.15) имеет доступ только **Администратор сервера**.

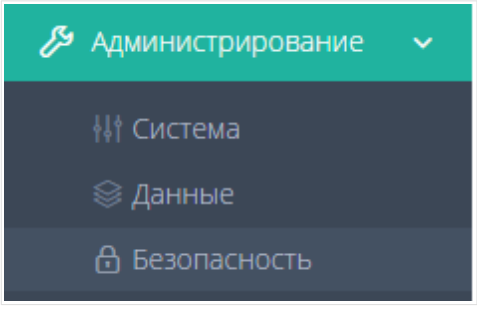


Рисунок 8.15 Меню «Безопасность»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3.1 Вкладка «Роли»

Во вкладке «Роли» (рисунок 8.16) создаются, настраиваются и удаляются роли.

Для создания или редактирования роли необходимо:

- Зайти на сервер под учетной записью **Администратора сервера** (Superadmin - пароль и логин по умолчанию).
- Выбрать в меню пункт Администрирование ---> Безопасность ---> Роли.
- Для создания новой роли необходимо нажать на кнопку (добавить), ввести имя роли и выставить разрешения для роли.
- Для сохранения новой роли необходимо нажать кнопку (сохранить).
- Для редактирования уже существующей роли необходимо выбрать роль и отредактировать необходимые параметры.
- Для удаления роли необходимо нажать на кнопку (удалить).

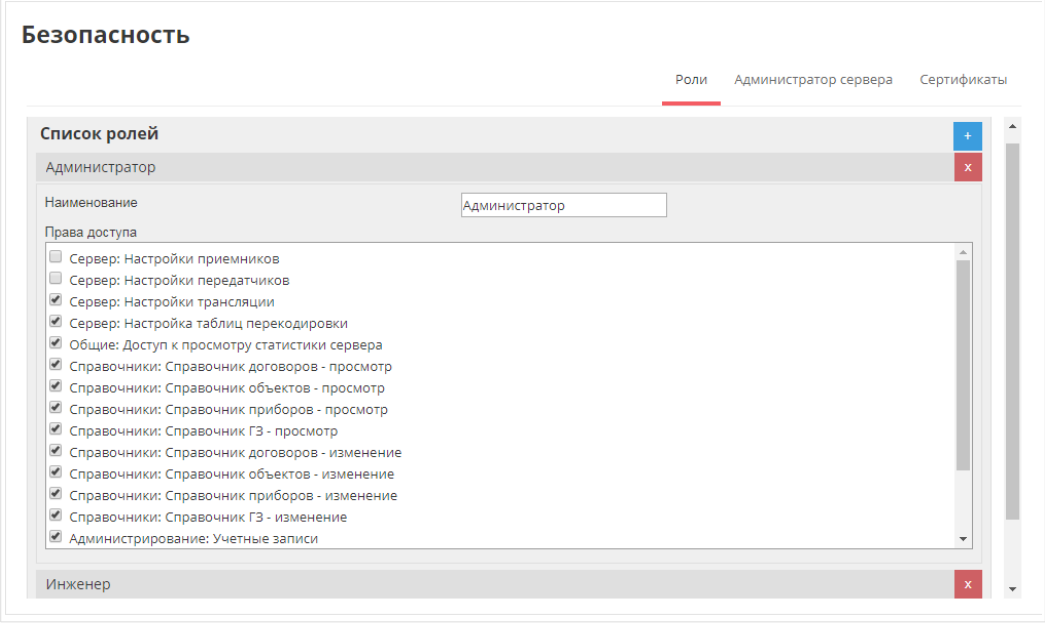


Рисунок 8.16 Вкладка «Роли»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3.1.1 Добавление новой роли

Чтобы добавить новую роль нужно:

1. Нажать на кнопку (добавить).

2. Подтвердить создание новой записи.

3. В поле «Наименование» ввести название новой роли.

4. Распределить права доступа, отмечая флагами разделы, которые станут доступны для новой роли.

5. Нажать на кнопку (Сохранить).

8.3.1.2 Редактирование роли

Чтобы внести изменение в роль нужно:

1. Щелкнуть по надписи с названием роли.

2. Внести в роль изменения (Изменить «Наименование», перераспределить права доступа).

3. Нажать на кнопку (Сохранить).

8.3.1.3 Удаление роли

Чтобы удалить роль нужно нажать на кнопку (удалить) и подтвердить удаление.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3.1.4 Описание прав доступа

- **Сервер: Настройки приемников**
  Доступ к списку драйверов приемников и возможность редактировать их параметры.

  Меню: Сервер -> Приемники.

- **Сервер: Настройки передатчиков**
  Доступ к списку драйверов передатчиков и возможность редактировать их параметры.

  Меню: Сервер -> Передатчики.

- **Сервер: Настройки трансляции**
  Доступ к списку трансляций и возможность их создавать, удалять и редактировать их

  параметры. Меню: Сервер -> Трансляции.

- **Сервер: Настройка таблиц перекодировки**
  Доступ к списку таблиц перекодировки и возможность их создавать, удалять и

  редактировать. Меню: Сервер -> Таблицы.

- **Общие: Доступ к просмотру статистики сервера**
  Право просмотра статистики сервера и мониторинга его работы. Меню: Главная.

- **Справочники: Справочник договоров - просмотр**
  Право просмотра списка и карточек договоров, без возможности добавлять,

  редактировать и удалять. Меню: Клиенты -> Договоры.

- **Справочники: Справочник объектов - просмотр**
  Право просмотра списка и карточек объектов, без возможности добавлять,

  редактировать и удалять. Меню: Клиенты -> Объекты.

- **Справочники: Справочник приборов - просмотр**
  Право просмотра списка и карточек договоров, без возможности добавлять,

  редактировать и удалять. Меню: Клиенты -> Приборы.

- **Справочники: Справочник ГЗ - просмотр**

SEC.RU | Короткий путь к информации Скачано с sec.ru

Право просмотра списка и карточек Групп Задержания (ГЗ), без возможности добавлять, редактировать и удалять. Меню: Охрана -> ГЗ.

- **Справочники: Справочник Ответств. лиц - просмотр**
  Право просмотра общего списка и карточек Ответственных лиц, без возможности добавлять, редактировать и удалять. Меню: Клиенты - Ответственные лица.

- **Справочники: Справочник договоров - изменение**
  Право просмотра, добавления, удаления и редактирования списка и карточек договоров. Меню: Клиенты -> Договоры.

- **Справочники: Справочник объектов - изменение**
  Право просмотра, добавления, удаления и редактирования списка и карточек объектов. Меню: Клиенты -> Объекты.

- **Справочники: Справочник приборов - изменение**
  Право просмотра, добавления, удаления и редактирования списка и карточек приборов. Меню: Клиенты -> Приборы.

- **Справочники: Справочник ГЗ - изменение**
  Право просмотра, добавления, удаления и редактирования списка и карточек Групп Задержания (ГЗ). Меню: Охрана -> ГЗ

- **Справочники: Справочник Ответств. лиц - изменение**
  Право просмотра, и редактирования общего списка и карточек Ответственных лиц. Меню: Клиенты - Ответственные лица.

- **Администрирование: Учетные записи**
  Доступ к списку учетных записей организации, с возможностью удаления, добавления и редактирования. Меню: Охрана -> Учетные записи.

- **Администрирование: Инженерный режим**
  Определяет доступ к информации о приборах, находящихся в инженерном режиме, в

SEC.RU | Короткий путь к информации Скачано с sec.ru

том числе просмотр и редактирование их параметров, получение ленты событий, отправка команд.

- **Администрирование: Режим администратора**
  Наделяет пользователя дополнительными правами для доступа к системным настройкам в контексте охранной организации.

- **Администрирование: Режим дежурного инкассатора**
  Специфическая настройка прав доступа к интерфейсу дежурного инкассатора, предназначена только для использования совместно с подключенным сервисом инкассации.

- **Клиенты: Просмотр протоколов работы пользователей**
  Право просмотра протокола работы системы КРОС. Меню: Администрирование -> Протокол.

- **Клиенты: Отправка сообщений через АПИ**
  Определяет право создавать сообщения и события средствами HTTP/JSON API. Предназначено для отладочных целей.

- **Клиенты: Отправка команд на прибор через АПИ**
  Определяет право управлять приборами средствами API посредством отправки команд.

- **Клиенты: Разрешение взятия/снятия**
  Разрешение работает только в случае наличия права отправлять команды на прибор средствами АПИ. Определяет право ставить прибор на охрану и снимать с охраны.

- **Клиенты: Конструктор отчетов**
  Доступ к генератору отчетов, в данный момент представлен в виде бета-версии.

- **Клиенты: Разрешение постановки на прогон**
  Позволяет регулировать разрешение постановки \ снятия объекта на прогон.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3.2 Вкладка «Администратор сервера»

Во вкладке «Администратор сервера» (рисунок 8.17) происходит настройка учетной записи **Администратора сервера**.

В поле «Имя пользователя» задается имя Администратора сервера.

В поле «Логин» задается логин для входа как Администратор сервера.

В поле «Новый пароль» задается новый пароль, заменяющий старый, для входа как Администратор сервера.

Примечание: В случае потери измененного пароля, для восстановления доступа к учетной записи Администратора сервера необходимо обратиться в службу технической поддержки представительства ООО «Элеста».

В выпадающем меню «Часовой пояс» определяется часовой пояс в котором находится сервер.

Для сохранения изменений, нужно нажать на кнопку «Сохранить».

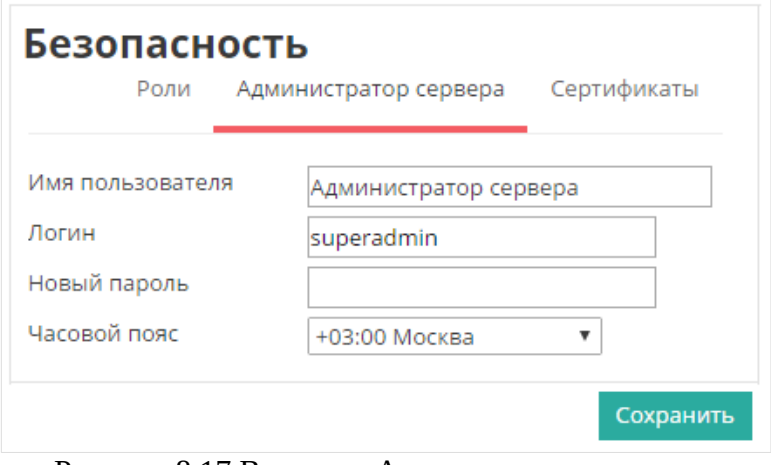


Рисунок 8.17 Вкладка «Администратор сервера»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3.3 Вкладка «Сертификаты»

КРОС использует протоколы HTTPS и шифрованные TCP/SSL соединения, для обеспечения которых требуется SSL сертификат. По умолчанию в дистрибутив КРОС входит самоподписанный сертификат, однако в систему может быть установлен контролируемый сертификат, который должен быть помещен в jks хранилище средствами java (см. http://java-online.ru/keystore-keytool.xhtml)

- Путь к хранилищу ключей

  Полный путь к контейнеру jks, содержащему SSL сертификаты.
- Пароль хранилища

  Пароль для хранилища.
- Пароль ключа

  Пароль для сертификата.

Для сохранения изменений, нужно нажать на кнопку «Сохранить».

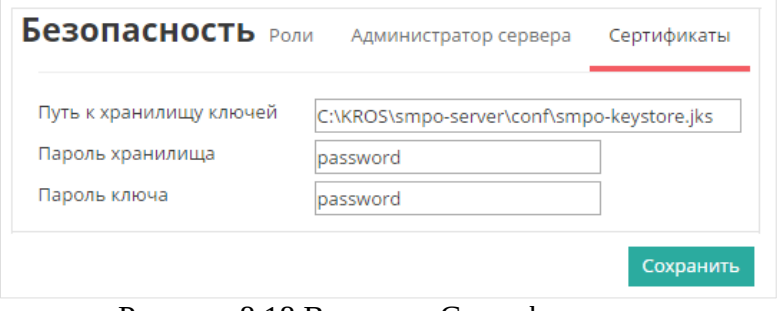


Рисунок 8.18 Вкладка «Сертификаты»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.4 Заявки

Функциональность сервера КРОС позволяет использовать сервер больше чем для одной охранной организации.
По умолчанию при первом запуске сервера создается одна охранная организация, но **Администратор сервера** может создавать новые охранные организации.
Для создания новой охранной организации требуется:

1. Создать заявку (рисунок 8.19).

Заявка на регистрацию охранной организации создается в интерфейсе авторизации.

Требуется выйти на страницу авторизации по адресу

http://localhost:9900

или

http://192.168.1.13:9900

192.168.1.13 - IP компьютера, на котором установлен сервер.

и нажать кнопку "Зарегистрировать ОО".

2. Заполнить появившеюся форму регистрации и нажать кнопку "Отправить заявку".

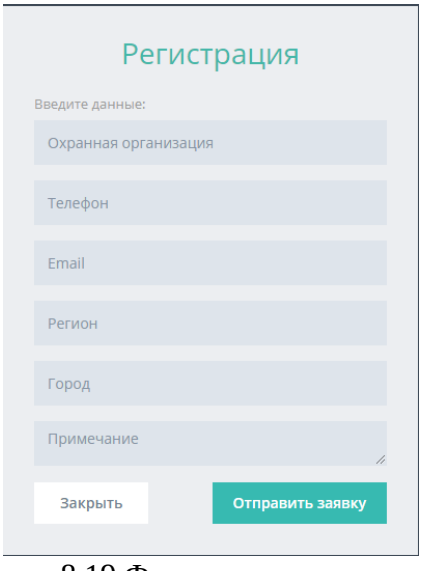


Рисунок 8.19 Форма регистрации заявки

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Принять заявку.

Для приема заявки необходимо зайти на сервер под учетной записью **Администратор сервера** (superadmin - логин и пароль по умолчанию), после чего зайти в меню Администрирование ---> Заявки. Там будет находиться новая заявка (рисунок 8.20).

Рисунок 8.20 Прием заявки

4. Зарегистрировать предприятие

Для регистрации нажмите синюю кнопку (пункт 3 на рисунке выше).
В появившемся окне необходимо принять заявку и нажать кнопку "Зарегистрировать предприятие" (рисунок 8.21).

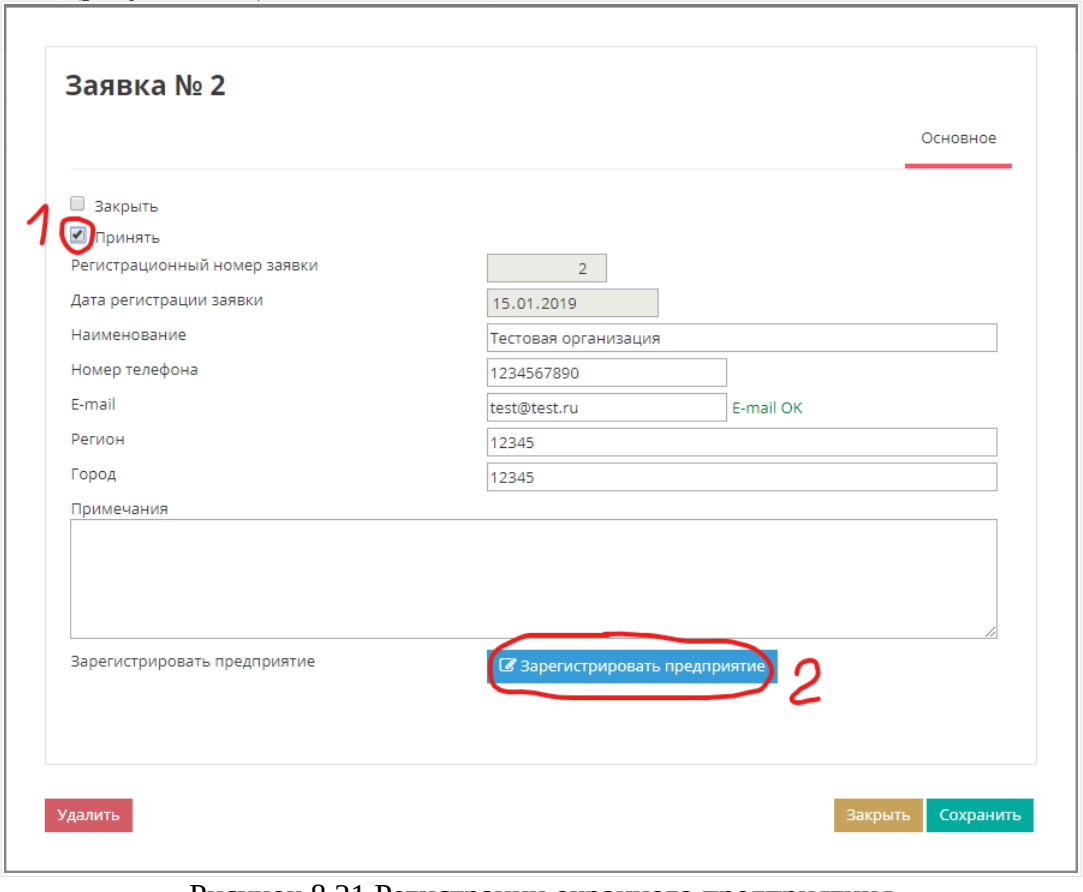


Рисунок 8.21 Регистрации охранного предприятния

5.Реквизиты организации

SEC.RU | Короткий путь к информации Скачано с sec.ru

В новом появившемся окне необходимо ввести реквизиты охранной организации и основную информацию, после чего нажать кнопку "Сохранить".

Также в этом окне есть возможность отправить на e-mail регистрационную карту нового охранного предприятия, в которой будет содержаться информация об учетных записях и портах, выделенных новой охранной организации.

8.5 Протокол

Во вкладке "Протокол" (рисунок 8.22) отображаются все события, произошедшие на сервере и в АРМ.

В протоколе указаны:

- Дата и время события
- Источник события
- Логин пользователя, вызвавшего событие
- Описание произошедшего события

В верхнем правом углу страницы отображается общее количество событий, а также же строка поиска и меню, в котором можно выбрать временной период, отображаемый в протоколе (сутки, неделя, месяц или три месяца)

Изначально право просмотра протокола есть у учетных записей admin и superadmin, однако права доступа к протоколу можно поменять во вкладке "Администрирование-Безопасность"

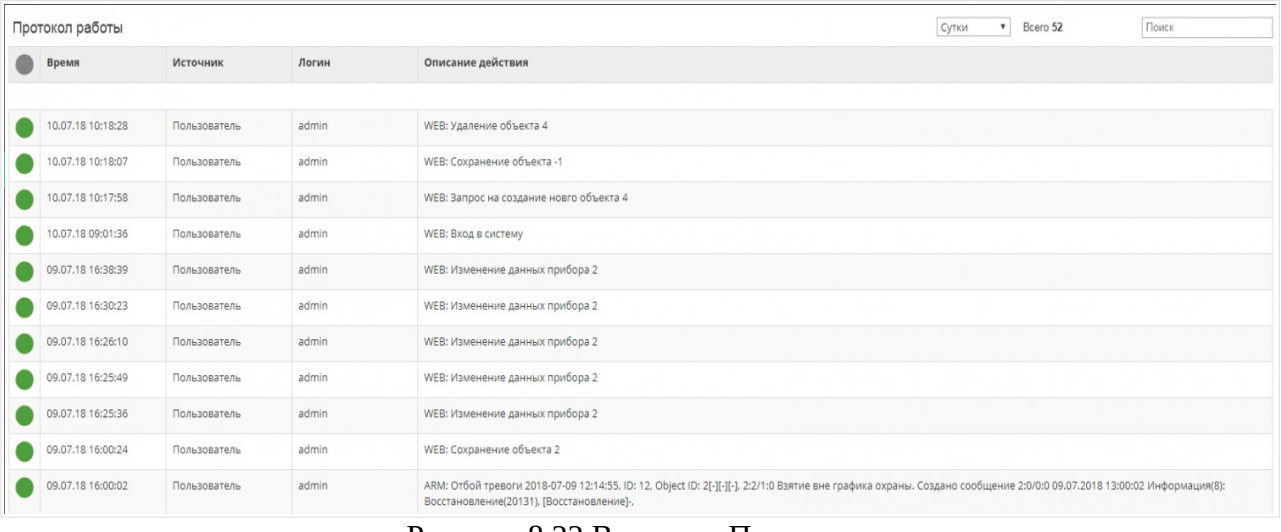


Рисунок 8.22 Вкладка «Протокол»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.6 Сообщения

С помощью пункта меню "Сообщения" (рисунок 8.23) имеется возможность отправлять информационные сообщения от имени **Администратора сервера** (superadmin - логин и пароль по умолчанию)
всем охранным организациям, заведенным на сервер КРОС. Для отправки сообщения вам необходимо:

1. Зайти на сервер под учетной записью "**Администратор сервера**" (superadmin - логин и пароль по умолчанию).

2. Зайти в меню Администрирование ---> Система.

3. Ввести сообщение, установить тип сообщения, а также выбрать кому отослать это сообщение, после чего нажать кнопку "Отправить".

