Комплекс распределенной обработки сообщений Юпитер-КРОС

Версия 2.6.1

ЕАСД. 582940.000-00 РЭ

Руководство по эксплуатации

ред 2.6

Санкт-Петербург
2026

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

Оглавление

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
2. Авторизация и роли пользователей 13
2.1 Авторизация 13
2.2 Роли и пользователи 14
2.2.1 Права пользователя superadmin 14
2.2.2 Пользователь Администратор предприятия 14
2.2.3 Менеджер 15
2.2.4 Инженер 15
2.3 Смена пользователя 16
4. Меню «Главная» 17
4.1 Состояние объектов 18
4.2 Состояние приборов 19
4.3 Используемые порты 20
4.4 Монитор 21
5. Меню «Сервер» 22
5.1 Приемники 22
5.1.1 Настройка приемников 23
5.1.1.1 Параметры приемников 25
5.1.1.1.1 Информация 25
5.1.1.1.2 Таймеры 26
5.1.1.1.3 Параметры 27
5.2 Передатчики 28
5.2.1 Настройка передатчиков 28
5.2.1.1 Параметры передатчиков 28
5.2.1.1.1 Информация 28
5.2.1.1.2 Параметры 29
5.3 Трансляции 30
5.3.1 Таблица трансляций 30
5.3.2 Создание трансляций 31
5.3.1 Добавление трансляции 31
5.3.1.1 Драйвер трансляции 32
5.3.1.1.1 Запись потока сообщений в CSV файл 34
5.3.1.1.2 Трансляция данных по протоколу SurGard(SurGard V4) 34
5.3.1.1.3 Ретранслятор пакетов в формате Envelope/JSON 37
5.3.1.1.4 Передача информации по протоколу ЕППС(Зеркалирование) 38
5.3.1.1.5 Трансляция по протоколу УАРМ 41
5.3.1.2 Таблица перекодировки 42
5.3.1.3 Зона ответственности 43
5.3.2 Сохранение, редактирование и удаление настроек трансляции 45
5.4 Таблицы 45

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

5.4.1 Описание раздела и полей таблиц сообщений/извещений 46
5.4.2 Добавление таблицы 47
5.4.3 Редактирование сообщения в таблице 48
5.4.4 Удаление таблицы сообщений 49
6. Меню «Клиенты» 50
6.1 Договоры 50
6.1.1 Добавление, редактирование и удаление договора охраны 52
6.1.1.1 Учётная карточка договора охраны 52
6.1.1.1.1 Вкладка «Основная» 52
6.1.1.1.2 Вкладка «Реквизиты» 54
6.1.1.1.3 Вкладка «Объекты» 57
6.1.1.2 Сохранение, редактирование и удаление договора охраны 57
6.1.2 Групповые операции с договорами охраны 58
6.1.3 Иерархия 59
6.2 Объекты 60
6.2.1 Добавление, редактирование и удаление объекта охраны 62
6.2.1.1 Учётная карточка объекта 62
6.2.1.1.1 Вкладка «Основная» 62
6.2.1.1.2 Вкладка «Информация» 65
6.2.1.1.3 Вкладка «Карта» 66
6.2.1.1.3 Вкладка «ХО» 67
6.2.1.1.4 Вкладка «План и Изображения» 71
6.2.1.1.4 Вкладка «Расписание охраны» 72
6.2.1.1.5 Вкладка «Приборы» 76
6.2.1.2 Сохранение, редактирование и удаление данных карточки объекта 77
6.2.2 Групповые операции с объектами охраны 78
6.3 Приборы 79
6.3.1 Учётная карточка прибора. Регистрация прибора в ручном режиме 82
6.3.2 Учётная карточка прибора. Регистрация прибора в штатном режиме 83
6.3.2.1 Вкладка «Основные» 84
6.3.1.2 Вкладка «Каналы связи» 87
6.3.1.2.1 Канал РК4 87
6.3.1.2.2 Канал EPPS 88
6.3.1.2.3 Канал CID 88
6.3.1.2.4 Канал UARM 88
6.3.1.2.5 Канал CSD 88
6.3.1.2.6 Канал TCP 89
6.3.1.2.7 Настройка параметров сообщений о потере канала связи 89
6.3.1.2.8 Удаление канала связи 89
6.3.1.3 Вкладка «СИМ-карты» 89
6.3.1.4 Вкладка «Зоны и разделы» 91
6.3.1.5 Вкладка «Расширители» 92
6.3.1.6 Вкладка «События» 93
6.3.1.6 Вкладка «Состояние» 95
6.3.2 Сохранение, редактирование и удаление записи прибора 95
6.3.3 Подмена прибора 96
6.3.4 Удаленное обновление ПО прибора 97
6.3.5 Групповые операции с приборами охраны 98