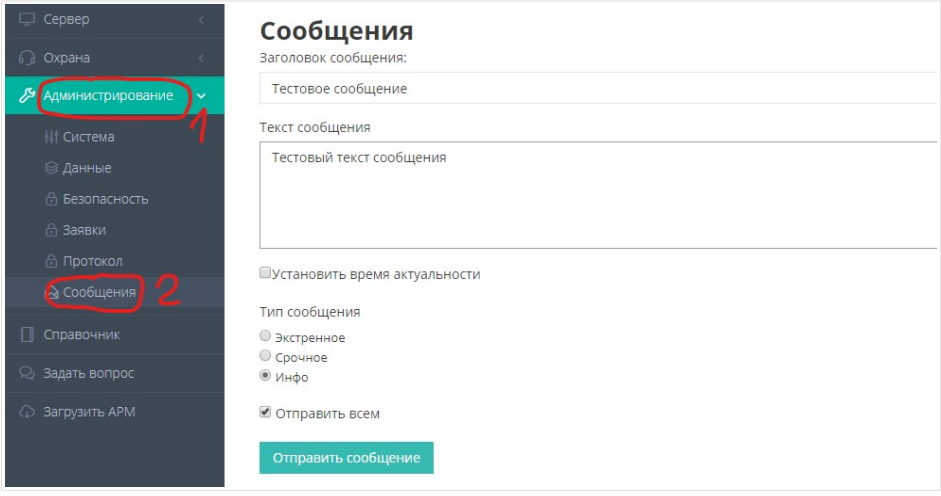


Рисунок 8.23 Меню «Сообщения»

После отправки сообщения оно будет отображаться в непрочитанных сообщениях в каждой охранной организации по нажатию на колокольчик (рисунок 8.23).

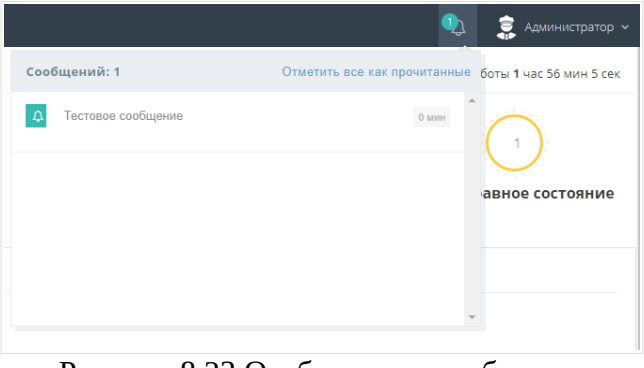


Рисунок 8.23 Отображение сообщения

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.7 Справочники

С помощью пункта меню «Справочники» имеется возможность редактировать различные справочники, используемые сервером «Юпитер-КРОС» и «АРМ Юпитер-КРОС».

8.7.1 Справочник «Типы объектов»

С помощью справочника «Типы объектов» (рисунок 8.24) имеется возможность добавлять, редактировать и удалять типы объектов, отображающиеся в карточках объекта в поле «Тип объекта».

- Для добавления нового типа объекта необходимо нажать на кнопку «Добавить» (Белый плюс в синем квадрате), добавить необходимые наименования и комментарий, если требуется, после чего нажать кнопку «Сохранить».
- Для удаления типа объекта нажать кнопку «Удалить» (белый крест в красном квадрате).

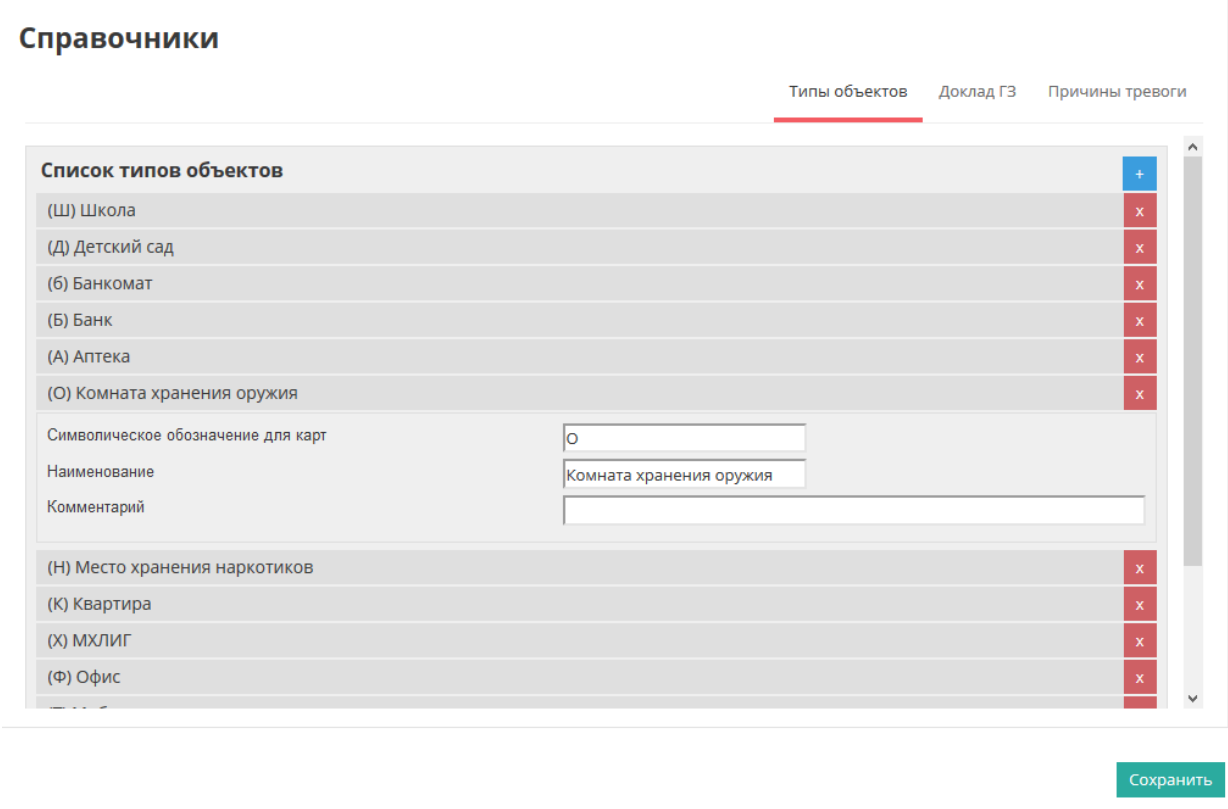


Рисунок 8.24 Вкладка «Типы объектов»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.7.2 Справочник «Доклад ГЗ»

С помощью справочника «Доклад ГЗ» (рисунок 8.25) имеется возможность добавлять, редактировать и удалять доклады ГЗ, отображающиеся в отчетах АРМ Юпитер-КРОС. Для просмотра справочника в АРМ Юпитер-КРОС необходимо открыть меню «Справочники» → «Доклады ГЗ»

- Для добавления нового доклада ГЗ необходимо нажать на кнопку «Добавить» и ввести необходимый текст в поле «Текст доклада», после чего нажать кнопку «Сохранить».
- Для удаления доклада ГЗ нажать кнопку «Удалить» (белый крест в красном квадрате).

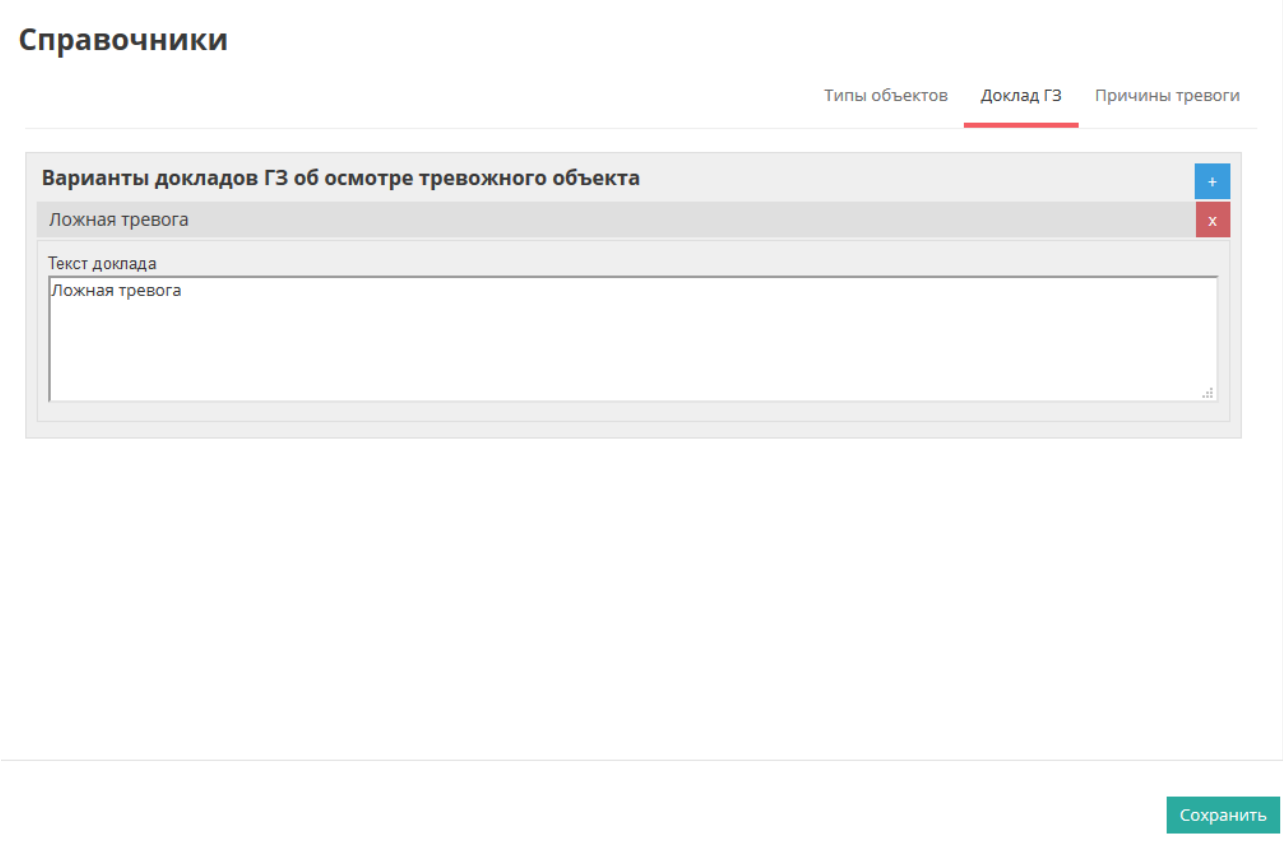


Рисунок 8.25 Вкладка «Доклад ГЗ»

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.7.3 Справочник «Причины тревоги»

С помощью справочника «Причины тревоги» (рисунок 8.26) имеется возможность добавлять, редактировать и удалять причины тревоги, отображающиеся в отчетах АРМ Юпитер-КРОС. Для просмотра справочника в АРМ Юпитер-КРОС необходимо открыть меню «Справочники» → «Причины тревоги».

- Для добавления новой причины тревоги необходимо нажать на кнопку «Добавить» и ввести необходимый текст в поле «Текст доклада», после чего нажать кнопку «Сохранить».
- Для удаления причины нажать кнопку «Удалить» (белый крест в красном квадрате).

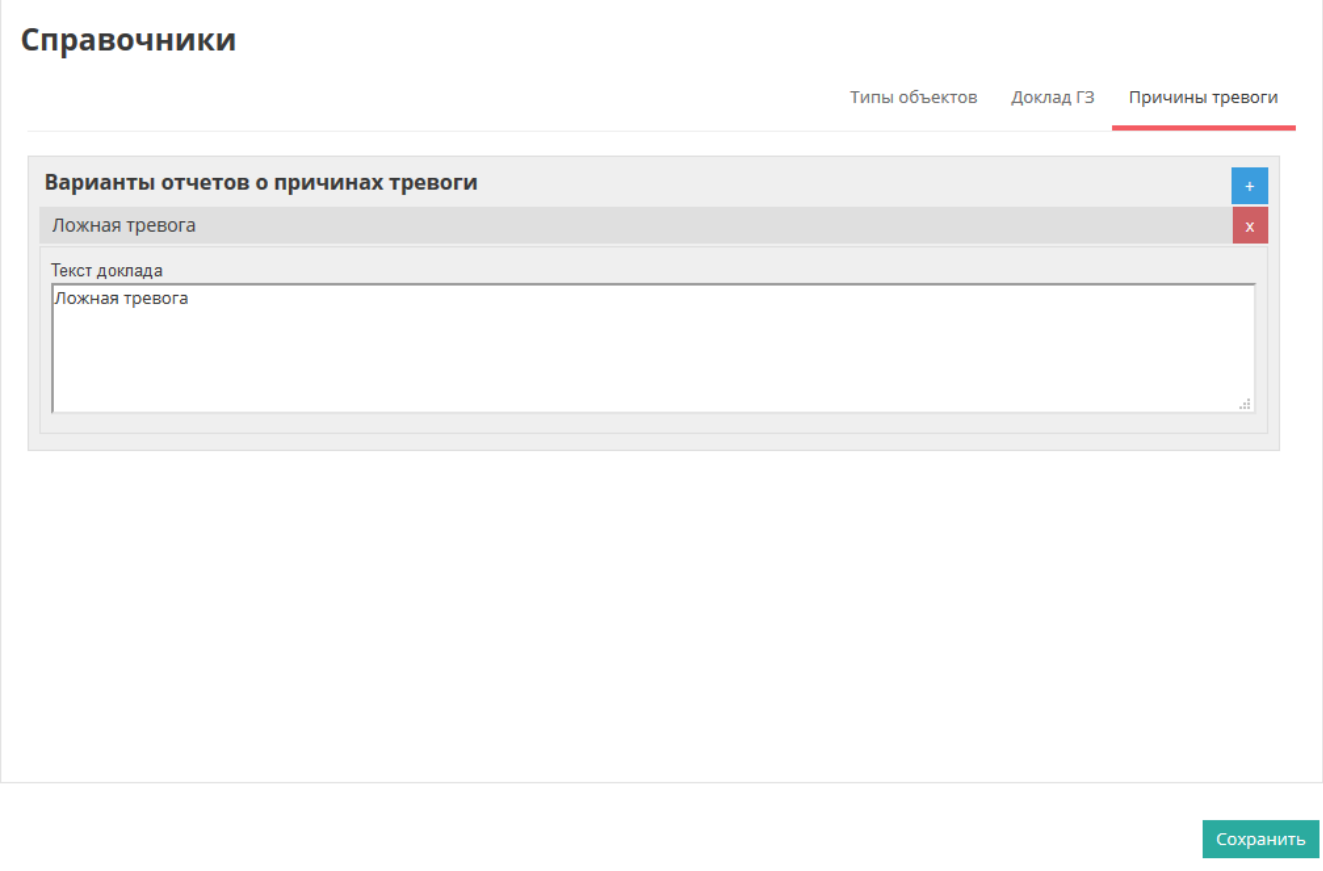


Рисунок 8.26 Вкладка «Причины тревоги»

SEC.RU | Короткий путь к информации Скачано с sec.ru

9. Зеркалирование («Горячий» резерв)

9.1 Общая информация

Зеркалирование позволяет осуществить совместную работу двух или более серверов КРОС в качестве равноправных сетевых станций использующих единое пространство данных.
Иными словами, например, система построенная на двух серверах подключенных в режиме зеркалирования full duplex(двусторонний обмен) позволяет:

1. Обеспечить корректное подключение прибора к любому из серверов и в дальнейшем динамически менять сервер подключения в процессе работы прибора поддерживая при этом единую обработку и хранение данных.
2. Обеспечить автоматическое распределение нагрузки по входящему трафику по серверам включенным в систему.
   Для этого достаточно настроить в приборе адрес второго сервера в качестве резервного. При этом в случае превышения пиковой нагрузки на основной сервер прибор, не получив вовремя подтверждения на отправленный пакет, автоматически переключится на резервный канал.
3. Обеспечить подключение АРМ и трансляцию данных для любого из серверов включенных в систему, тем самым обеспечивая равномерное распределение нагрузки по исходящему трафику.
4. Обеспечить работоспособность системы в случае выхода из строя одного из серверов без остановок и перезагрузок.

Зеркалирование может работать в двух режимах:

- **half duplex** - односторонний обмен:

  В этом случае один из компьютеров, обычно принимающий данные от прибора, выступает в качестве ведущего (или основного), а второй - в качестве ведомого (или резервного). В этом случае все события и изменения получаемые ведущим компьютером зеркалируются на ведомый компьютер. Ведомый компьютер позволяет осуществлять мониторинг, управлять приборами на уровне команд, однако все изменения базы данных

SEC.RU | Короткий путь к информации Скачано с sec.ru

сделанные на нем (в том числе отбой тревог) не будут отражаться на ведущем. Таким образом режим half duplex целесообразно использовать для "холодного" резервирования, т.е. для поддержания текущего состояния на резервном компьютере на случай выхода из строя основного.

- **full duplex** - двусторонний обмен:

  В этом случае оба компьютера выступают в качестве равноправных серверных станций, способных принимать соединения от приборов и передавать данные в АРМ или трансляции. Все события и изменения получаемые одним из компьютеров зеркалируются на второй. Оба компьютера работают с единым множеством данных и позволяют осуществлять мониторинг, управлять приборами на уровне команд и вносить изменения в базу данных. Таким образом режим half duplex целесообразно использовать как для "горячего" резервирования, так и в целях распределения нагрузки в направлении обработки данных и каналов связи.

9.2 Настройка системы

В общем случае настройка работы двух компьютеров в режиме **half duplex** сводится к двум шагам:

1.Создание трансляции ЕППС с ведущего компьютера на ведомый.

2.Разрешение ведомому компьютеру принимать данные с ведущего.

Для настройки режима **full duplex** достаточно продублировать эти шаги в обратном направлении:

1.Создать трансляцию ЕППС с ведомого компьютера на ведущий.

2.Разрешение ведущему компьютеру принимать данные с ведомого.

Настройки осуществляются в режиме доступа **Администратор сервера** (superadmin).

SEC.RU | Короткий путь к информации Скачано с sec.ru

9.3 Создание трансляции

На ведущем компьютере:

1. Перейти Меню: Сервер -> Трансляции (рисунок 9.1).
2. Нажать кнопку Создать трансляцию.
3. Ввести Наименование, например "ПРОВЕРКА СВЯЗИ".
4. Выбрать охранную организацию из списка Отправитель.
   Именно выбранная охранная организация будет выступать в качестве источника данных для трансляции.
   Если необходимо настроить зеркалирование нескольких охранных организаций - для каждой необходимо создать отдельную трансляцию.
5. Указать Код идентификации получателя - это идентификатор охранной организации на ведомом сервере, в которую будут поступать данные от организации отправителя. Определить этот идентификатор можно если на ведомом сервере открыть список организаций Меню: Охрана -> Реквизиты. Нужное значение отображается в колонке Код.
6. Ввести Адрес (IP4 или Доменное имя) - адрес ведомого сервера.
   Если система разворачивается в локальной сети то необходимо указать локальный сетевой адрес (например 192.168.1.147).
7. Ввести Порт - номер порта ведомого компьютера. По умолчанию 4000.
8. Сохранить данные.

SEC.RU | Короткий путь к информации Скачано с sec.ru

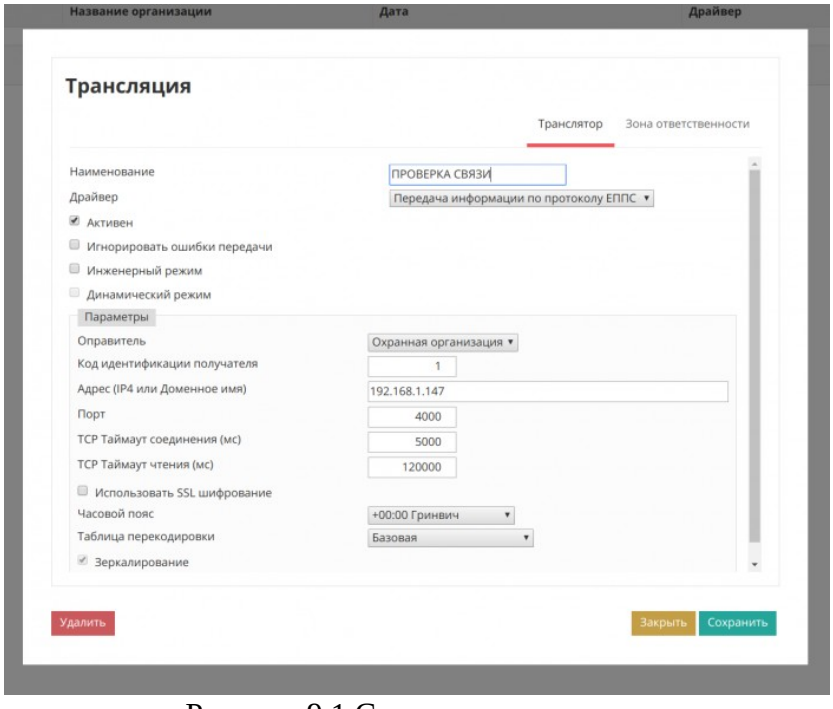


Рисунок 9.1 Создание трансляции

9.4 Разрешение приема данных

На ведомом компьютере:

1.Перейти Меню: Охрана -> Реквизиты.

2.Открыть на редактирование карту организации, которая будет принимать данные зеркалирования.

3.Открыть закладку Параметры.

4.В поле Адреса разрешенные для приема зеркалирования ввести адрес ведущего сервера. Если система разворачивается в локальной сети то необходимо указать локальный сетевой адрес (например 192.168.1.147).

5.Сохранить данные (рисунок 9.2).