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

6.3.5.1 Групповые операции с приборами охраны. Вкладка «Операции» 98
6.3.5.2 Групповые операции с приборами охраны. Вкладка «Смена IP» 99
6.3.5.2 Групповые операции с приборами охраны. Вкладка «Параметры каналов связи» 99
6.4 Ответственные лица 100
6.4.1 Добавление и редактирование ответственного лица 102
6.4.1.1 Учетная карточка Ответственного лица 102
7. Меню «Охрана» 106
7.1 Реквизиты 106
7.1.1 Реквизиты охранной организации. Вкладка «Основные Данные» 107
7.1.2 Реквизиты охранной организации. Вкладка «Реквизиты» 109
7.1.3 Реквизиты охранной организации. Вкладка «Параметры» 110
7.1.3.1 Параметры соединения 111
7.1.3.2 Активность GSM Модема 111
7.1.3.3 Каналы IP Модема 112
7.1.3.4 Инженерный режим 113
7.1.3.5 Режим работы 114
7.1.3.6 Обработка тревог 115
7.1.3.7 Режим работы АРМ 116
7.1.3.8 Контроль резервного питания 117
7.1.3.9 Параметры учета состояния договора 117
7.1.3.10 Настройки доступа к SMPP серверу 118
7.1.3.10.1 Настройки доступа к SMPP серверу 118
7.1.3.10.2 Создание Таблицы фильтра для СМС 119
7.1.3.10.3 Включение СМС информирования для Ответственного лица 119
7.1.4 Реквизиты охранной организации. Вкладка "Тарификация" 119
7.1.5 Реквизиты охранной организации. Вкладка "Календарь" 119
7.1.6 Сохранение, редактирование и удаление данных 120
7.2 Учетные записи 121
7.2.1 Карта пользователя 121
7.2.1.1 Карта пользователя. Вкладка «Идентификация» 121
7.2.1.2 Карта пользователя. Вкладка «Работа в КРОС» 122
7.2.1.3 Карта пользователя. Вкладка «Параметры» 123
7.2.1.4 Карта пользователя. Вкладка «Фильтры» 124
7.2.3 Сохранение, редактирование и удаление учетной записи 126
7.3 Группы задержания 126
7.3.1 Карточка учёта ГЗ 127
7.3.1.1 Карточка учёта ГЗ. Вкладка «Основное» 127
7.3.1.2 Карточка учёта ГЗ. Вкладка «Зона ответственности» 127
7.3.1.1 Карточка учёта ГЗ. Вкладка «Редактирование геозоны» 129
7.3.2 Сохранение, Редактирование и Удаление записи о ГЗ 130
8. Меню «Администрирование» 131
8.1 Администрирование. Система 131
8.1.1 Система. Вкладка «Сервер» 132
8.1.2 Система. Вкладка «Вкладка «SMTP сервер» 133
8.1.3 Система. Вкладка «Вкладка «HTTP сервер» 134
8.1.4 Система. Вкладка «Вкладка «Репозиторий» 136
8.1.5 Система. Вкладка «Вкладка «Блок DDos» 138
8.1.6 Система. Вкладка «Вкладка «Протоколирование» 139

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

8.1.7 Система. Вкладка «Вкладка «Часы сервера» ... 140
8.2 Администрирование. Данные ... 141
8.2.1 Данные. Вкладка «SQL Сервер» ... 141
8.2.2 Данные. Вкладка «Резервирование БД» ... 142
8.2.2 Данные. Вкладка «Резервирование ПО» ... 144
8.2.2.1 Резервирование средствами КРОС ... 144
8.2.2.2 Резервирование ПО средствами ОС ... 146
8.2.3 Данные. Вкладка «Очистка БД» ... 147
8.3 Администрирование. Безопасность ... 148
8.3.1 Безопасность. Вкладка «Роли» ... 148
8.3.1.1 Права доступа ... 149
8.3.1.2 Создание, редактирование и удаление роли ... 151
8.3.2 Безопасность. Вкладка «Администратор сервера» ... 152
8.3.3 Безопасность. Вкладка «Доступ API» ... 153
8.3.4 Безопасность. Вкладка «Сертификаты» ... 153
8.3.5 Безопасность. Усиленная парольная защита ... 152
8.3.5.1 Назначение ... 152
8.3.5.2 Включение и отключение режима ... 153
8.3.5.3 Настраиваемые параметры ... 153
8.3.5.4 Требования к паролю и валидация ... 154
8.3.5.5 Индикация надёжности пароля и условия активации режима ... 155
8.3.5.6 Управление сроком действия пароля ... 156
8.3.5.7 Защита от подбора пароля ... 158
8.3.5.8 Истечение срока действия пароля ... 160
8.3.5.9 Создание охранной организации при включённом режиме ... 162
8.4 Администрирование. Заявки ... 163
8.4.1 Подача заявки на регистрацию ... 164
8.4.2 Обработка заявки на регистрацию ... 164
8.5 Администрирование. Протокол ... 166
8.6 Администрирование. Сообщения ... 167
8.7 Администрирование. Справочники ... 168
8.7.1 Справочники. Вкладка «Типы объектов» ... 169
8.7.2 Справочники. Вкладка «Доклад ГЗ» ... 170
8.7.2 Справочники. Вкладка «Причины тревоги» ... 170
9. Отчеты. Конструктор отчетов ... 171
9.1 Общий вид конструктора отчетов ... 172
9.2 Создание отчета по базовому шаблону ... 172
9.3 Создание шаблона отчета в конструкторе отчетов ... 174
9.4 Запись шаблона отчета ... 175
9.5 Оперативная карточка объекта ... 176
9.6 Сохранение и печать отчета ... 177
10. Регистрация прибора на сервере КРОС ... 178
10.1 Оформление договора на обслуживание ... 178
10.2 Регистрация объекта ... 178
10.3 Настройка прибора ... 178
10.4 Активация прибора ... 179
11. Зеркалирование («Горячий» резерв) ... 180
11.1 Общая информация ... 180

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

11.2 Настройка системы 181
11.3 Создание трансляции 181
11.4 Разрешение приема данных 182
12. Импорт базы данных из Юпитер-7 183
12.1 Перенос базы данных Юпитер-7 в Юпитер-КРОС 183
12.1.1 Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС 183
12.1.2 Создание файла конфигурации Юпитер-7 184
12.1.2 Импорт файла конфигурации в Юпитер-КРОС 185
12.1.2.1 Соответствие карточек Юпитер-7 при переносе в Юпитер-КРОС 186
12.2 Трансляция из Юпитер-7 в КРОС 186
12.2.1 Настройка трансляции 187
12.3. Настройка параметров на сервере Юпитер-КРОС 187
12.4. Замена серверов 187
13. Использование мобильного приложения «Личный кабинет» при трансляции из Юпитер-7 в Юпитер-КРОС 188
14. Настройка часов УМКА для работы на сервере КРОС 189
14.1 Первоначальная настройка часов 189
14.2 Настройка отслеживания часов 190
Приложение №1. Приборы, подлежащие переносу 193
Приложение №2 Поэтапный перевод оборудования с Юпитер-7 на Юпитер-КРОС 194
1. Концепция 194
2. Подготовка карточек объектов в Юпитер-7 к переносу в Юпитер-КРОС 195
3. Автоматизированный механизм переноса объектов 195

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

Введение

Назначение руководства

Настоящее руководство содержит сведения об особенностях 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(WEB-АРМ) — автоматизированное рабочее место и его web-версия.