SEC.RU | Короткий путь к информации Скачано с sec.ru

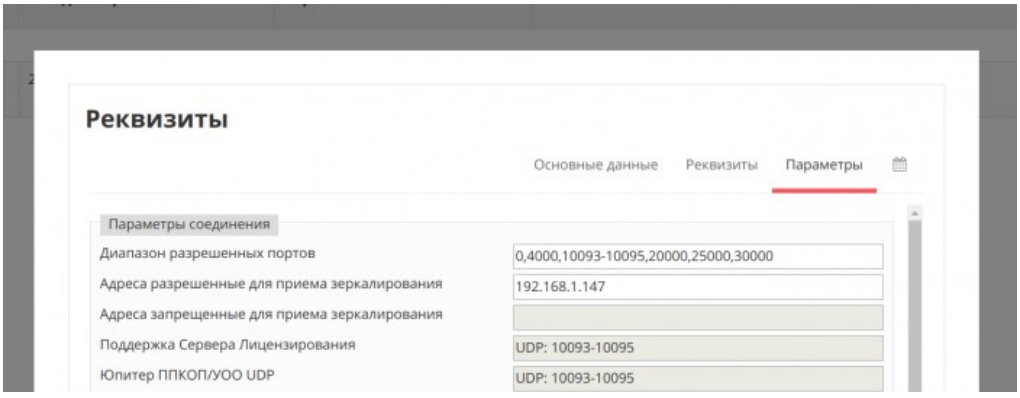


Рисунок 9.2 Разрешение приема данных

Система зеркалирования готова к работе. Возможно потребуется несколько минут для установки первого соединения и начальной синхронизации данных.

10. Импорт базы данных

10.1 Перенос базы данных Юпитер-7 в Юпитер-КРОС

В инструкции указана последовательность действий для случая, когда у пользователя уже есть текущая работающая БД Юпитер-7

Чтобы конвертировать базу данных Юпитер-7 в базу данных КРОС необходим Файл конфигурации

Юпитер-КРОС распознает xml и zip конфигурации.
zip-файл состоит из xml-файла и может содержать картинки объектов.

10.1.1 Создание файла конфигурации Юпитер-7

Файл конфигурации оборудования по умолчанию расположен на диске С, путь:

```
C:\jupiter-18.win\export.2017-10-17-12.20.30.zip
```

Если файла конфигурации не создано заранее, то это нужно сделать следующим образом:

1. Запустите АРМ ДПУ версии 7.19.0.24 или выше;
2. Откройте меню Файл;
3. Выберите пункт меню Экспорт;
4. Выберите пункт меню Конфигурацию;

Все шаги этой операции можно увидеть на рисунке 10.1

SEC.RU | Короткий путь к информации Скачано с sec.ru

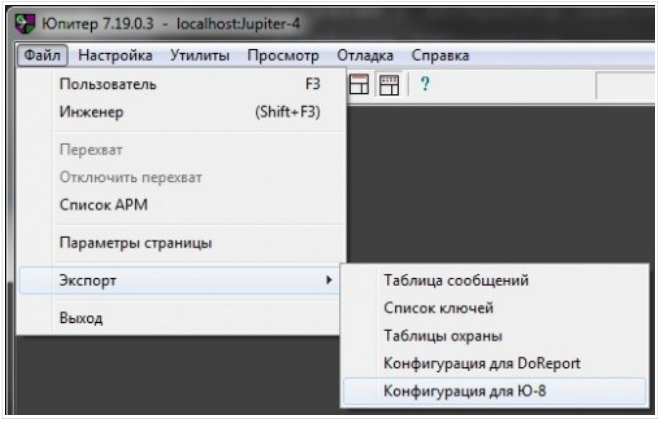


Рисунок 10.1 Создание файла конфигурации

10.1.2 Импорт файла конфигурации в Юпитер-КРОС

Для выгрузки базы данных Юпитер-7 в Юпитер КРОС необходимо (рисунок 10.2):

1. Заходим под **администратором охранной организации** (admin-логин и пароль по умолчанию).
2. Переходим Клиенты-Объекты.
3. В правом верхнем углу нажимаем Импорт.
4. Выбираем файл с конфигурацией и нажимаем Загрузить.
5. После окончания импорта обновляем страницу.

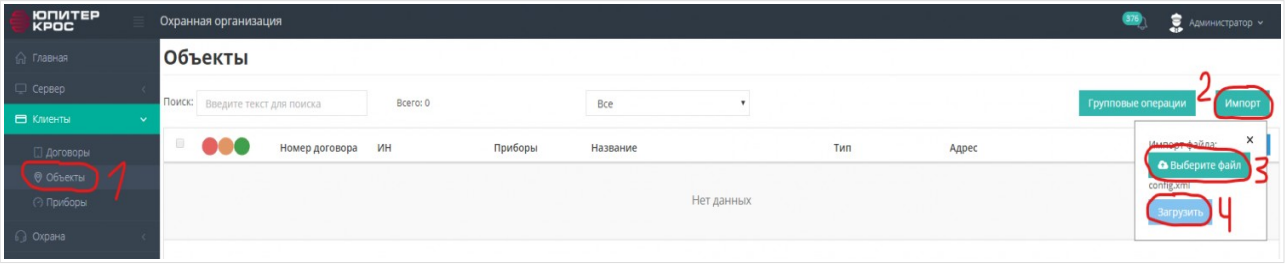


Рисунок 10.2 Выгрузка базы данных

Информацию по импорту можно увидеть в http логе, расположенном на сервере в папке Log.

В приборах:
- IP/GPRS создаются 3 канала связи: ЕППС, ПК4, CSD.
- 18 кГц – ЕППС.

Примечание:
Если в карточке объекта Юпитер-7 указан адрес без города, то Автоматически подставляется город из Охранной организации, а именно:
Охрана-Реквизиты-Редактирование охр.орг.-Реквизиты-Юридический адрес

SEC.RU | Короткий путь к информации Скачано с sec.ru

10.2 Соответствие карточек Юпитер-7 при переносе в Юпитер-КРОС

Юпитер 7 ⟶ КРОС

№	Карточка Прибора (КП)	Карточка раздела (КР)	Раздел (Р)		Карточка объекта	Прибор	Раздел (Р)	Договор (Д)
1	-	-	-	⟶	-	+	+	-
2	-	-	+		-	+	+	-
3	-	+	-	⟶	-	+	+	-
4	-	+	+	⟶	КР	+	+	Д кр
5	+	-	-	⟶	КП	+	+	Д кп
6	+	-	+	⟶	КП -	- +	- +	Д кп -
7	+	+	-	⟶	КП КР	- +	- +	Д кп Д кр
8	+	+	+	⟶	КП КР	- +	- +	Д кп Д кр
9	-	-	Р1 и Р2	⟶	-	+	Р1 и Р2	-
10	-	КР1 и КР2	Р1 и Р2	⟶	КР1 КР2	+ +	Р1 Р2	Д кр1 -

SEC.RU | Короткий путь к информации Скачано с sec.ru

10.3 Настройка трансляции из Юпитер-7 в Юпитер-КРОС

ВНИМАНИЕ!
Трансляция ЕППС предназначена ТОЛЬКО для СТАРОГО оборудования
Новые приборы (IP/GPRS) необходимо подключать напрямую к КРОС без трансляции.
Трансляция ЕППС поддерживается АРМ ДПУ версии 7.20.0.8 или выше.

В папку с Jupiter.exe требуется обязательно поместить файл epps_codes.ini.

Юпитер-7 и Юпитер-КРОС необходимо устанавливать НА РАЗНЫЕ компьютеры во избежание падения производительности.

Последняя версия АРМ ДПУ и epps_codes.ini предоставляется по запросу.

Настройка трансляции:
В Юпитер-7 выбрать: Настройки-Соединение с Юпитер-8 (рисунок 10.3).

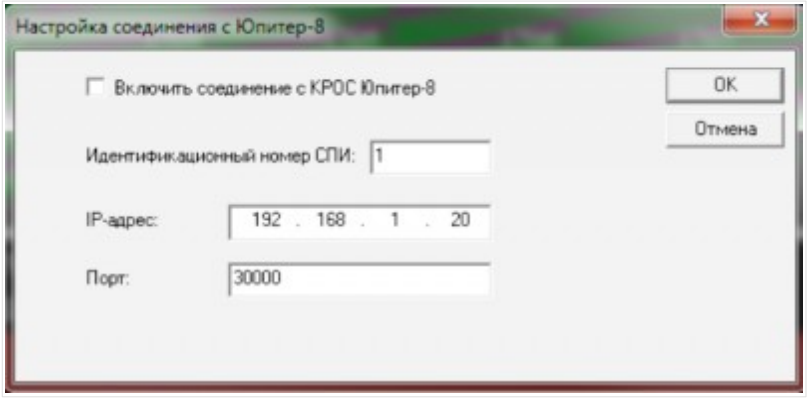


Рисунок 10.3 Соединение с Юпитер-КРОС

- Идентификационный номер СПИ- id охранной организации в КРОС.
- IP-адрес сервера КРОС.
- TCP Порт, выделенный для охранной организации для приема данных по ЕППС.

Примечание.
Приборы 18КГц работают с КРОС только через Юпитер-7.

SEC.RU | Короткий путь к информации Скачано с sec.ru

10.4 Настройка работы с мобильным приложением «Личный кабинет» при трансляции из Юпитер-7 в Юпитер-КРОС

Для того, чтобы иметь возможность работать с мобильным приложением "Личный кабинет" требуется:

1. Выгрузить базу из Юпитер-7 в Юпитер КРОС.
2. Под учетной записью **администратора охранной организации** (admin-логин и пароль по умолчанию) зайти в меню Клиенты ---> Объекты.
3. Выбрать объект, для которого должен быть заведен личный кабинет.
4. Открыть карточку выбранного объекта и зайти в меню "ХО". В этом меню отобразятся все ответственные лица, выгруженные из Юпитер-7 (рисунок 10.4).
5. Выбрать ответственное лицо, которому необходимо предоставить доступ к личному кабинету.
6. Открыв нужное ответственное лицо, задать ему логин и пароль на вход в личный кабинет, а также поставить галочку "Доступ в личный кабинет".
7. Нажать кнопку "Сохранить".

   После этих действий пользователь сможет зайти в мобильное приложение "Личный кабинет" и управлять объектом.

SEC.RU | Короткий путь к информации Скачано с sec.ru

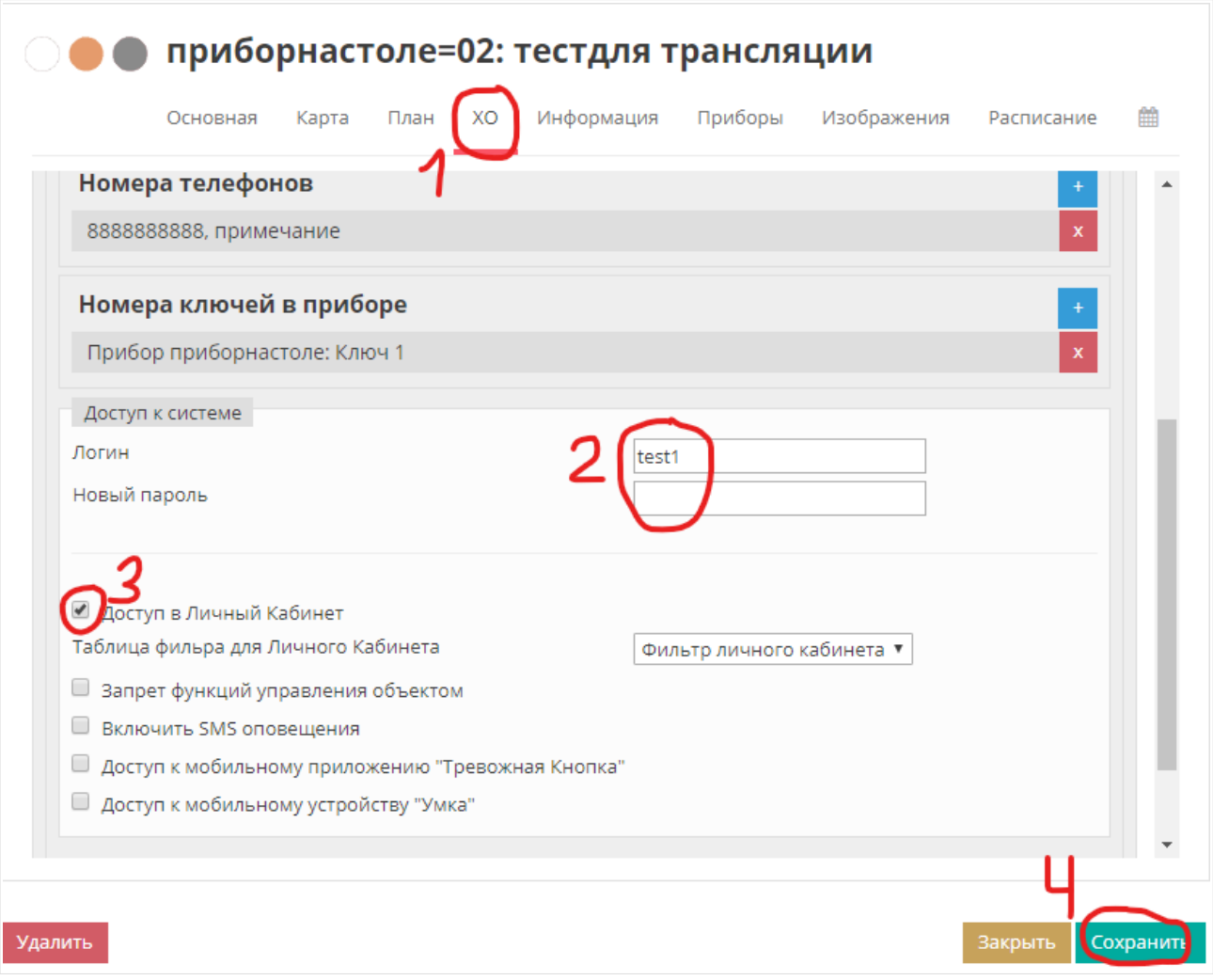


Рисунок 10.4 Настройка ответственного лица

SEC.RU | Короткий путь к информации Скачано с sec.ru

11. Настройка часов УМКА для работы на сервере «Юпитер-КРОС»

11.1 Первоначальная настройка часов

Сервер «Юпитер-КРОС» имеет возможность работы с устройством мониторинга координат и адресной безопасности Юпитер-УМКА. Устройство выполнено в виде наручных часов с сенсорным экраном и предназначено для обеспечения связи, передачи тревожного извещения, определения местоположения.

Для подключения часов "Умка" к серверу Юпитер-КРОС необходимо:

1. Определить номер телефона (SIM-карты) в часах для первоначальных настроек.
2. Задать в часах адрес сервера (IP-адрес и TCP-порт), на который в дальнейшем будут подключаться часы. Для этого:

   Отправляем на часы sms-команду:

   pw,123456,ip,123.123.123.123,6001#

   Где:

   - IP: 123.123.123.123 (Внешний белый IP-адрес компьютера, на который установлен сервер КРОС) .
   - TCP порт: 6001 (порт, по умолчанию установленный для связи часов с сервером КРОС).

   При успешной смене адреса и порта на телефон, с которого вы отправляли СМС придет подтверждение следующего вида - [surl,123.123.123.123,port,6001#] ok!

3. Войти под учётной записью, имеющей доступ к редактированию договора. По умолчанию это право имеет **Администратор охранной организации**.
4. Создать договор. Для этого нажать в левом меню Клиенты ---> Договоры ---> Создать новый договор (рисунок 11.1).

   В договоре необходимо указать номер договора и поставить состояние договора "Активен".

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рисунок 11.1 Создание договора

5. Создать ответственное лицо, задать логин и пароль для доступа в личный кабинет, установить галочку доступа в личный кабинет и доступа к мобильному устройству Умка (рисунок 11.2).

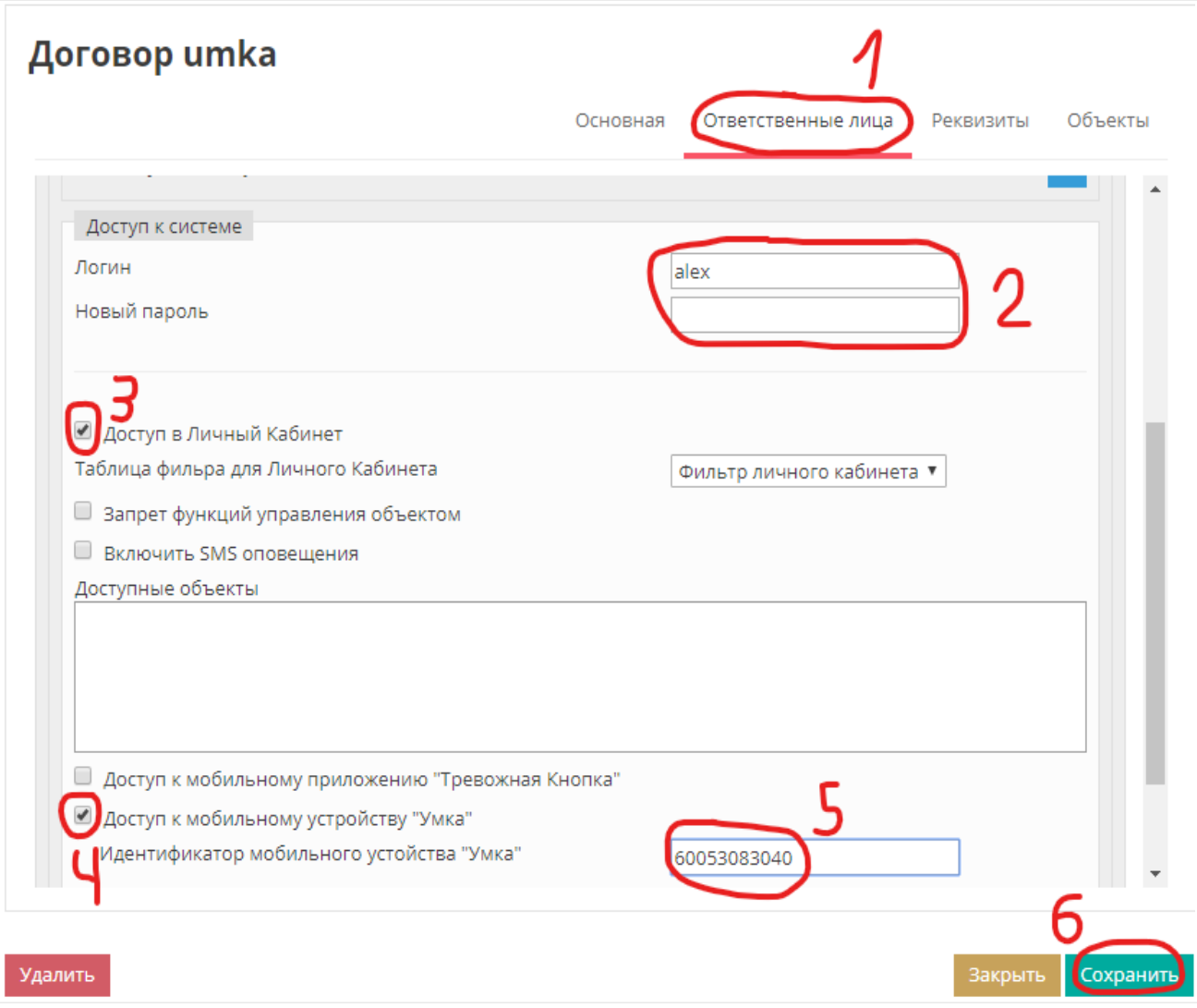


Рисунок 11.2 Настройка ответственного лица

6. Ввести ID или REGCODE часов, наклеен с оборотной стороны часов (пункт 5 на изображении выше), после чего нажимаем кнопку Сохранить.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Для непрерывной записи трека часов Умка в настройках ответственного лица установить галочку “Всегда записывать трек перемещения”, трек начинает передаваться каждые 20 сек.

7. Зайти в Личный кабинет созданного Ответственного лица и видим мобильный Объект с названием "УМКА" (рисунки 11.3 и 11.4).

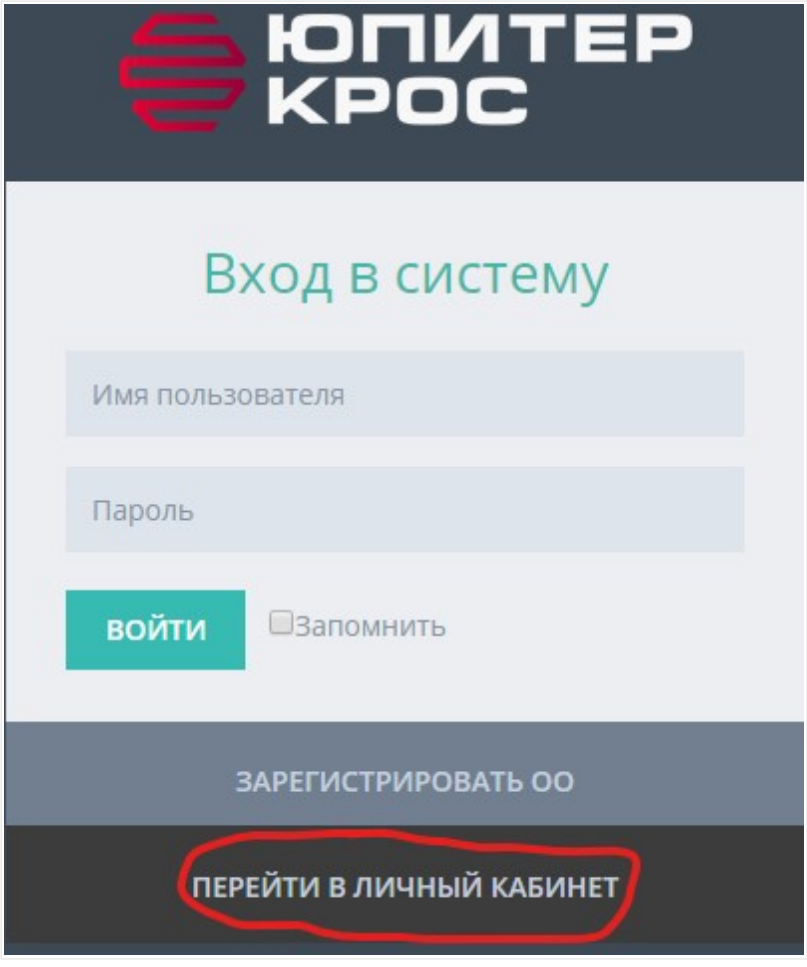
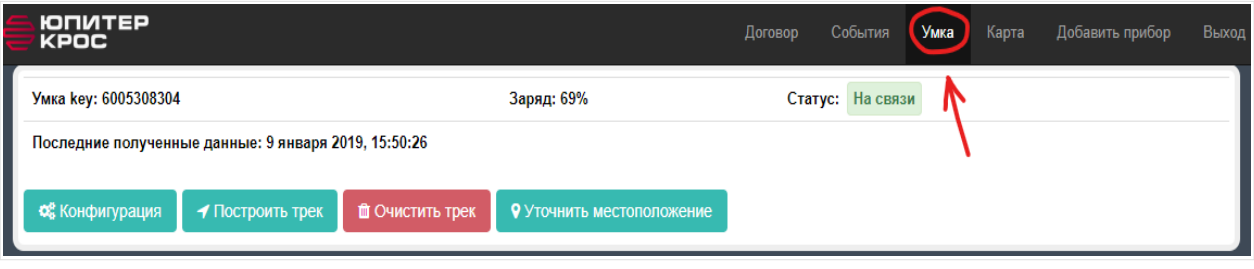


Рисунок 11.3 Переход в личный кабинет



SEC.RU | Короткий путь к информации Скачано с sec.ru

Рисунок 11.4 Отображение часов

11.2 Настройка отслеживания часов в приложении АРМ ДПУ

Перед настройкой часов для работы с АРМ ДПУ предполагается, что первоначальная настройка часов проведена корректно согласно инструкции выше.