АРМ ДПУ — автоматизированное рабочее место дежурного пульта управления.

АРМ ДО — автоматизированное рабочее место дежурного офицера.

АРМ СК — ситуационная карта

БД — база данных.

ГЗ — группа задержания.

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.

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.

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

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

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

КТС — кнопка тревожной сигнализации.

ЛК — личный кабинет.

Оборудование — комплекс всех технических средств СПИ «Юпитер».

ОО — Охранная организация.

ОПС — охранно-пожарная сигнализация.

Прибор — см. устройство.

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

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.

ТК — тревожная кнопка.

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

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

ШС — шлейф охранно-пожарной сигнализации.

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 - WEB-АРМ (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

- Сатурн-ЛК
- Юпитер-ТК v2.0
- Юпитер-ГЗ

8. Открытый протокол ЕППС (Единый Протокол Передачи Сообщений). Работа с системами сторонних производителей по протоколам:

- TCP SurGard
- TCP SurGard V4

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

10. API для сторонних разработчиков расширений и драйверов.

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

1.3 Рекомендованные системные требования

Таблица 1. 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 10 Мбит\сек	Не ниже 30 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 порт 9900 или иной 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, 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 или другие ОС на основе Debian.

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

Windows: x64 - 7 и выше. Корпорация Майкрософт прекращает поддержку Windows 7 - 14.01.2020 Рекомендуем использовать новые версии с последними обновлениями безопасности. Для корректной работы комплекса рекомендуется настроить брандмауэр.

Рекомендуемые браузеры:

- Google Chrome от 90 версии и новее
- Opera от 76 версии и новее
- Firefox от 90 версии и новее

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

2. Авторизация и роли пользователей.

2.1 Авторизация

После установки СПИ КРОС, для дальнейшей настройки предусмотрен web-интерфейс.

В браузере необходимо набрать адресную строку:

http://192.168.0.10:9900, где192.168.0.10 — ip-адрес сервера КРОС в локальной сети

или

localhost:9900, если сервер КРОС установлен на данном компьютере.

На странице откроется окно для ввода данных пользователя (рис. 1)

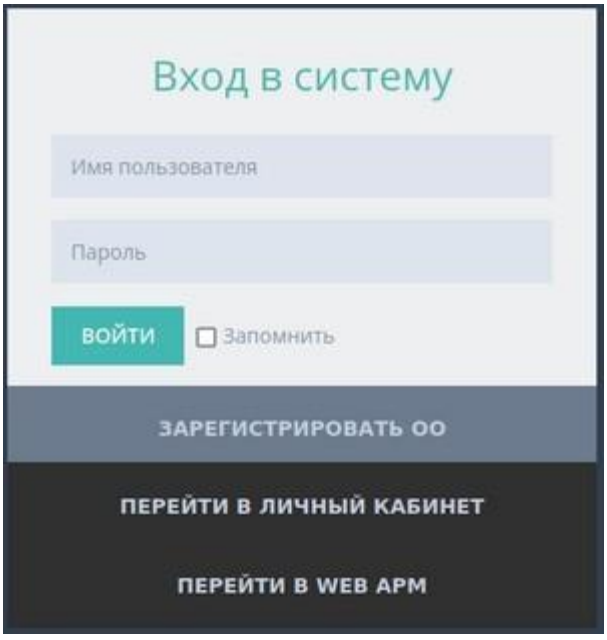


Рис. 1 Форма ввода логина и пароля

В зависимости от вводимых параметров можно попасть в управление самим сервером(superadmin) или в управление параметрами охранной организации(admin). Пароль у пользователя можно изменить после регистрации. Так же, доступ к серверу может получить пользователь с правами, определёнными его ролью.

После ввода авторизационных данных, нажать «Войти».

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

2.2 Роли и пользователи

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

2.2.1 Права пользователя superadmin

Superadmin осуществляет общее администрирование сервера и имеет доступ к следующему функционалу:

- 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 администраторов охранных организаций;
- Обновление версии сервера;
- Настройка базы данных;
- Распределение прав доступа(ролей);
- Настройка трансляций по протоколу ЕППС;
- Резервное копирование сервера
- Управление режимом «Усиленная парольная защита»

2.2.2 Пользователь Администратор предприятия

Функции доступные администратору охранной организации:

- Добавление трансляций передачи сообщений;

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

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

2.2.3 Менеджер

Функции:

- Добавление договоров охраны;
- Добавление объектов охраны.

2.2.4 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

2.3 Смена пользователя

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

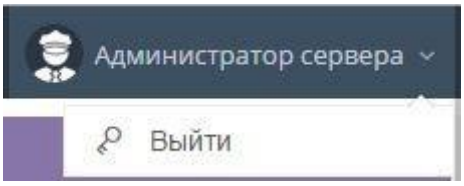


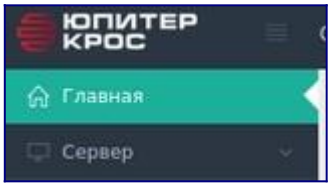
Рис. 2 Окно выхода из учетной записи

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

Более подробно роли описаны в разделе «Администрирование» подраздел «Безопасность» вкладка «Роли»

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

4. Меню «Главная»



Меню "Главная" - страница, содержащая основную справочную информацию по комплексу КРОС.
Здесь отображается информация по объектам и приборам, закреплённым за охранной организацией.
Общая информация по количеству объектов и приборов, зарегистрированным на сервере КРОС, в случае с несколькими охранными организациями, доступна только пользователю – superadmin.

Заголовок окна выглядит следующим образом:



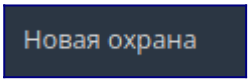
, где



- при нажатии на логотип, происходит переход на пункт меню "Главная" из любого раздела КРОС.



- позволяет убрать надписи бокового меню, увеличивая полезную информационную площадь.



- наименование текущей охранной организации.



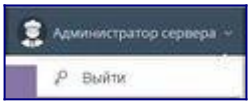
- индикатор наличия системных уведомлений. При его активации открывается список сообщений



, где можно **Закрыть** окно нажав "X", или отказаться от дальнейшего информирования о данном событии, нажав **НЕ ПОКАЗЫВАТЬ БОЛЬШЕ**, или, нажав **ПОНЯТНО**, оставить сообщение активным.



- индикатор наличия сообщений в ходе работы ОП.



- указывает на активный аккаунт, а также, при нажатии, позволяет выйти из текущей учетной записи.

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

4.1 Состояние объектов

Данное меню служит для мониторинга текущего состояния объектов охраны, и дает общую сводку по охраняемым объектам (рис. 3).

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. Высота столбца отображает количество событий в конкретный период времени. Информация по взятиям, снятиям, тревогам и неисправностям отображается в виде графиков соответствующих цветов.(цифра 3 на изображении внизу).