1. Зайти в личный кабинет созданного ответственного лица и выбираем пункт "Конфигурация" (рисунок 11.5).

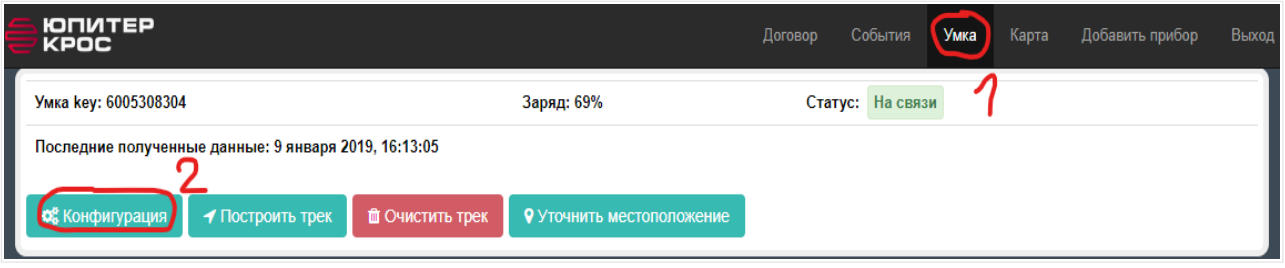


Рисунок 11.5 Конфигурация часов

2. В меню "Конфигурация" устанавливаем центральный номер "Sos1", так как без него не будет работать передача координат и тревоги в АРМ (рисунок 11.6).

Можно установить номер СИМ-Карты, вставленной в ваши часы "Умка", либо любой другой номер мобильного телефона, если вы хотите, чтобы на него дублировалось сообщение о тревоге.

SEC.RU | Короткий путь к информации Скачано с sec.ru

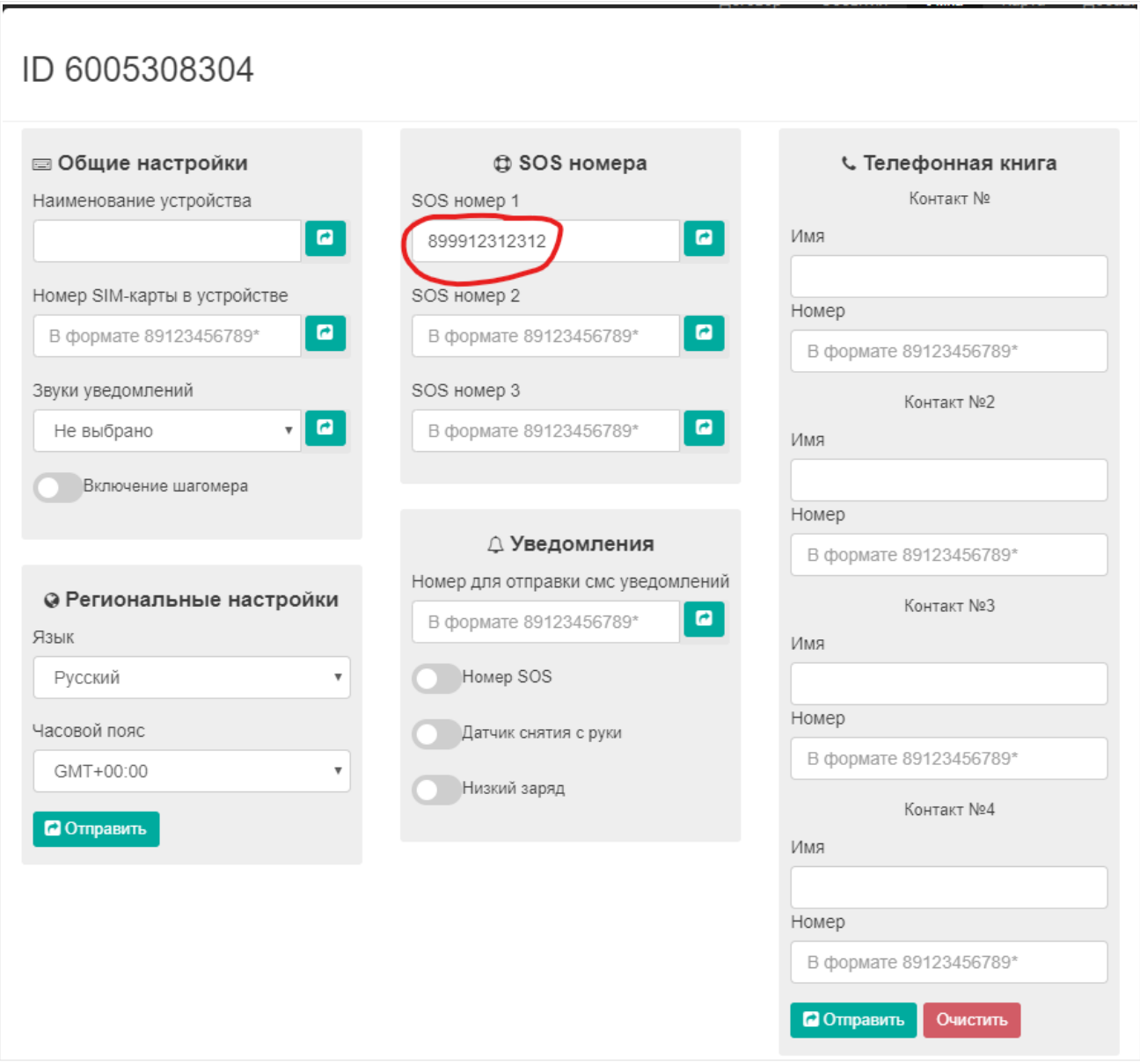


Рисунок 11.6 Установка номера

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. При нажатии на кнопку SOS на часах, в АРМ отправляется тревога (рисунок 11.7).

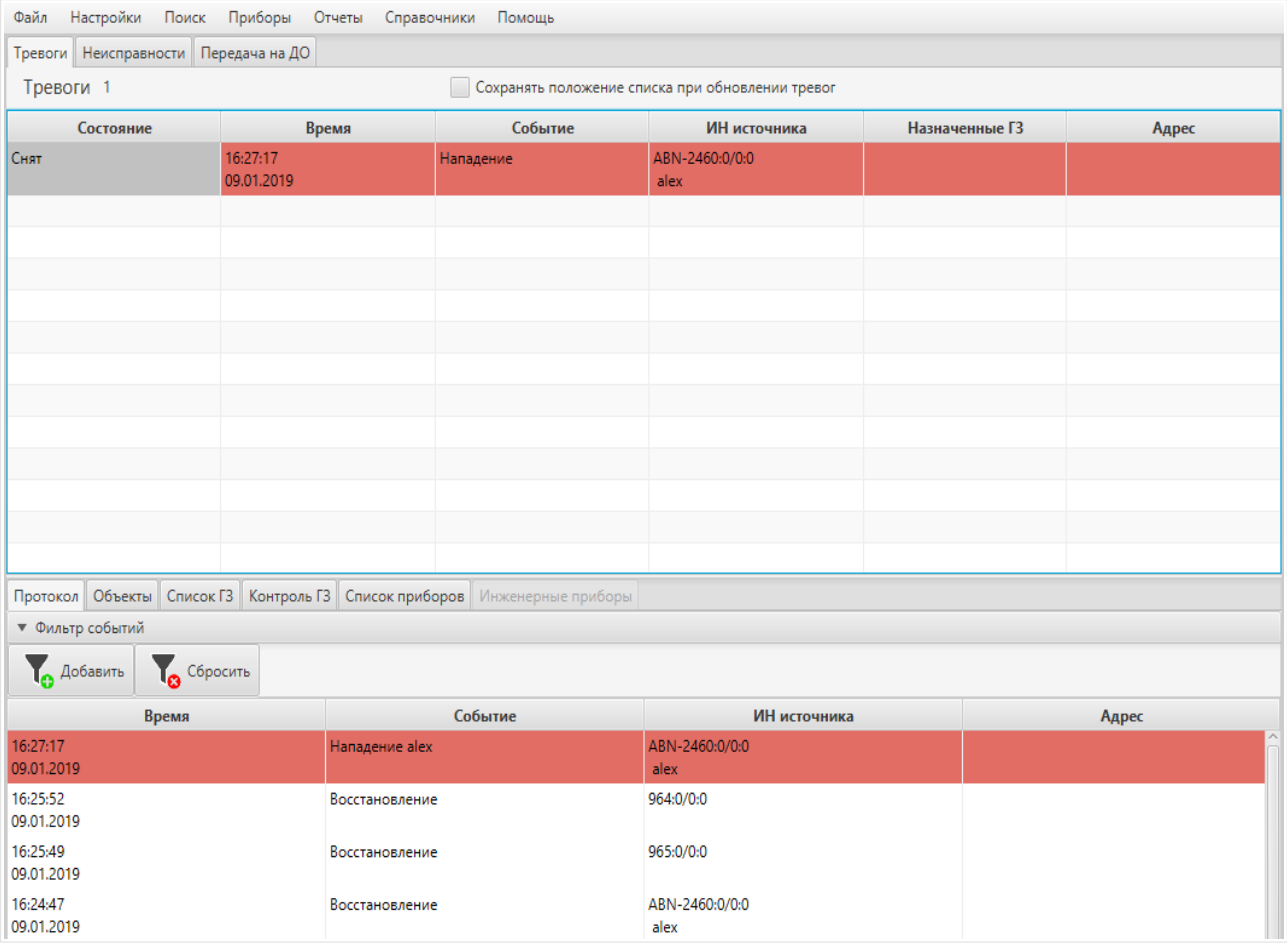


Рисунок 11.7 Тревога на АРМ

4. Для просмотра подробной информации по тревоге необходимо дважды кликнуть на активную тревогу, после чего откроется окно тревоги.

SEC.RU | Короткий путь к информации Скачано с sec.ru

В этом окне можно отследить по карте откуда была отправлена тревога (рисунок 11.8).

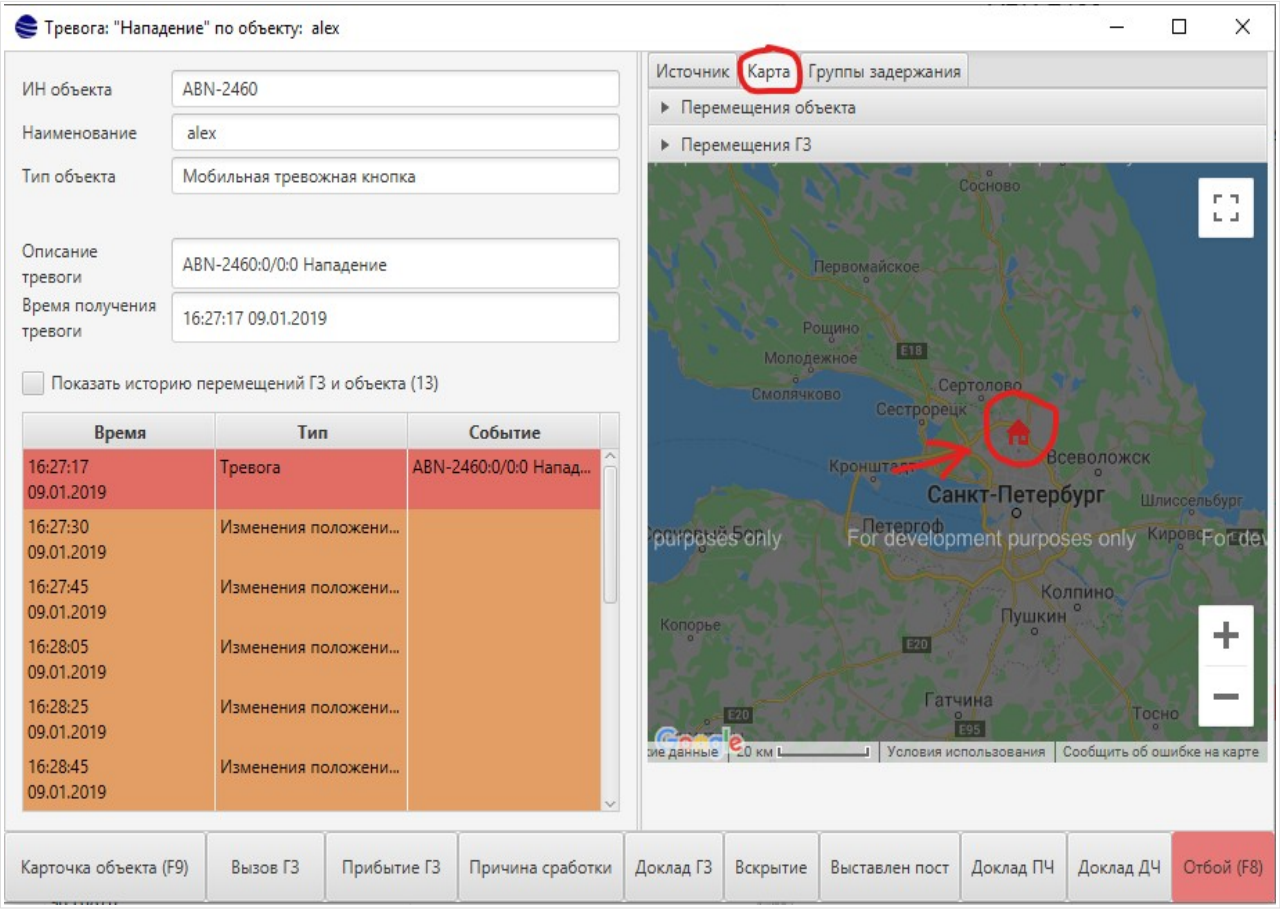


Рисунок 11.8 Отображения координат тревоги

Дальнейшее взаимодействие с тревогой происходит по тому же принципу, как и с обычной тревогой с прибора.

Если вы столкнулись с ошибкой «Нет подключения к сети», то:

1. Убедитесь что часы включены.
2. Проверьте поступает ли входящий звонок на часы.
3. Убедитесь, что SIM-карта имеет положительный баланс и доступ в интернет.
4. Проверьте, соответствуют ли ID на часах и в личном кабинете.

SEC.RU | Короткий путь к информации Скачано с sec.ru

12 Конструктор отчетов

В меню "Отчеты" имеется возможность строить отчеты как по базовым шаблонам, так и создавать свои варианты отчетов с необходимыми в конкретной ситуации полями.

Для открытия меню "Отчеты" необходимо авторизоваться под учетной записью Администратор, и в левом меню выбрать пункт "Отчеты". Будет выведено стартовое окно с шаблонами отчетов.

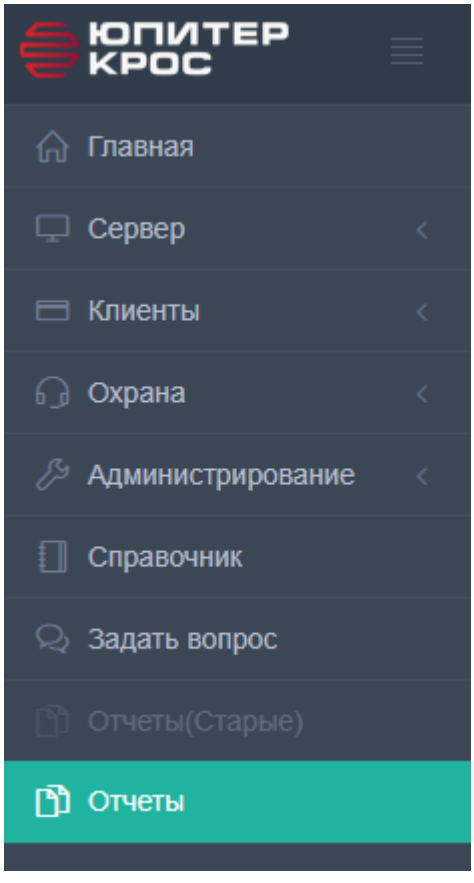


Рис. 12 Меню «Отчеты»

SEC.RU | Короткий путь к информации Скачано с sec.ru

12.1 Общий вид конструктора отчетов

В конструкторе отчетов предусмотрены базовые предустановленные шаблоны отчетов (цифра 1 на изображении ниже). Базовые шаблоны невозможно удалить.

При нажатии на кнопку карандаш (цифра 5 на изображении ниже) будет создана копия базового отчета, с возможностью гибкой настройки полей.

Кнопка с вопросительным знаком (цифра 2 на изображении ниже) откроет справочную статью в Википедии.

Кнопка со щитом (цифра 3 на изображении ниже) позволяет строить отчеты по оперативным карточкам.

Кнопка с шестеренкой (цифра 4 на изображении ниже) открывает конструктор отчетов, в котором возможно построить полностью индивидуальный отчет с только необходимыми в конкретной ситуации полями.

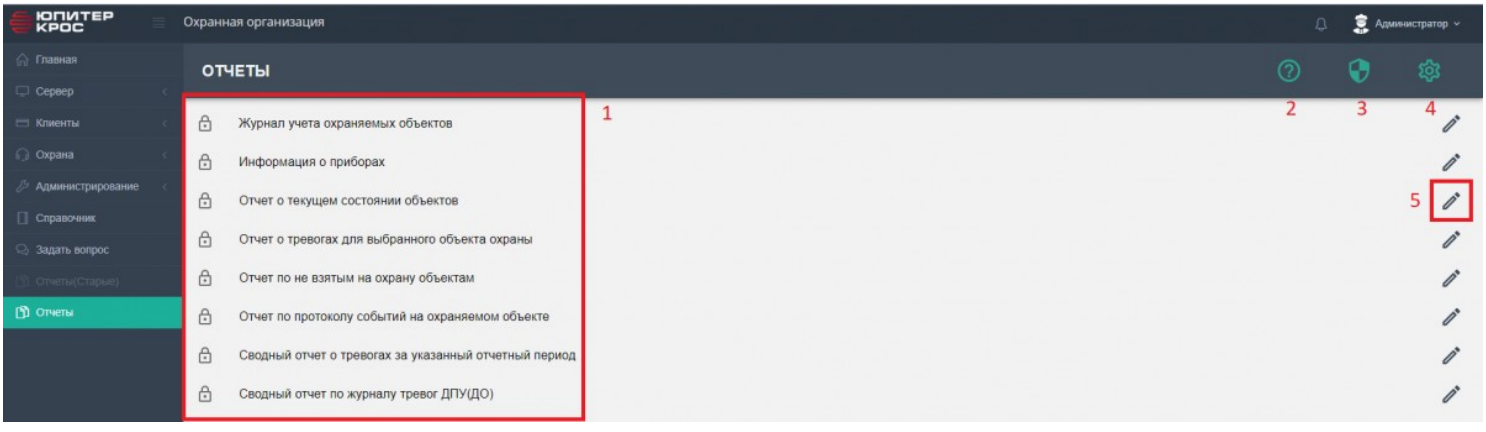
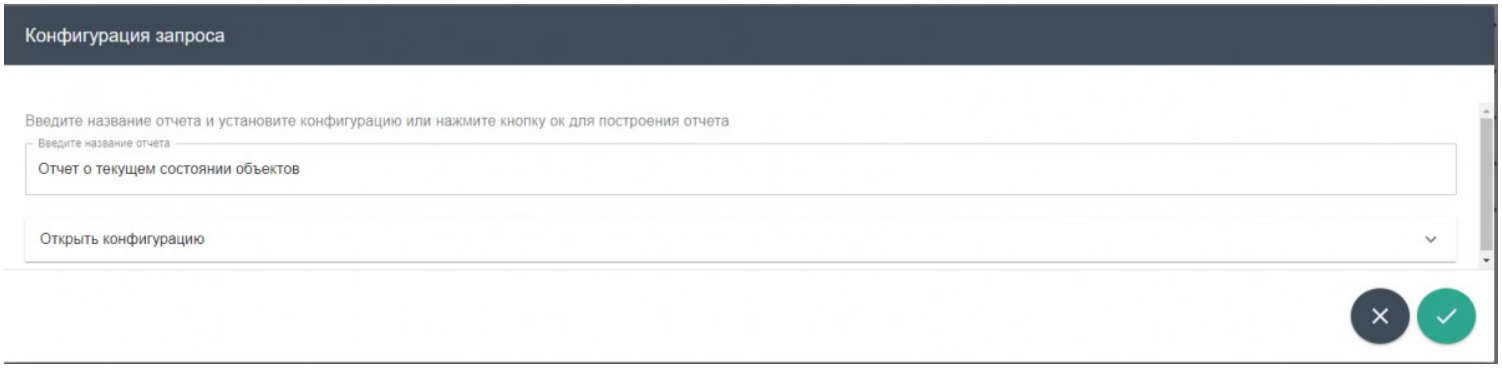


Рис 12.1 Общий вид конструктора отчетов

SEC.RU | Короткий путь к информации Скачано с sec.ru

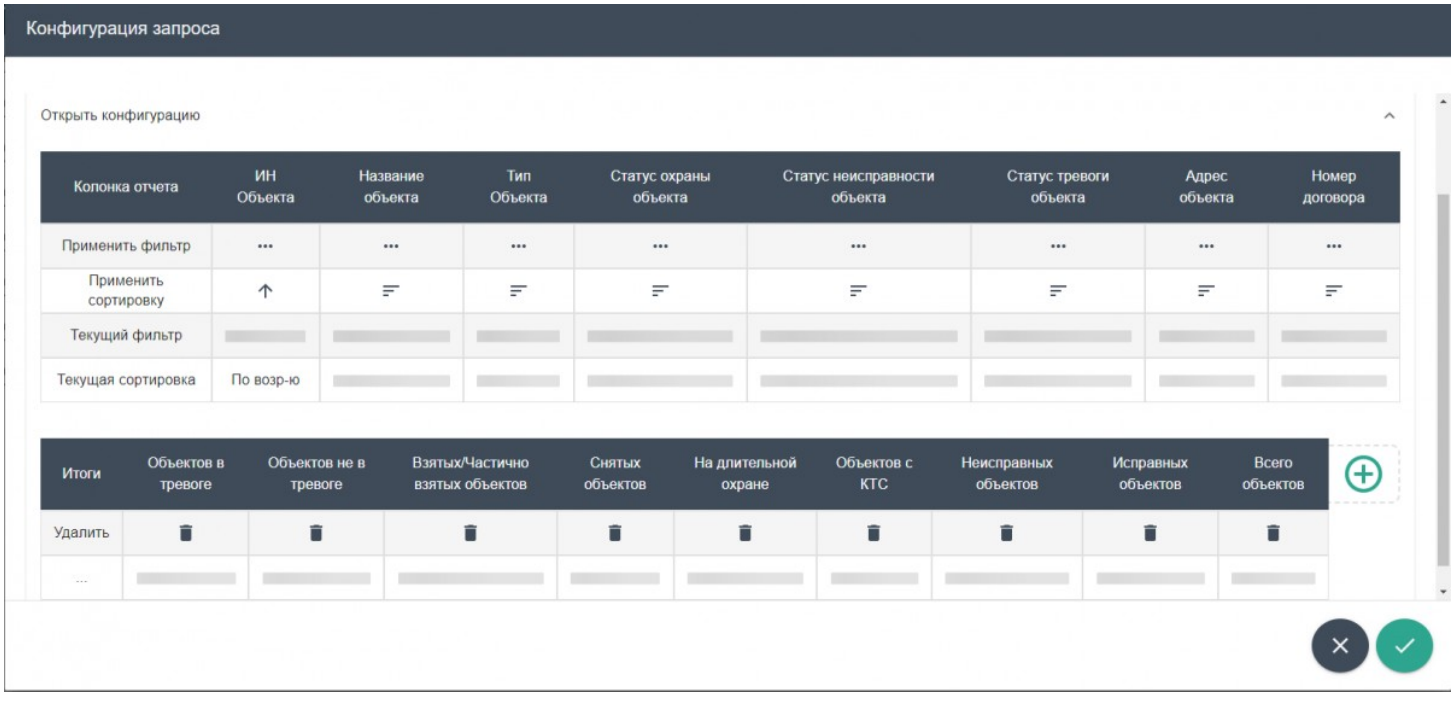
12.2 Создание отчета по базовому шаблону

Для построения отчета по базовому шаблону необходимо выбрать шаблон, одинарно кликнув на него левой кнопкой мыши. Будет открыто окно, в котором необходимо задать название отчета, либо оставить стандартное. Конфигурация отчета не является обязательной. Для построения отчета необходимо нажать зеленую кнопку с галочкой.

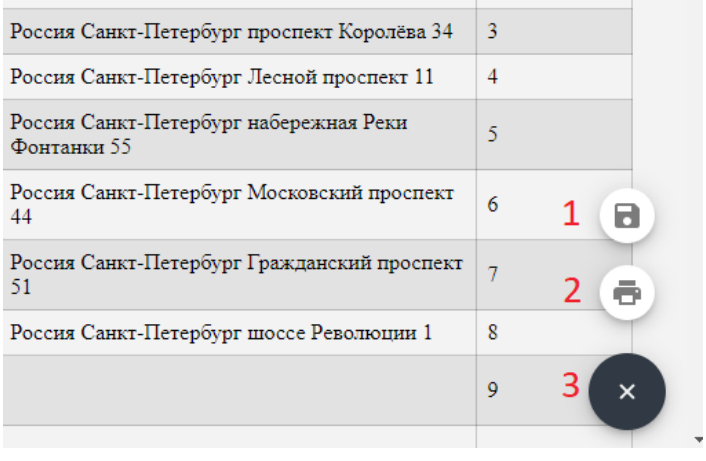


SEC.RU | Короткий путь к информации Скачано с sec.ru

При нажатии кнопки "Открыть конфигурацию" появляется возможность задавать фильтры и сортировки для отчета. Данный шаг является необязательным, если ничего здесь не настраивать, отчет будет построен полностью.



Для сохранения отчета в виде таблицы формата xls необходимо нажать на кнопку № 1. Для отправки отчета на печать нажать кнопку №2 Для закрытия меню печати нажать кнопку №3



SEC.RU | Короткий путь к информации Скачано с sec.ru

12.3 Создание шаблона отчета в конструкторе отчетов

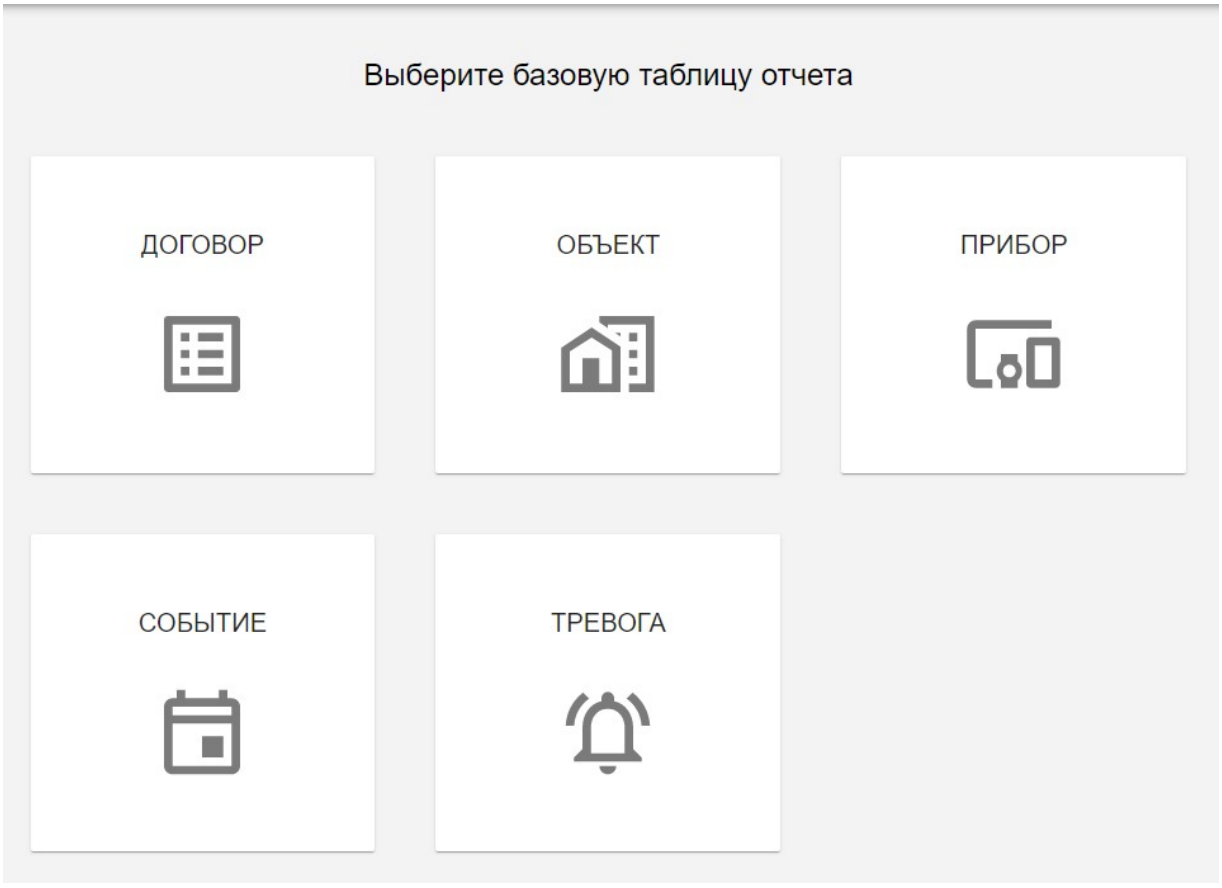
Конструктор отчетов позволяет создавать шаблоны необходимых именно Вам отчетов. Создав отчет с необходимыми параметрами требуется сохранить шаблон, после чего он попадет на главную страницу к другим базовым шаблонам.

В отличии от базовых шаблонов, созданные в конструкторе шаблоны можно удалять и редактировать.

Для создания отчета в конструкторе отчетов необходимо:

1. Нажать на кнопку с шестеренкой.

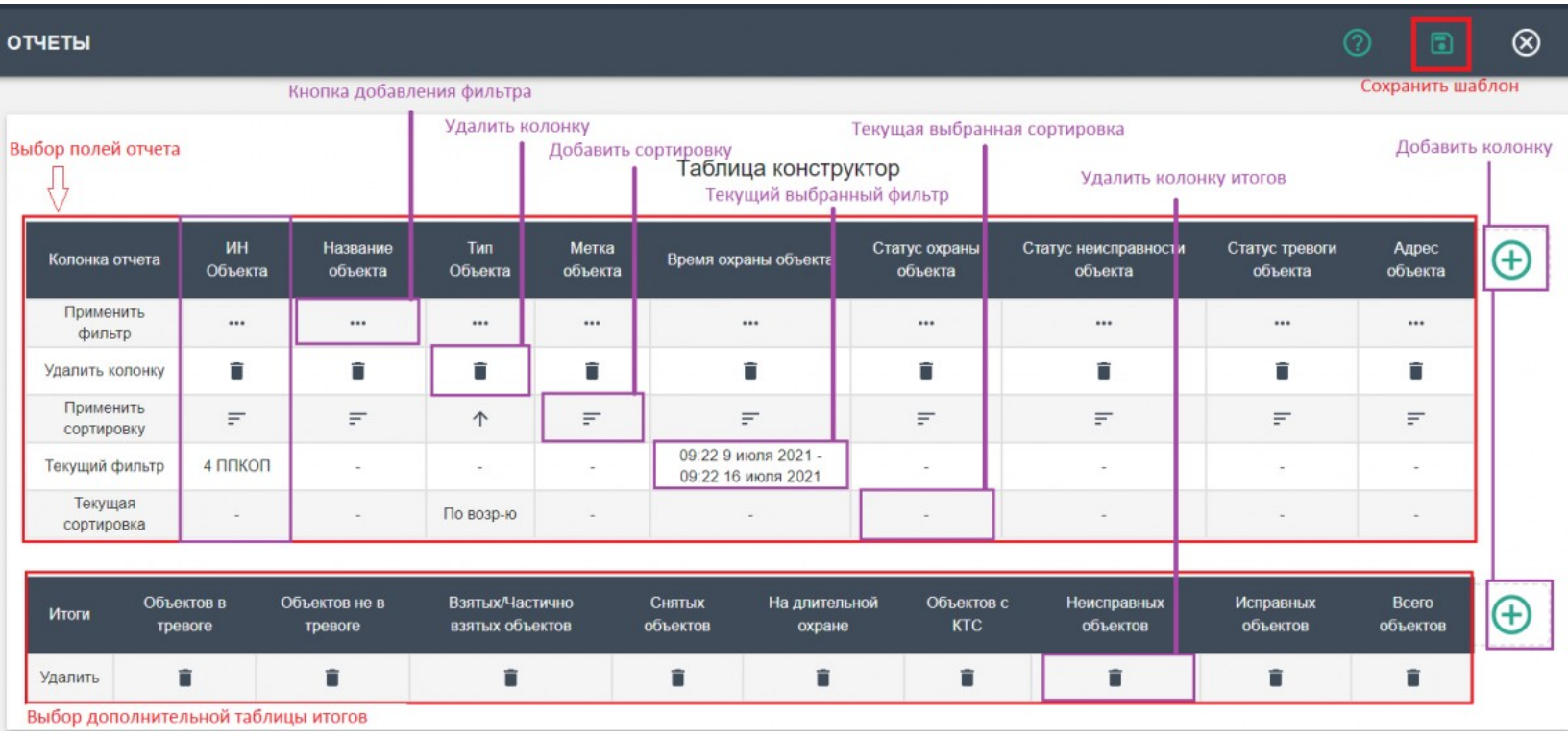
2. В появившемся меню выбрать базовую таблицу для отчета. На основе этой таблицы будет построен отчет.



SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Выбрать необходимые поля, задать сортировки и фильтры. Можно удалить ненужные колонки, нажав на значок "Корзина", или же добавить необходимые, нажав на кнопку "Плюс".

4. После добавления всех необходимых колонок и фильтров нажать на кнопку "Сохранить", ввести название шаблона и нажать "Применить". Составленный шаблон будет добавлен на главную страницу конструктора отчетов, откуда можно его построить



SEC.RU | Короткий путь к информации Скачано с sec.ru

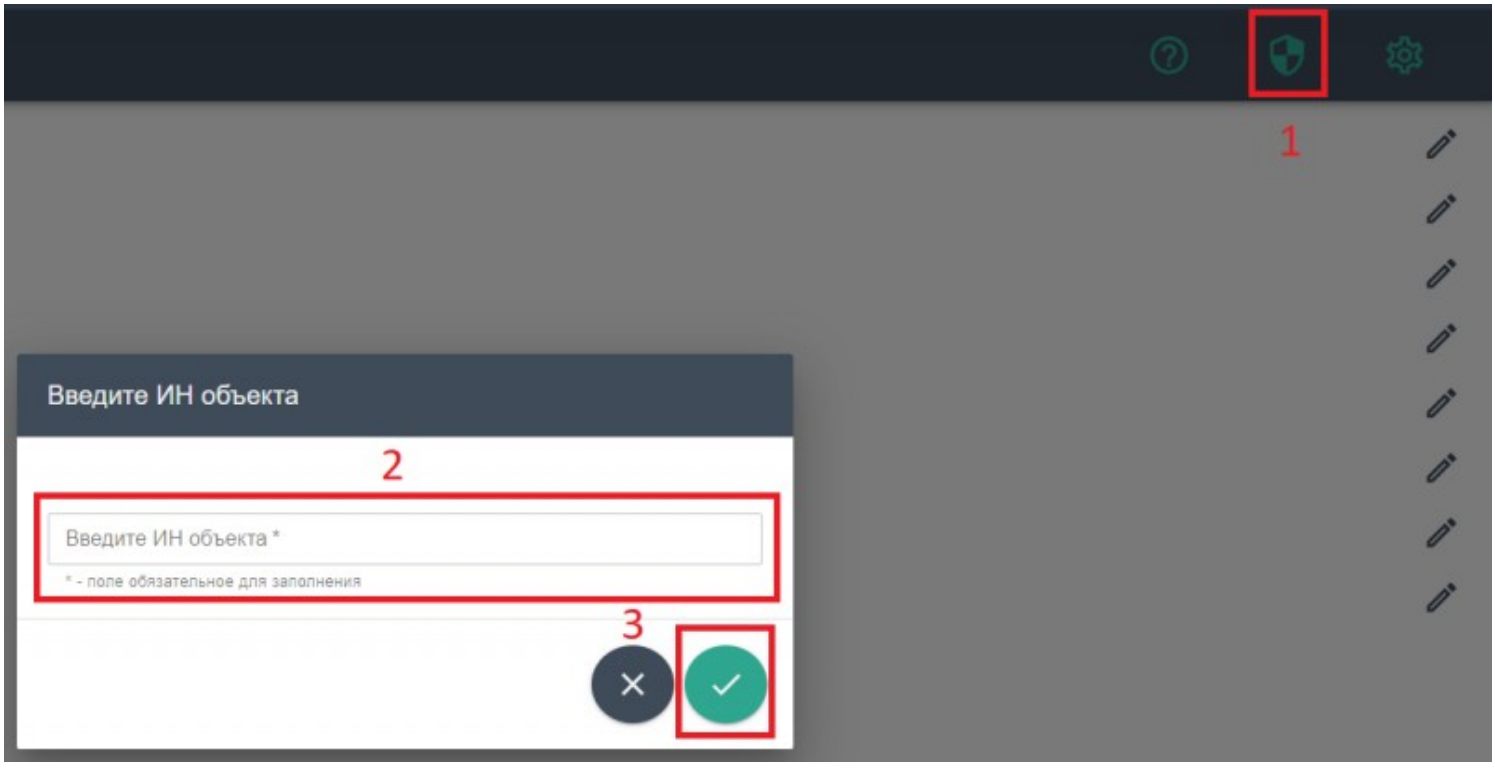
12.4 Построение оперативной карточки объекта

Для построения оперативной карточки объекта необходимо:

1. Нажать на кнопку "Оперативная карточка" (Цифра 1 на изображении ниже).

2. Ввести ИН объекта.(Цифра 2 на изображении ниже).

3. Нажать кнопку "Подтвердить".(Цифра 3 на изображении ниже). Будет построен отчет.

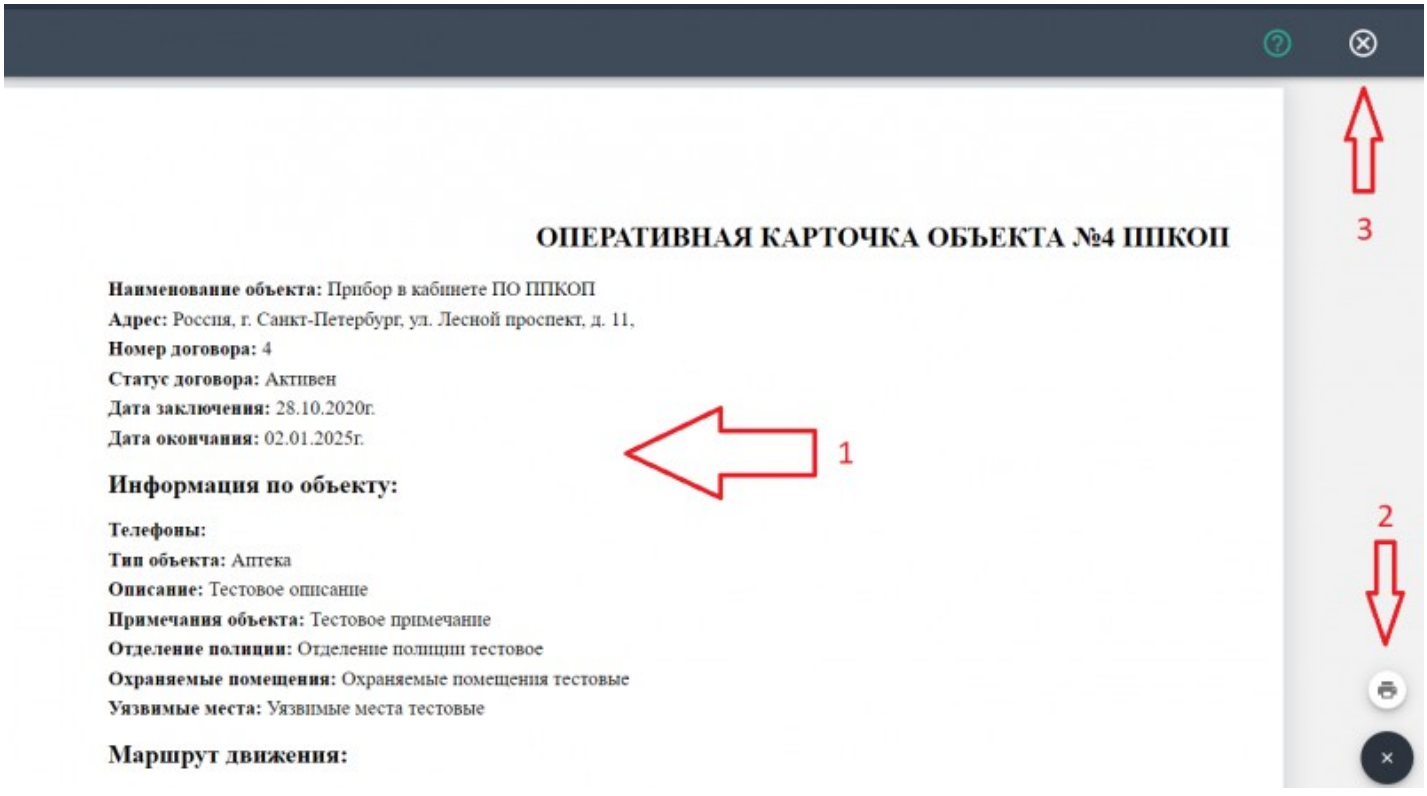


SEC.RU | Короткий путь к информации Скачано с sec.ru

Основное пространство занимает тело оперативной карточки (Цифра 1 на изображении ниже).