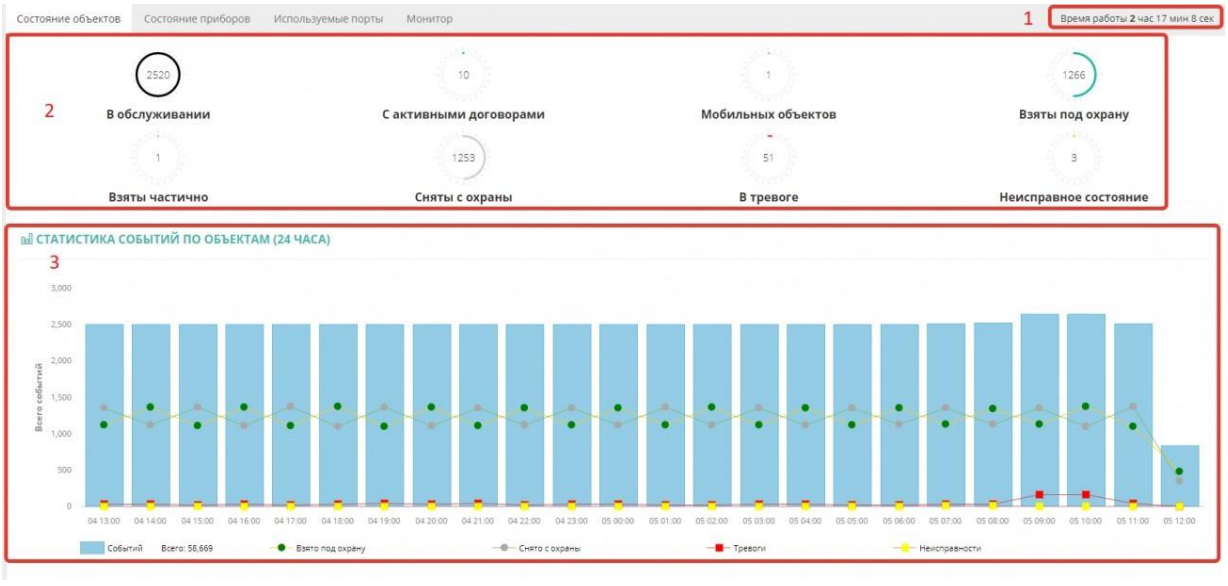


Рис. 3 Состояние объектов

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 (рис. 4).

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. Статистика отображает общее количество событий за час, количество взятых и снятых приборов, а также приборов, находящихся в тревожном и неисправном состоянии.(цифра 3 на изображении внизу).

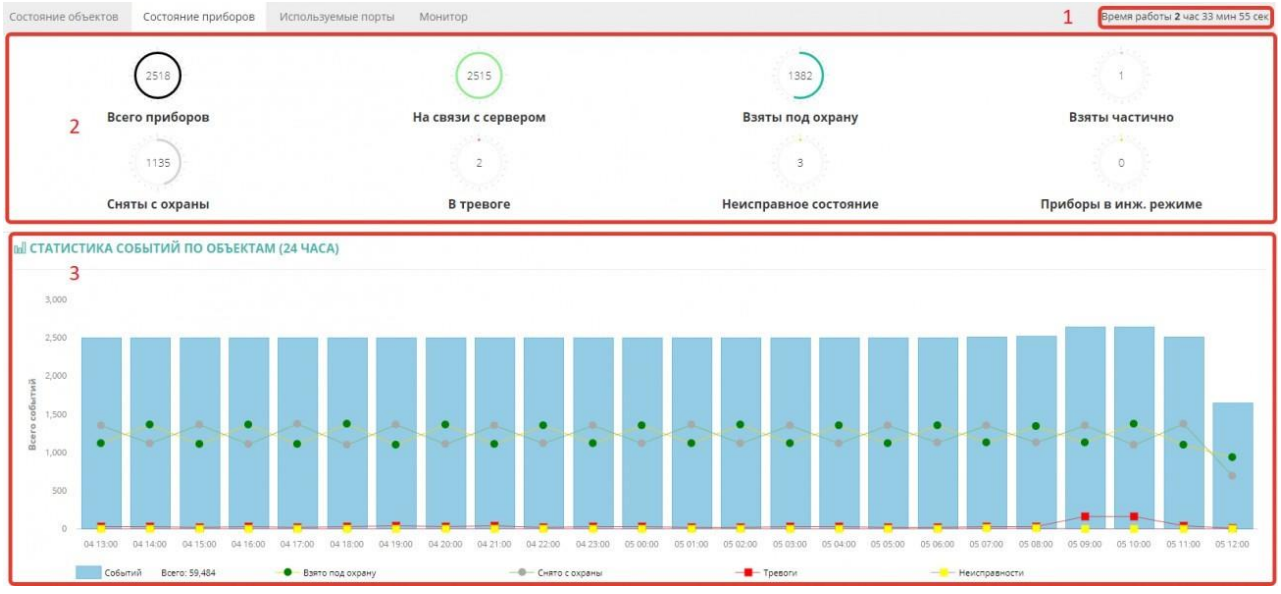


Рис. 4 Состояние приборов

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 (рис. 5).