Для распечатывания оперативной карточки необходимо нажать на кнопку "Распечатать" (Цифра 2 на изображении ниже).

Для закрытия оперативной карточки нажать кнопку "Закрыть" (Цифра 3 на изображении ниже).



SEC.RU | Короткий путь к информации Скачано с sec.ru

Приложения

Приложение №1 Перевод IP-GPRS оборудования Юпитер-7 на Юпитер-КРОС (выгрузка полной конфигурации)

Перевод оборудования с сервера Юпитер-7 на сервер Юпитер-КРОС путем единоразовой выгрузки полной конфигурации приборов.

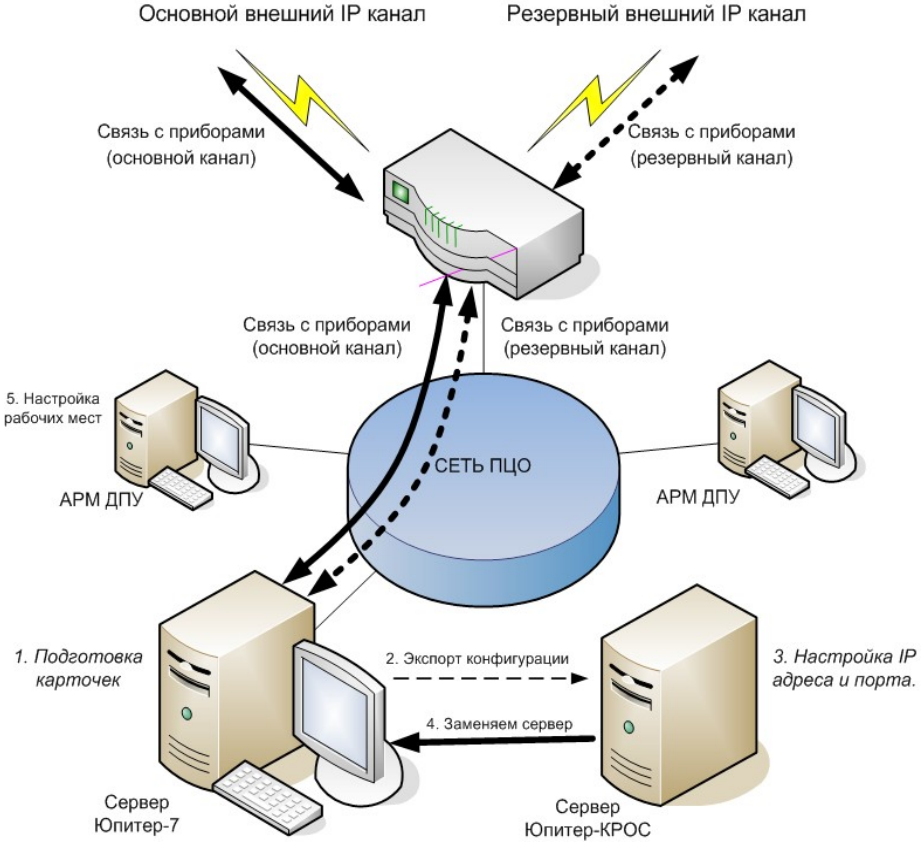
Плюсы:

- самый быстрый вариант перевода.

Минусы:

- процесс адаптации сотрудников к новому ПО происходит в «боевых условиях».

1. Концепция



SEC.RU | Короткий путь к информации Скачано с sec.ru

Последовательность операций:

1. Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС.
2. Экспорт конфигурации из Юпитер-7 на сервер Юпитер-КРОС.
3. Настройка на сервере Юпитер-КРОС тех же параметров, что использует Юпитер-7: IP-адрес компьютера-сервера внутри локальной сети, а также порт для работы с приборами.
4. Выключение сервера Юпитер-7 и установка на его место сервера Юпитер-КРОС. Так как сервер Юпитер-КРОС имеет те же настройки, что и сервер Юпитер-7 (и база данных перенесена на новый сервер), то приборы установят связь с новым сервером автоматически.
5. Настройка рабочих мест.

2. Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС

В Юпитер-7 и Юпитер-КРОС используется разные принципы заведения объектов:

- В Юпитере-7 карточки заводятся для прибора и его разделов.
- В Юпитер-КРОС карточка заводится для объекта.

Таким образом, при переносе в Юпитер-КРОС, создаются отдельные объекты для каждой импортированной карточки прибора и его разделов. В Юпитер-КРОС предусмотрен механизм объединения карточек, который будет рассмотрен ниже.

Для упрощения процесса переноса в Юпитер-7 рекомендуется удалить разделы в тех приборах, где используется только один раздел, тем самым убрав дополнительную карточку раздела, тогда при переносе будет создан только один объект в Юпитер-КРОС.

Внимание!

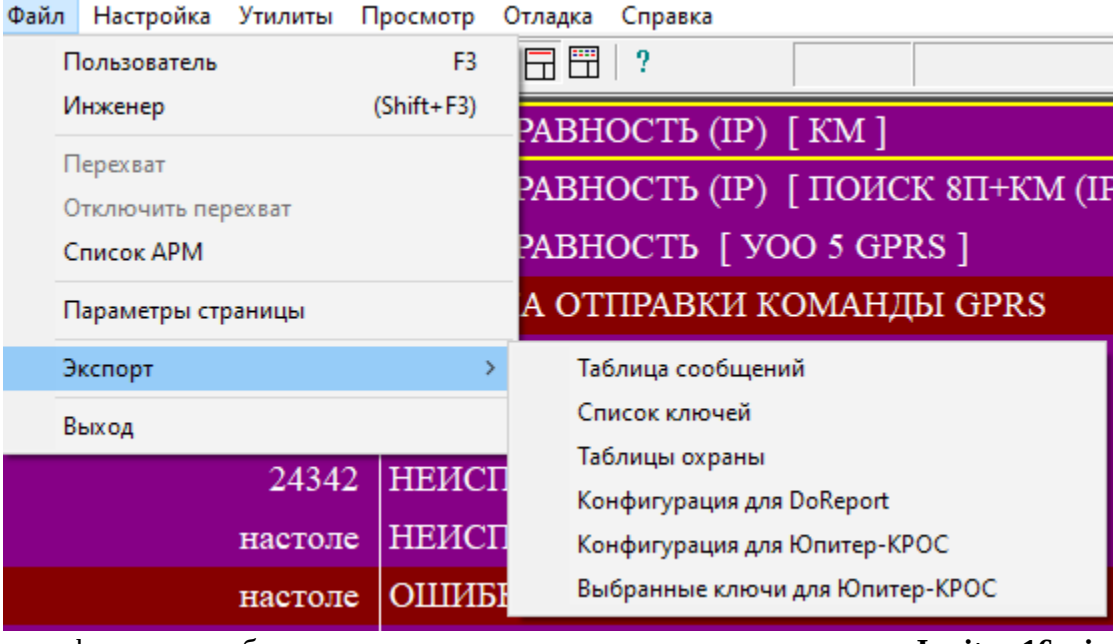
Удалять разделы в Юпитер-7 допускается только в случае, когда в приборе настроен один раздел. Если в приборе настроено 2 и более разделов, то в процессе переноса в Юпитер-КРОС будут созданы отдельные объекты для прибора и для его разделов, которые позже можно будет объединить средствами Юпитер-КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Экспорт конфигурации из Юпитер-7 в Юпитер-КРОС

Для экспорта конфигурации необходимо выполнить следующие действия:

3.1. Для экспорта конфигурации из Юпитер-7 необходимо в меню «Файл» выбрать пункт «Экспорт»/«Конфигурация для Юпитер-КРОС». Существует возможность выгрузить либо полную конфигурацию, либо только выбранные ключи.



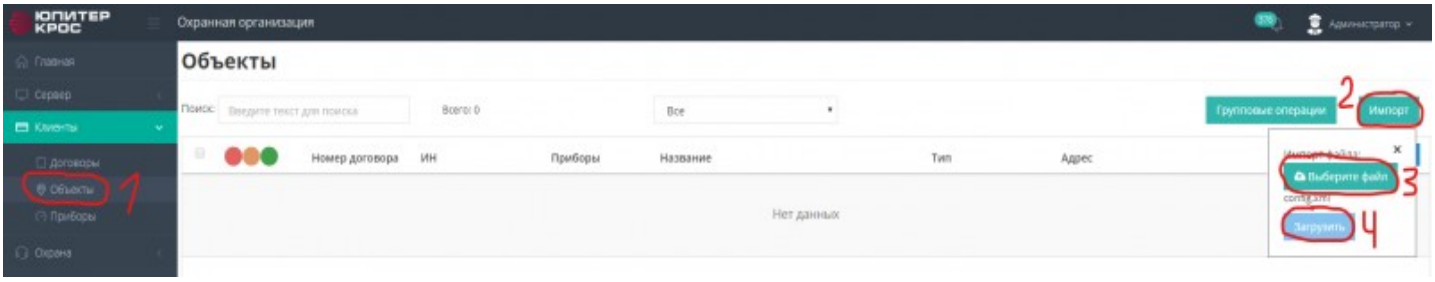
Файл конфигурации оборудования по умолчанию создается в каталоге **Jupiter-16.win**
Пример:
Jupiter-16.win\export.2017-10-17-12.20.30.zip
где ***export.2017-10-17-12.20.30.zip*** — созданный файл конфигурации.

3.2. Далее файл конфигурации необходимо перенести на компьютер, на который установлен сервер Юпитер-КРОС.

3.3. На сервере Юпитер-КРОС необходимо:

- зайти под учётной записью администратора охранной организации (*admin**admin*- логин и пароль по умолчанию)
- перейти в меню «Клиенты»-«Объекты»
- нажать кнопку «Импорт»
- выбрать файл конфигурации
- нажать кнопку «Загрузить».
- Начнётся процесс импорта. По завершению импорта необходимо обновить страницу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

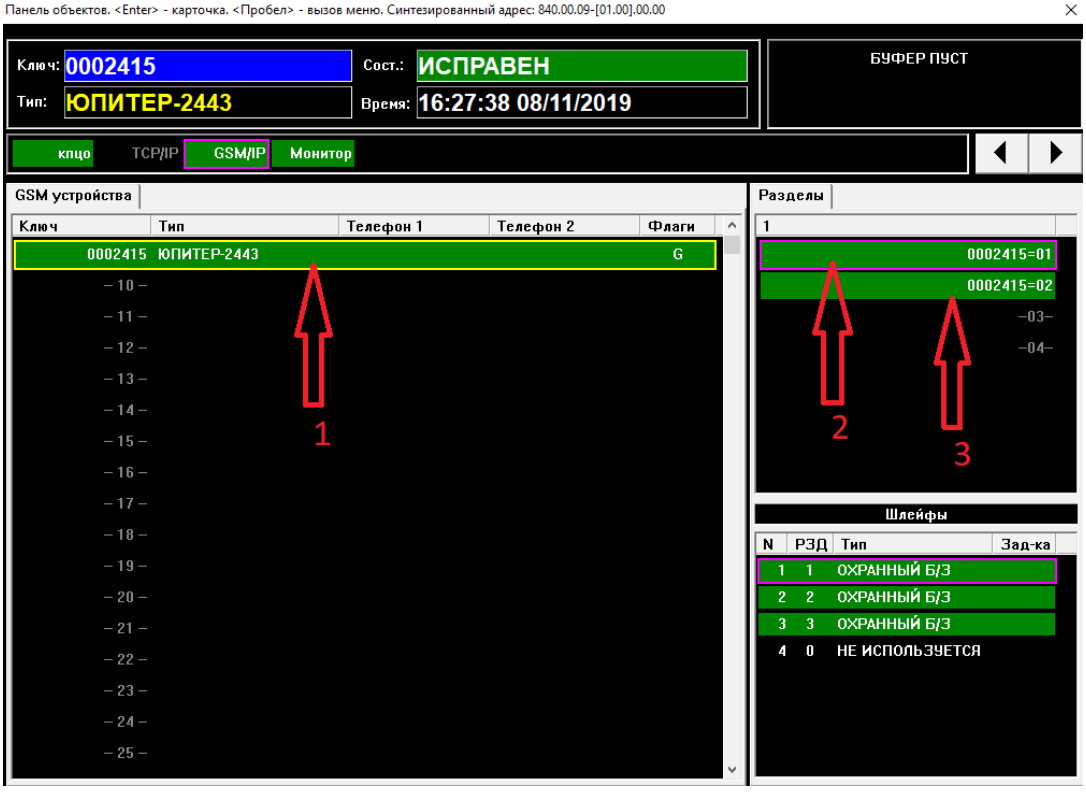


3.4. Импортированные в Юпитер-КРОС карточки объектов будут отображаться на сервере КРОС в меню «Клиенты» → «Объекты». Из-за особенностей переноса карточек из Юпитер-7 в Юпитер-КРОС для приборов, у которых есть разделы в Юпитер-7, будут созданы отдельные объекты в Юпитер-КРОС для карточек прибора и каждого из его разделов, как показано на изображении ниже.

Приборы без разделов перенесутся одним объектом и не потребуют дополнительных операций по объединению карточек.

настоле	настоле		голова прибора на столе
настоле	настоле=01	настоле	раздел на охрану отдела по2
настоле	настоле=02	настоле	Охрана отдела по3

Соответствие карточек в Юпитер 7 и Юпитер-КРОС показано на изображениях ниже:



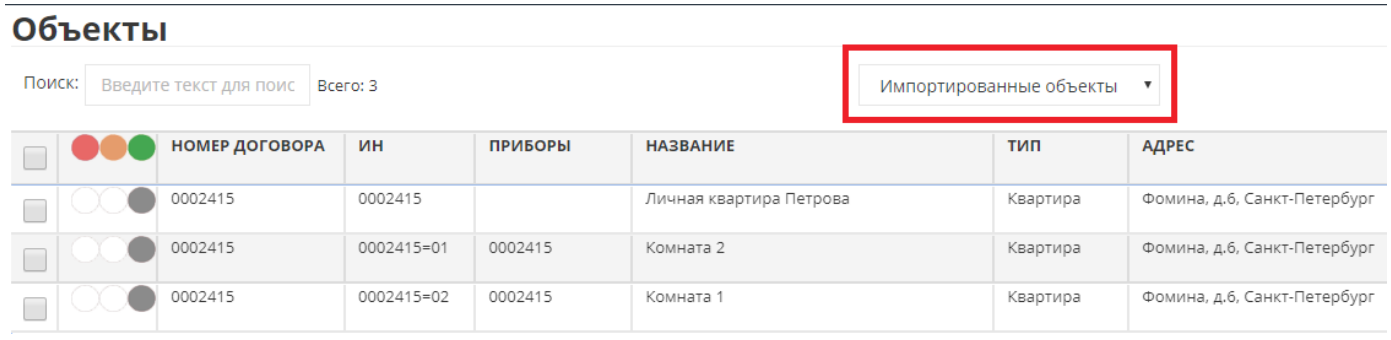
SEC.RU | Короткий путь к информации Скачано с sec.ru

	НОМЕР ДОГОВОРА	ИН	ПРИБОРЫ	НАЗВАНИЕ
	0002415	0002415	1	Личная квартира Петрова
	0002415	0002415=01	0002415 2	Комната 2
	0002415	0002415=02	0002415 3	Комната 1

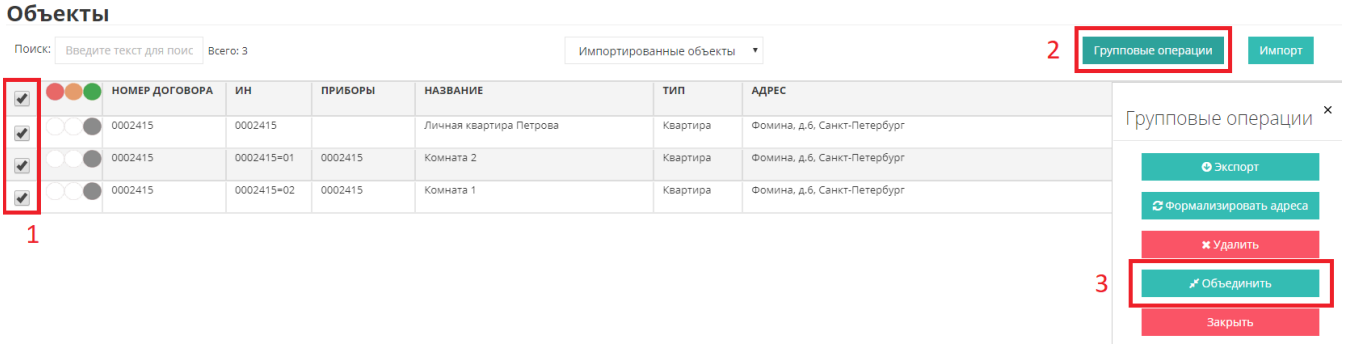
Цифра 1 — «Головная» карточка прибора с ключом «0002415»
Цифра 2 — Раздел №1 прибора «0002415»
Цифра 3 — Раздел №2 прибора «0002415»

3.5. Если перенесенные карточки прибора и раздела являются одним объектом, то эти карточки можно объединить.

Для объединения необходимо открыть меню «Клиенты»-«Объекты» и установить фильтр «Импортированные объекты».

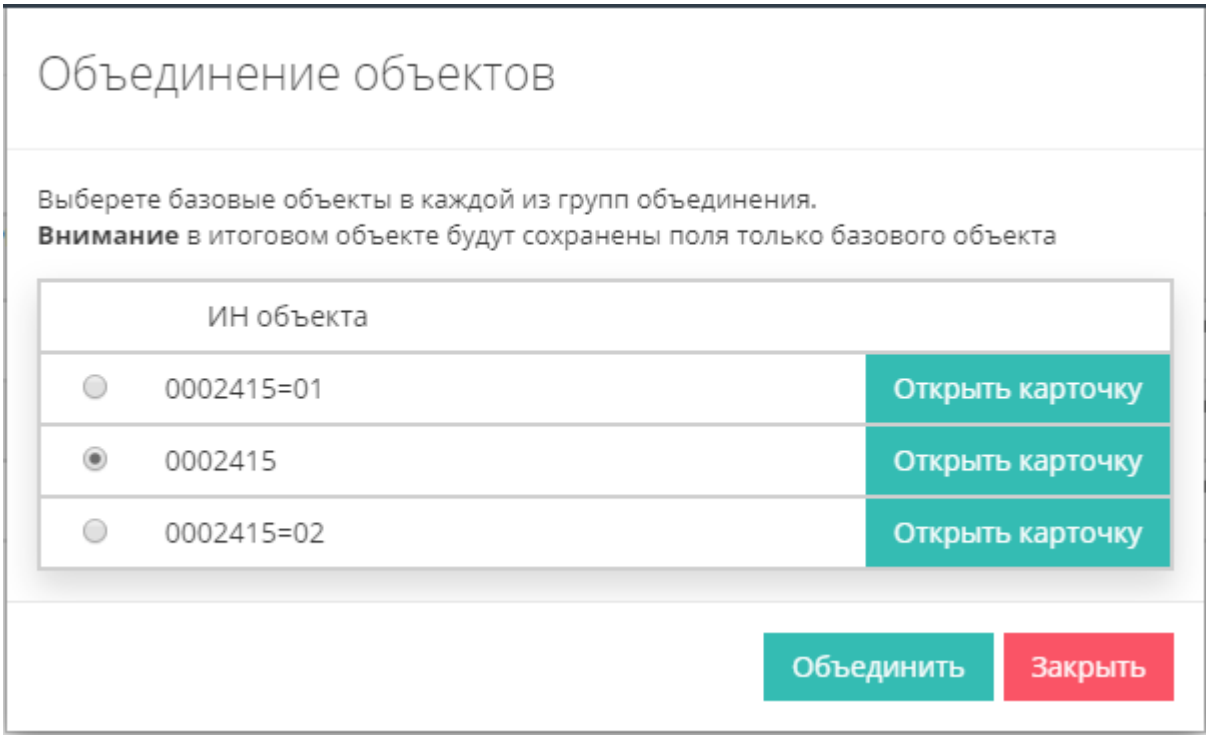


3.6. Выбрать все карточки объекта, который необходимо объединить, далее нажать кнопку «Групповые операции», далее кнопку «Объединить».

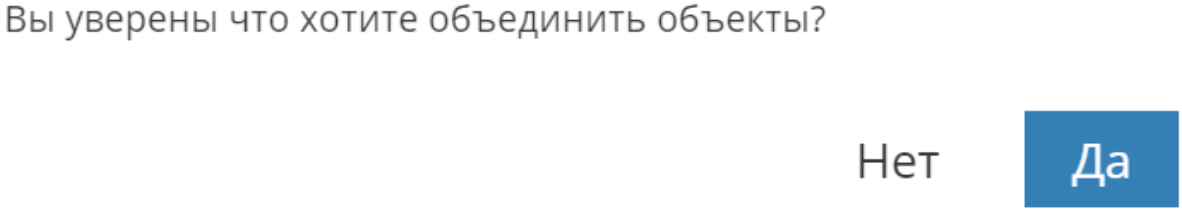


SEC.RU | Короткий путь к информации Скачано с sec.ru

3.7. Откроется окно объединения карточек. По нажатии на кнопку «Открыть карточку» откроется карточка объекта, в которой нужно проверить корректность данных импорта и, при необходимости, внести изменения. На данном этапе необходимо выбрать одну главную карточку объекта, именно она будет отображаться в Юпитер-КРОС после объединения. Данные других карточек сохранены не будут. После выбора основной карточки необходимо нажать кнопку «Объединить».

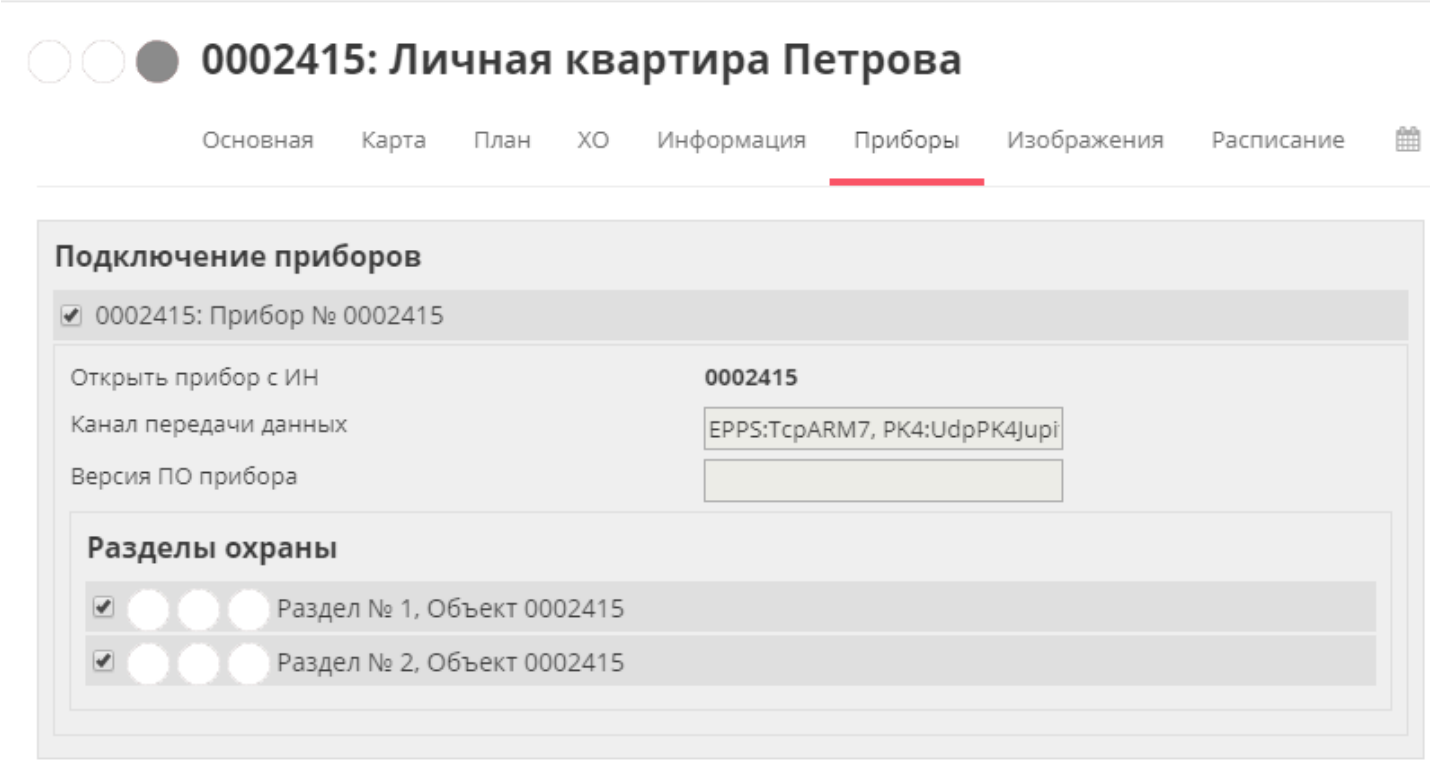


3.8. Будет запрошено подтверждение операции. Нажать «Да».



SEC.RU | Короткий путь к информации Скачано с sec.ru

3.9. После объединения карточка прибора будет выглядеть как на изображении ниже:



Как видно на изображении, осталась одна карточка объекта, к которой привязаны два раздела прибора.

4. Настройка параметров на сервере Юпитер-КРОС

Настройка порта для подключения приборов подробно описана в инструкции по развертыванию программного обеспечения СПИ Юпитер-КРОС.

Обращаем ваше внимание, что при настройке Юпитер-КРОС должен быть указан тот же самый порт, по которому приборы подключаются к Юпитер-7.

Во избежание конфликта IP-адресов следует отсоединить сетевой кабель от компьютера сервера КРОС. Далее необходимо присвоить компьютеру сервера Юпитер-КРОС IP-адрес сервера Юпитер-7.

5. Замена серверов

После выполнения всех вышеуказанных условий, необходимо отключить от сети или сменить IP-адрес на сервере Юпитер-7 и подсоединить к локальной сети сервер Юпитер-КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Так как сервер Юпитер-КРОС теперь имеет те же настройки, что и сервер Юпитер-7 (база данных перенесена на новый сервер), то приборы установят связь с новым сервером автоматически.

6. Настройка рабочих мест

Для запуска АРМ Юпитер-КРОС воспользуйтесь инструкцией “АРМ.Быстрый старт”.

7. Приборы, подлежащие переносу

Сервер Юпитер-КРОС работает со следующими системами передачи извещений и оконечными устройствами:

- GSM/IP-устройства — устройства, связанные с пультом по GSM- или IP-сетям. Система поддерживает следующие устройства:
  - УОО «Юпитер IP/GPRS»
    - Юпитер-2413 (GSM)
    - Юпитер-2443 (Ethernet+GSM)
    - Юпитер 2444 (с ЖК)
    - Юпитер 2445 (подкл.расш.)
    - Юпитер 2463 (с WI-FI)
  - УОО «Юпитер 242x»
    - УОО «Юпитер 2420»
    - УОО «Юпитер 2421»
    - УОО «Юпитер 2422»
    - УОО «Юпитер 2424»
    - УОО «Юпитер 2425»
    - УОО «Юпитер 2426»
    - УОО «Юпитер 2427»
    - УОО «Юпитер 2428»
    - УОО «Юпитер 2429»
  - УОО «Юпитер-232x»
    - УОО «Юпитер 2320»
    - УОО «Юпитер 2321»
    - УОО «Юпитер 2326»
  - ППКОП «Юпитер IP/GPRS»
    - Юпитер-1431, 4 ШС, без клавиатуры
    - Юпитер-1433, 4 ШС, с клавиатурой
    - Юпитер 1831, 8 ШС, без клавиатуры
    - Юпитер 1833, 8 ШС, с клавиатурой
    - Юпитер 1931, 16 ШС, без клавиатуры
    - Юпитер 1933, 16 ШС, с клавиатурой
  - ППКОП "ЮПИТЕР-4GSM"

SEC.RU | Короткий путь к информации Скачано с sec.ru

Приложение №2 Перевод IP-GPRS оборудования Юпитер-7 на Юпитер-КРОС (поэтапный перенос)

Перевод оборудования с сервера Юпитер-7 на сервер Юпитер-КРОС путем постепенного переноса приборов.

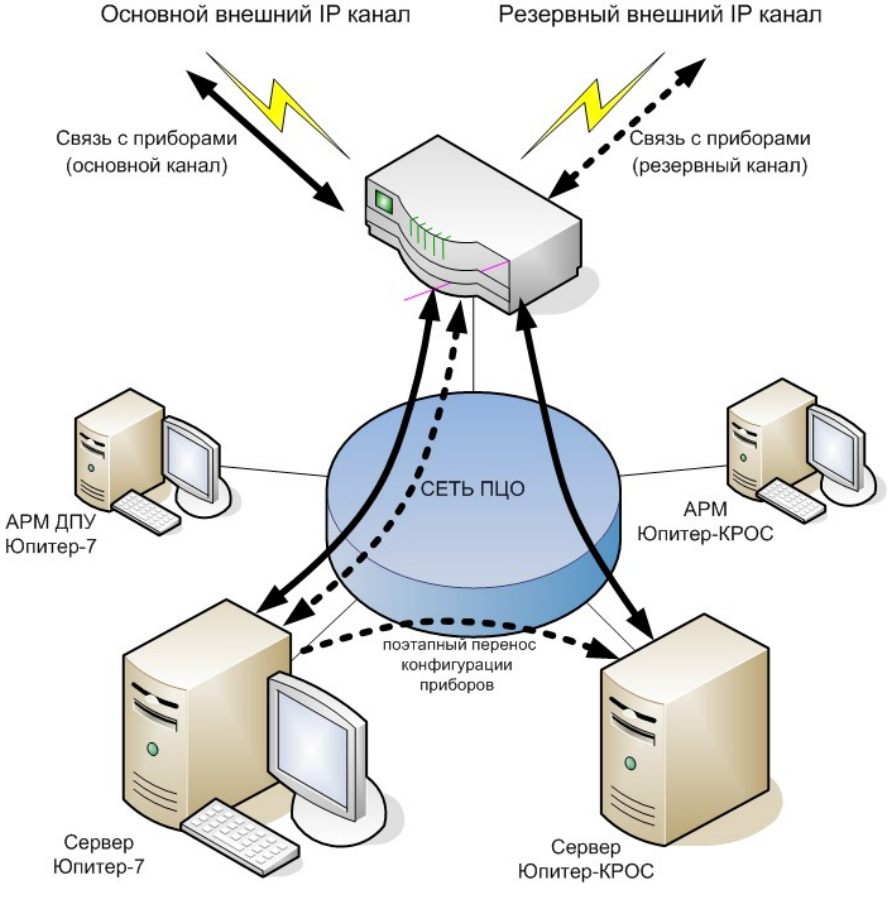
Плюсы:

- постепенная адаптация персонала к новому ПО.
- самая надёжная схема, так как фактически перевод каждого объекта происходит под полным контролем инженера.
- сразу же сверяются перенесённые данные, приводятся в порядок карточки объектов.
- хороший вариант для крупных пультов, особенно в случае объединения нескольких серверов Юпитер.

Минусы:

- более растянутый по времени перевод объектов.
- в период перехода необходимо работать сразу с двумя системами.

1. Концепция:



SEC.RU | Короткий путь к информации Скачано с sec.ru

Сервер Юпитер-КРОС разворачивается параллельно с существующим сервером Юпитер-7.

Новые объекты заводятся на сервер Юпитер-КРОС, одновременно идет процесс постепенного переноса объектов с Юпитер-7 на Юпитер-КРОС.

2. Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС

В Юпитер-7 и Юпитер-КРОС используется разные принципы заведения объектов:

- В Юпитере-7 карточки заводятся для прибора и его разделов.
- В Юпитер-КРОС карточка заводится для объекта.

Таким образом при переносе в Юпитер-КРОС создаются отдельные объекты для каждой импортированной карточки прибора и его разделов. В Юпитер-КРОС предусмотрен механизм объединения карточек, который будет рассмотрен ниже.

Для упрощения процесса переноса, в Юпитер-7 рекомендуется удалить разделы в тех приборах, где настроен только один раздел, тем самым убрав дополнительную карточку раздела, и при переносе будет создан только один объект в Юпитер-КРОС.

Внимание!

Удалять разделы в Юпитер-7 допускается только в случае, когда в приборе настроен один раздел. Если в приборе настроено 2 и более разделов, то в процессе переноса в Юпитер-КРОС будут созданы отдельные объекты для прибора и для его разделов, которые позже можно будет объединить средствами Юпитер-КРОС.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Автоматизированный механизм переноса объектов

Между АРМ Юпитер-7 и Юпитер-КРОС реализован автоматический перенос приборов.

Процесс переноса представляет из себя передачу в Юпитер-КРОС данных экспорта, для выбранных приборов, и автоматическая смена в настройках прибора 3-го IP-адреса и порта пульта для обмена сообщениями по GPRS/Ethernet.

В приборе имеется, для двух SIM-карт и сети Ethernet, по три IP-адреса и порта соответственно.

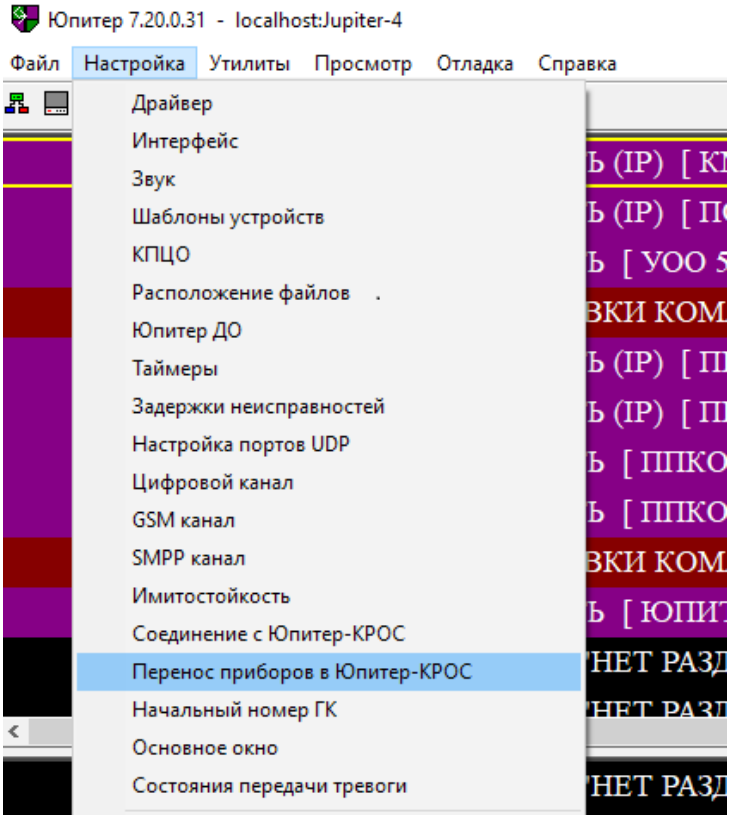
Если прибор использует для связи с Юпитер-7 первый или второй IP-адрес и порт, то изменение третьего не приведет к потере связи с прибором.

Если (в качестве третьего IP-адреса и порта) будет назначен IP-адрес и порт Юпитер-КРОС, то (при блокировке этого прибора в Юпитер-7) прибор будет пытаться соединиться с пультом, перебирая все три варианта. Дойдя до 3-го адреса он соединиться с Юпитер-КРОС.

Далее, в процессе работы с 3-им адресом, первый или второй адрес можно также переназначить на Юпитер-КРОС.

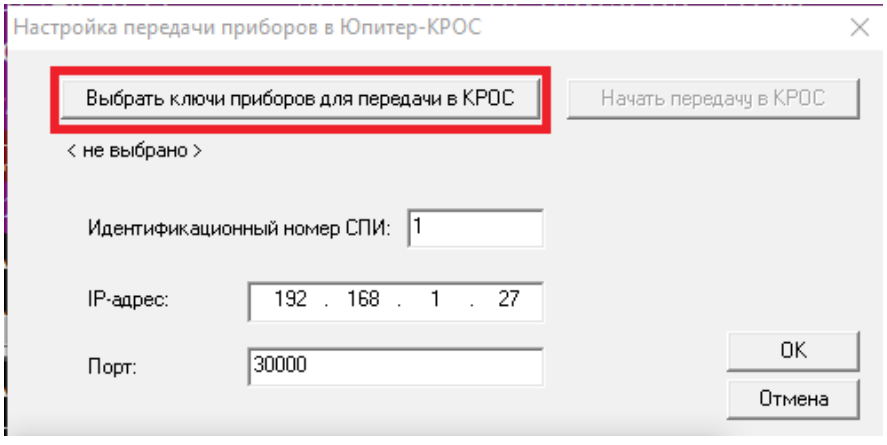
Для осуществления переноса приборов необходимо:

3.1. В Юпитер-7, в меню «Настройка» выбрать пункт «Перенос приборов в Юпитер-КРОС».

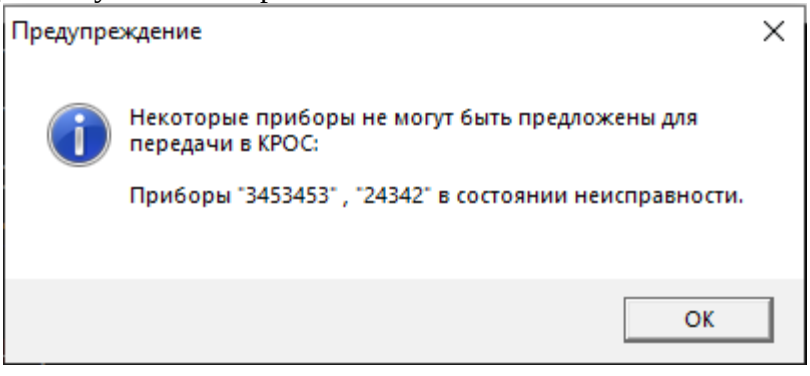


SEC.RU | Короткий путь к информации Скачано с sec.ru

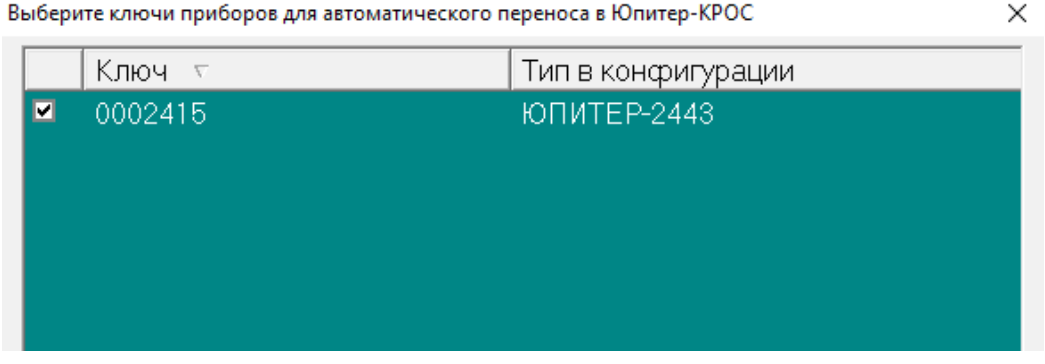
3.2. В появившемся окне нажать на кнопку «Выбрать ключи приборов для передачи в КРОС».



3.3. Если какие-либо приборы не могут быть переданы в Юпитер-КРОС, то появится предупреждение с указанием причины.



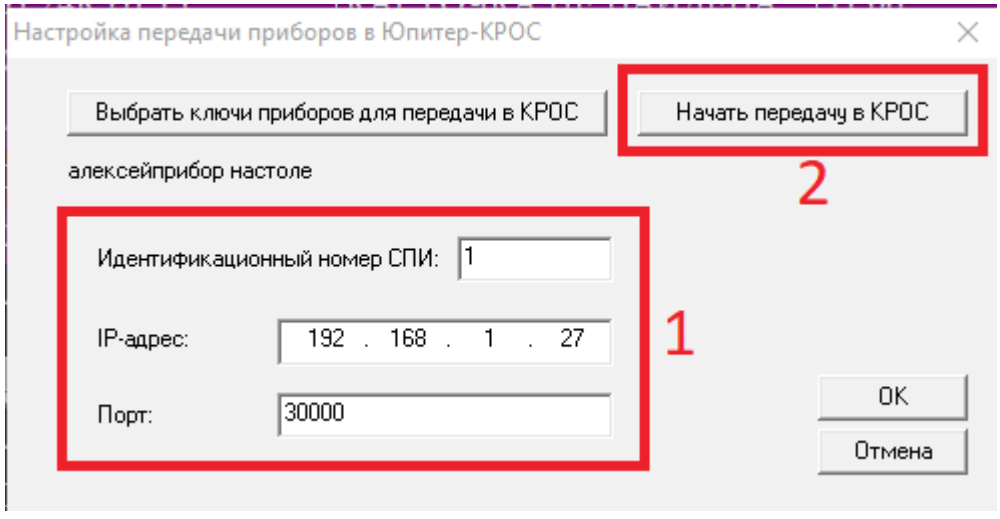
3.4. В появившемся окне выбрать приборы, которые необходимо перенести в Юпитер-КРОС, и нажать кнопку «OK».



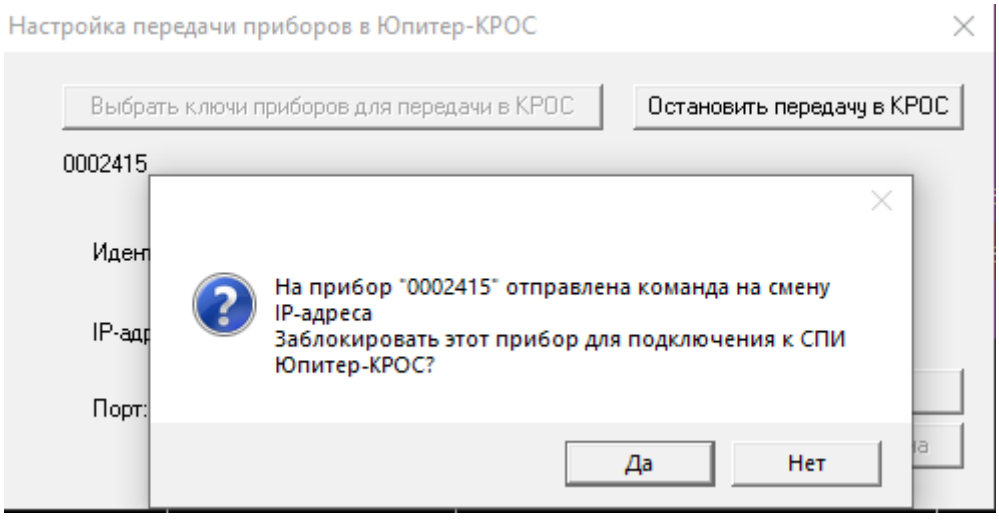
SEC.RU | Короткий путь к информации Скачано с sec.ru

3.5. Внести данные для соединения Юпитер-7 и Юпитер-КРОС:

a) Идентификационный номер СПИ —по умолчанию оставить 1
b) IP-адрес — ввести IP-адрес сервера КРОС
c) Порт — по умолчанию оставить 30000
d) После введения всех данных нажать «Начать передачу в КРОС», далее «ОК»



3.6. После передачи команд на смену IP-адресов будет предложено заблокировать переведенные приборы в Юпитер-7 чтобы они могли переключиться на Юпитер-КРОС. Необходимо выбрать «Да», в противном случае карточки приборов на Юпитер-КРОС будут созданы, однако приборы продолжат соединяться с Юпитер-7.

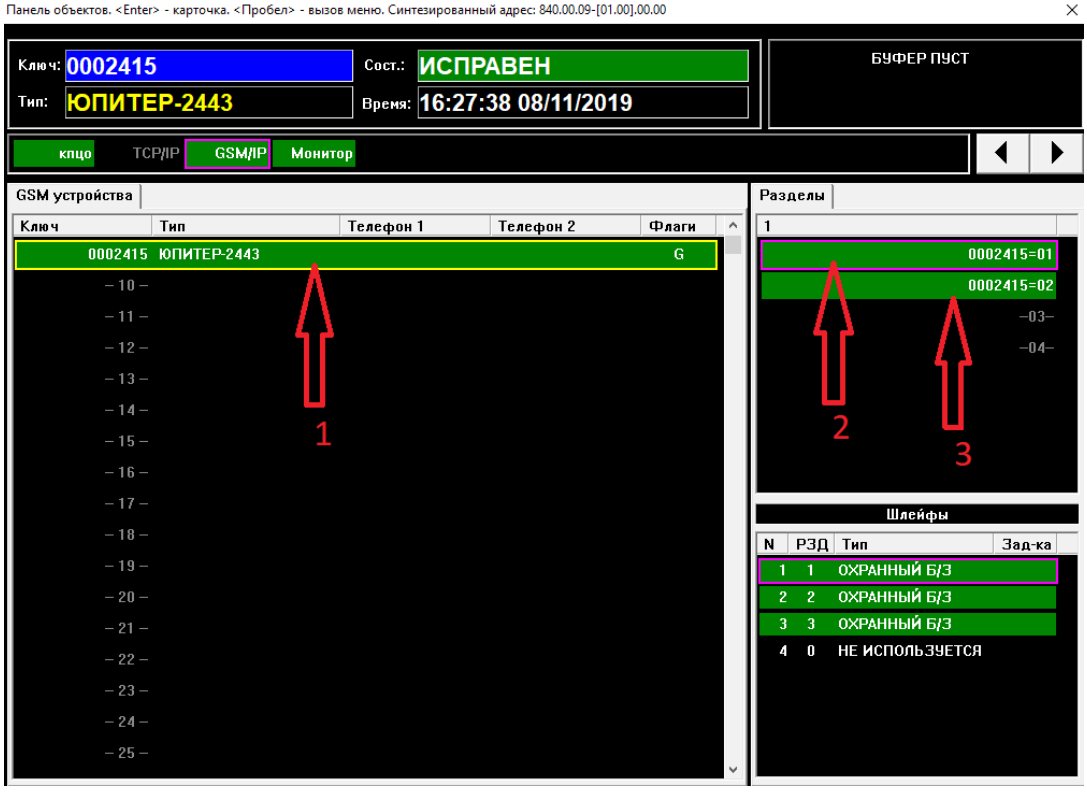


SEC.RU | Короткий путь к информации Скачано с sec.ru

3.7. Необходимо зайти на сервер КРОС под учетной записью администратора охранной организации (*admin\admin* - логин и пароль по умолчанию).
Импортированные в Юпитер-КРОС карточки объектов будут отображаться на сервере КРОС в меню «Клиенты»→«Объекты». Из-за особенностей переноса карточек из Юпитер-7 в Юпитер-КРОС для приборов, у которых есть разделы в Юпитер-7, будут созданы отдельные объекты в Юпитер-КРОС для карточек прибора и каждого из его разделов, как показано на изображении ниже.

настоле	настоле		голова прибора на столе
настоле	настоле=01	настоле	раздел на охрану отдела по2
настоле	настоле=02	настоле	Охрана отдела по3

Соответствие карточек в Юпитер 7 и Юпитер-КРОС показано на изображениях ниже:



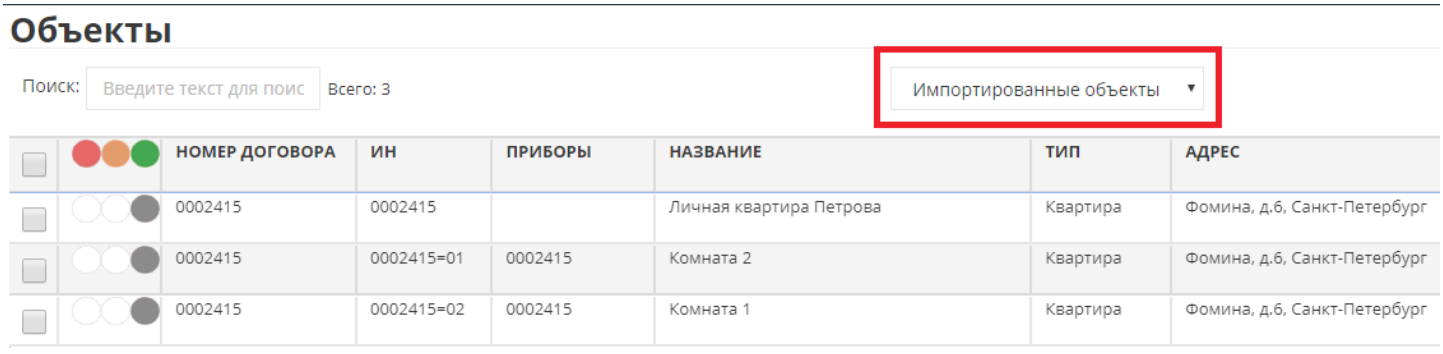
SEC.RU | Короткий путь к информации Скачано с sec.ru

	НОМЕР ДОГОВОРА	ИН	ПРИБОРЫ	НАЗВАНИЕ
	0002415	0002415	1	Личная квартира Петрова
	0002415	0002415=01	0002415 2	Комната 2
	0002415	0002415=02	0002415 3	Комната 1

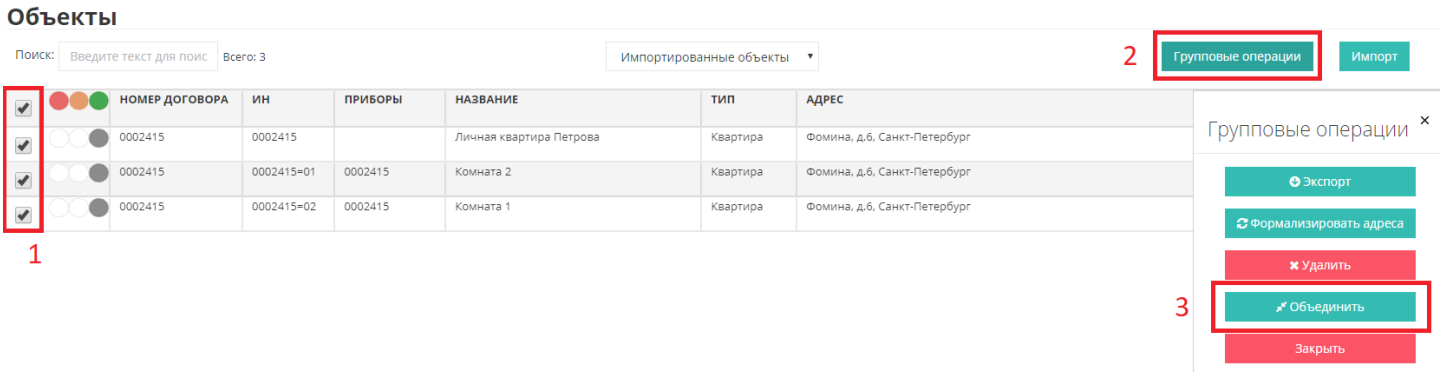
Цифра 1 — «Головная» карточка прибора с ключом «0002415»
Цифра 2 — Раздел №1 прибора «0002415»
Цифра 3 — Раздел №2 прибора «0002415»

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.8. Если перенесенные карточки прибора и раздела являются одним объектом, то эти карточки можно объединить.
Для объединения необходимо открыть меню «Клиенты» → «Объекты» и выставить фильтр «Импортированные объекты».



3.9. Выбрать все карточки объекта, который необходимо объединить, после чего нажать кнопку «Групповые операции» и кнопку «Объединить».

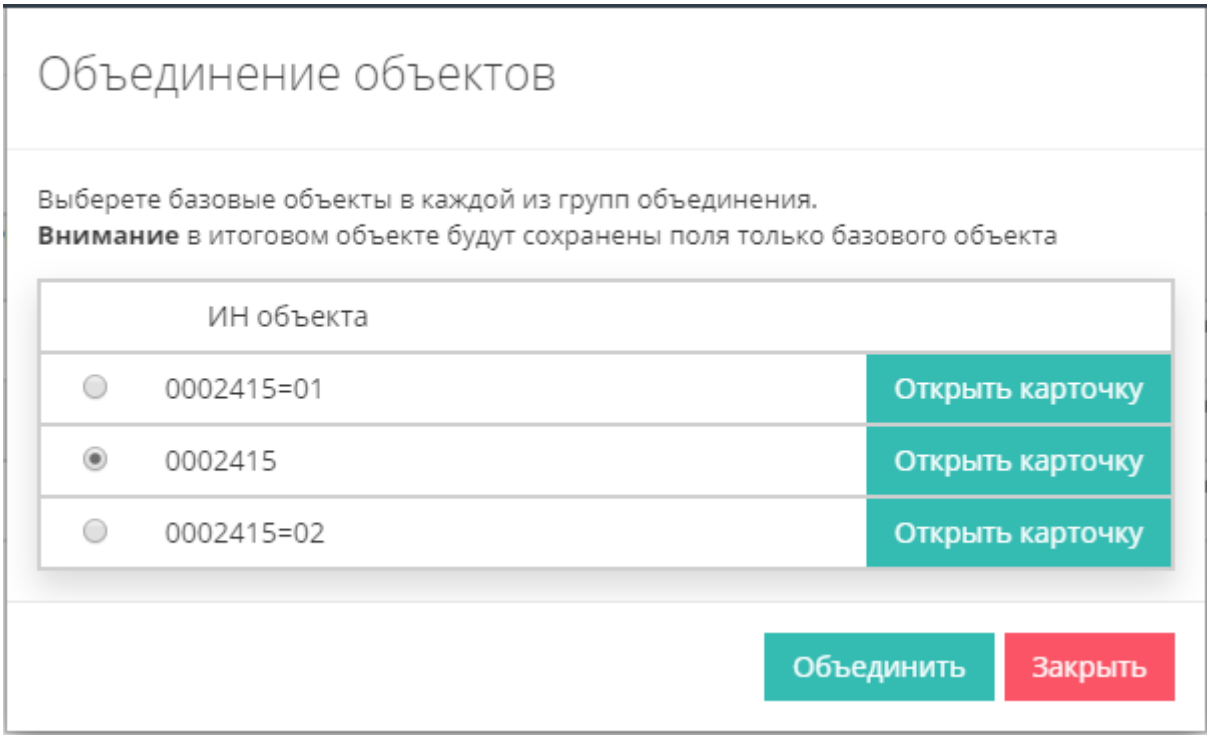


SEC.RU | Короткий путь к информации Скачано с sec.ru

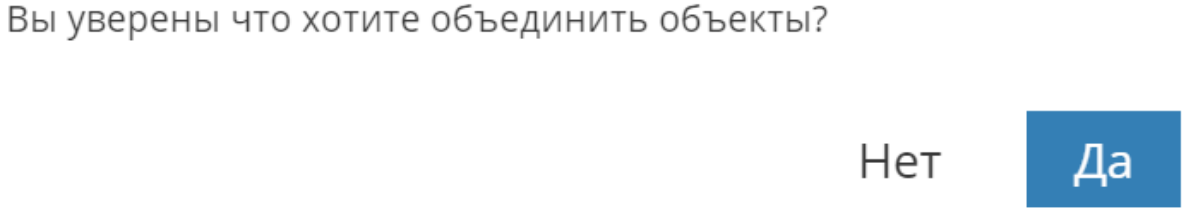
3.10. Откроется окно объединения карточек.

По нажатии на кнопку «Открыть карточку» откроется карточка объекта в которой нужно проверить корректность данных импорта, и при необходимости внести изменения.

На данном этапе необходимо выбрать одну главную карточку объекта, именно она будет отображаться в Юпитер-КРОС после объединения. Данные других карточек сохранены не будут. После выбора основной карточки необходимо нажать кнопку «Объединить».

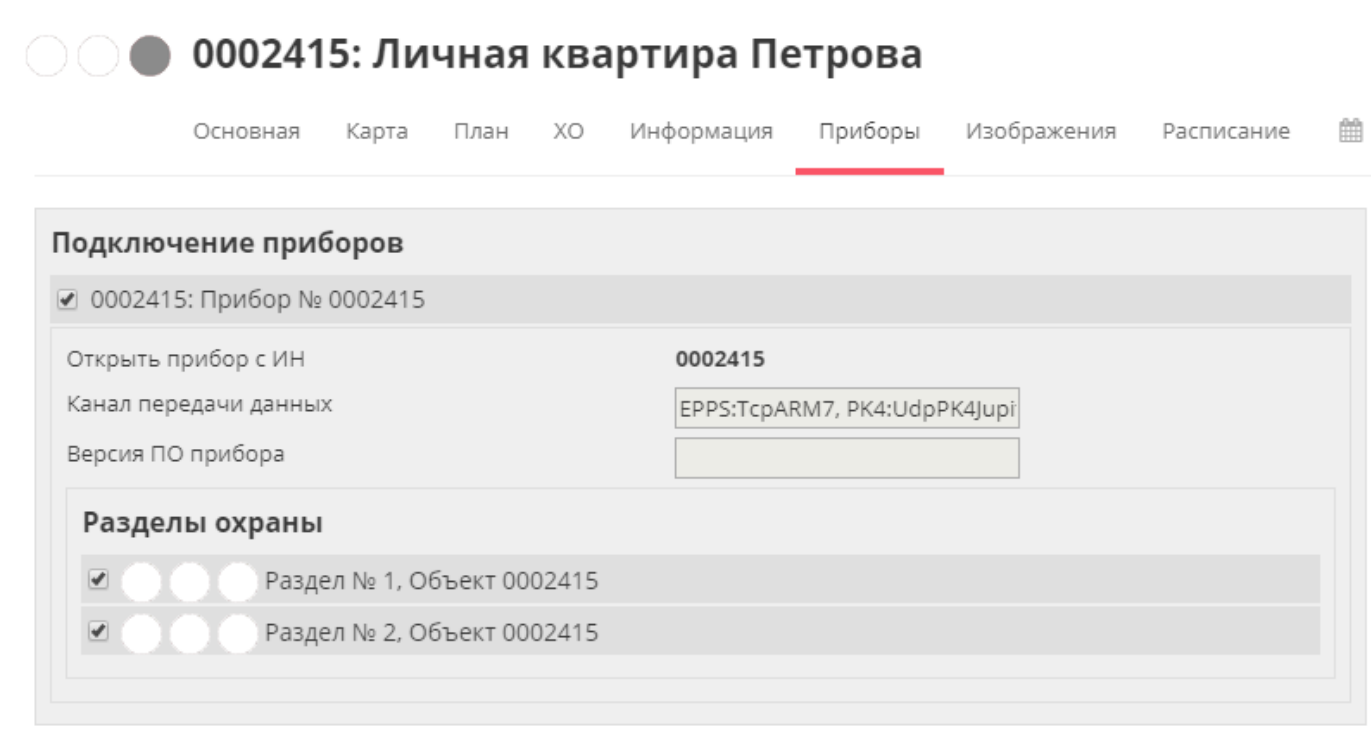


3.11. Будет запрошено подтверждение операции. Нажать «Да».



SEC.RU | Короткий путь к информации Скачано с sec.ru

3.12. После объединения карточка прибора будет выглядеть как на изображении ниже:



Как видно на изображении, осталась только одна карточка объекта к которой привязаны два раздела прибора.

3.13. После того, как все приборы вышли на связь с Юпитер-КРОС, необходимо поменять IP-адреса серверов приема сообщений, настроенных в приборе для сервера Юпитер-7 на основной и резервный адрес Юпитер-КРОС.

Для этого нужно:

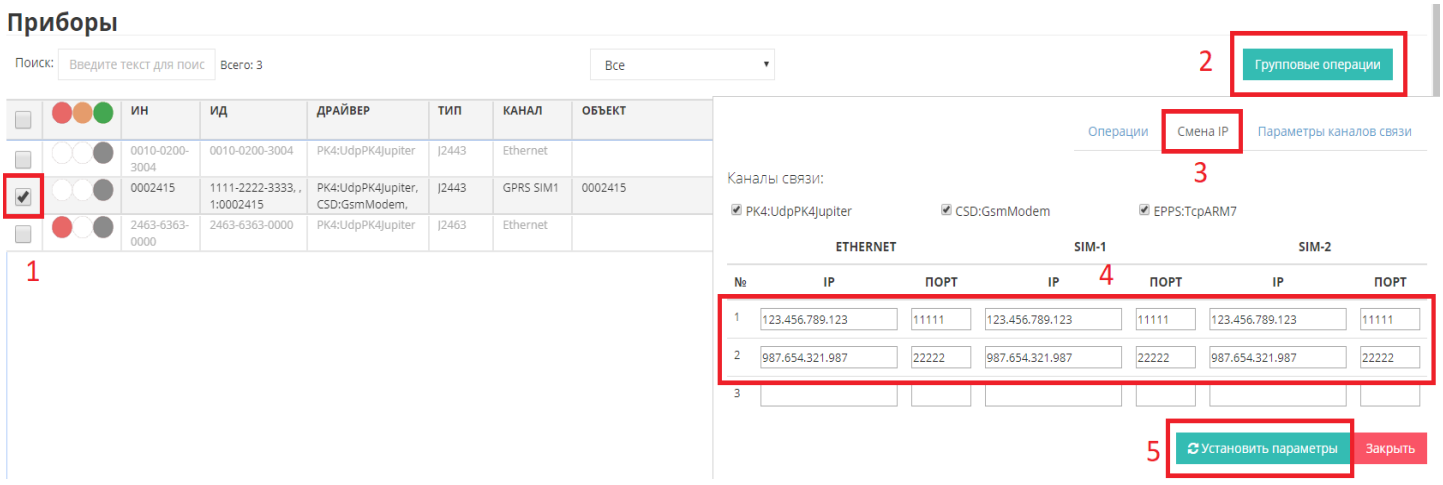
a) Выбрать приборы, IP-адреса которых необходимо поменять
b) Нажать кнопку «Групповые операции», далее выбрать меню «Смена IP»
c) В поле №1 внести основной IP-адрес и порт, в поле №2 внести резервный IP-адрес и порт, поле №3 заполнить нулями.
d) После внесения адресов и портов нажать кнопку «Установить параметры».

   При необходимости успешность смены IP-адресов можно проверить, запустив удаленный конфигуратор.

   Внимание!

   Прибор должен находиться в снятом состоянии, чтобы иметь возможность сменить IP-адрес и порт.

SEC.RU | Короткий путь к информации Скачано с sec.ru



Данный механизм позволяет осуществить поэтапный перенос объектов.
Когда процесс переноса будет завершен, сервер Юпитер-7 может быть отключен.

4. Приборы, подлежащие переносу

Сервер Юпитер-КРОС работает со следующими системами передачи извещений и оконечными устройствами:

- GSM/IP-устройства — устройства, связанные с пультом по GSM- или IP-сетям. Система поддерживает следующие устройства:
  - УОО «Юпитер IP/GPRS»
    - Юпитер-2413 (GSM)
    - Юпитер-2443 (Ethernet+GSM)
    - Юпитер 2444 (с ЖК)
    - Юпитер 2445 (подкл.расш.)
    - Юпитер 2463 (с WI-FI)
  - УОО «Юпитер 242x»
    - УОО «Юпитер 2420»
    - УОО «Юпитер 2421»
    - УОО «Юпитер 2422»
    - УОО «Юпитер 2424»
    - УОО «Юпитер 2425»
    - УОО «Юпитер 2426»
    - УОО «Юпитер 2427»
    - УОО «Юпитер 2428»
    - УОО «Юпитер 2429»
  - УОО «Юпитер-232x»
    - УОО «Юпитер 2320»
    - УОО «Юпитер 2321»
    - УОО «Юпитер 2326»

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ППКОП «Юпитер IP/GPRS»
  - Юпитер-1431, 4 ШС, без клавиатуры
  - Юпитер-1433, 4 ШС, с клавиатурой
  - Юпитер 1831, 8 ШС, без клавиатуры
  - Юпитер 1833, 8 ШС, с клавиатурой
  - Юпитер 1931, 16 ШС, без клавиатуры
  - Юпитер 1933, 16 ШС, с клавиатурой
- ППКОП "ЮПИТЕР-4GSM"

SEC.RU | Короткий путь к информации Скачано с sec.ru