Данная вкладка исключительно информативная, для изменения портов следует воспользоваться меню Охрана → Реквизиты → Редактирование охранной организации

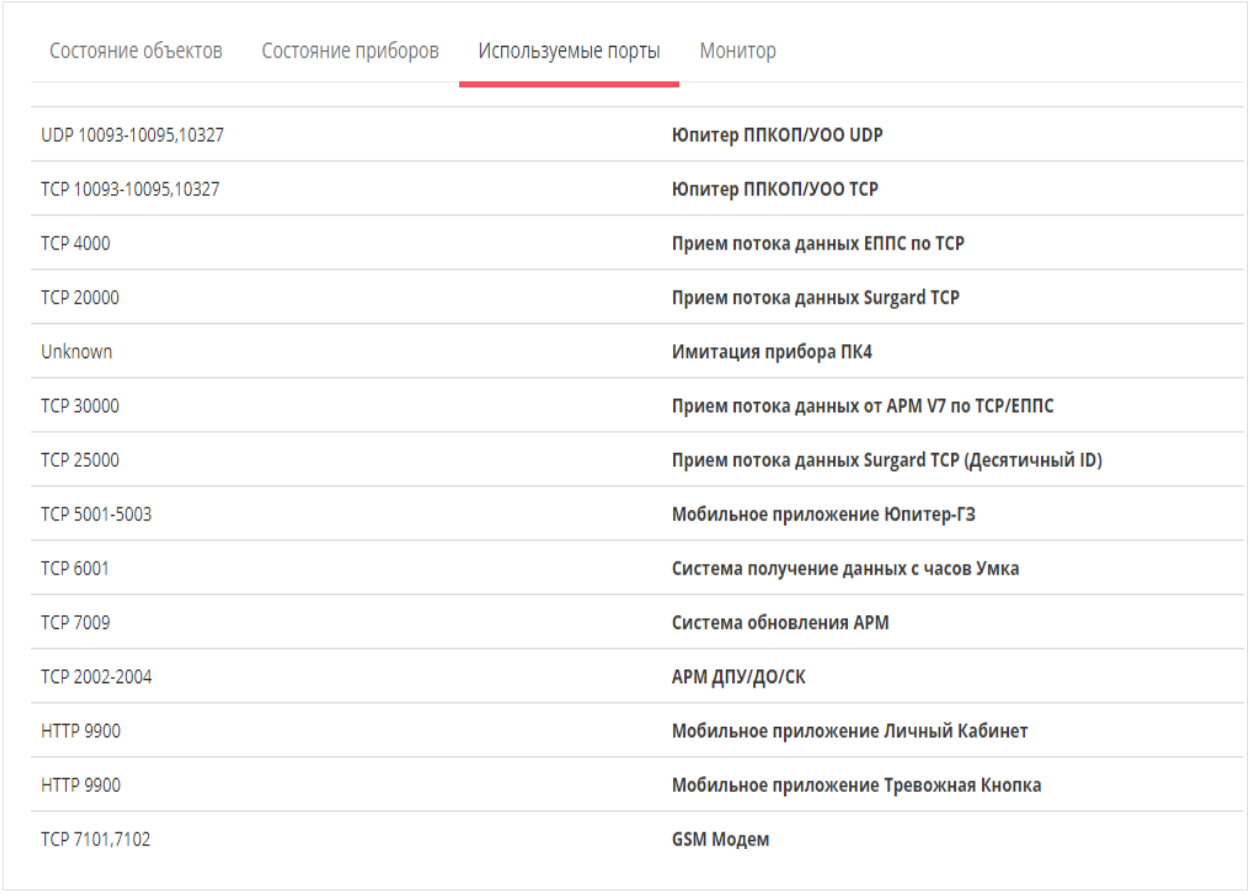


Рис. 5 Используемые порты

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

4.4 Монитор

Данная вкладка предназначена для мониторинга входящих и исходящих соединений сервера КРОС (рис. 6).

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.

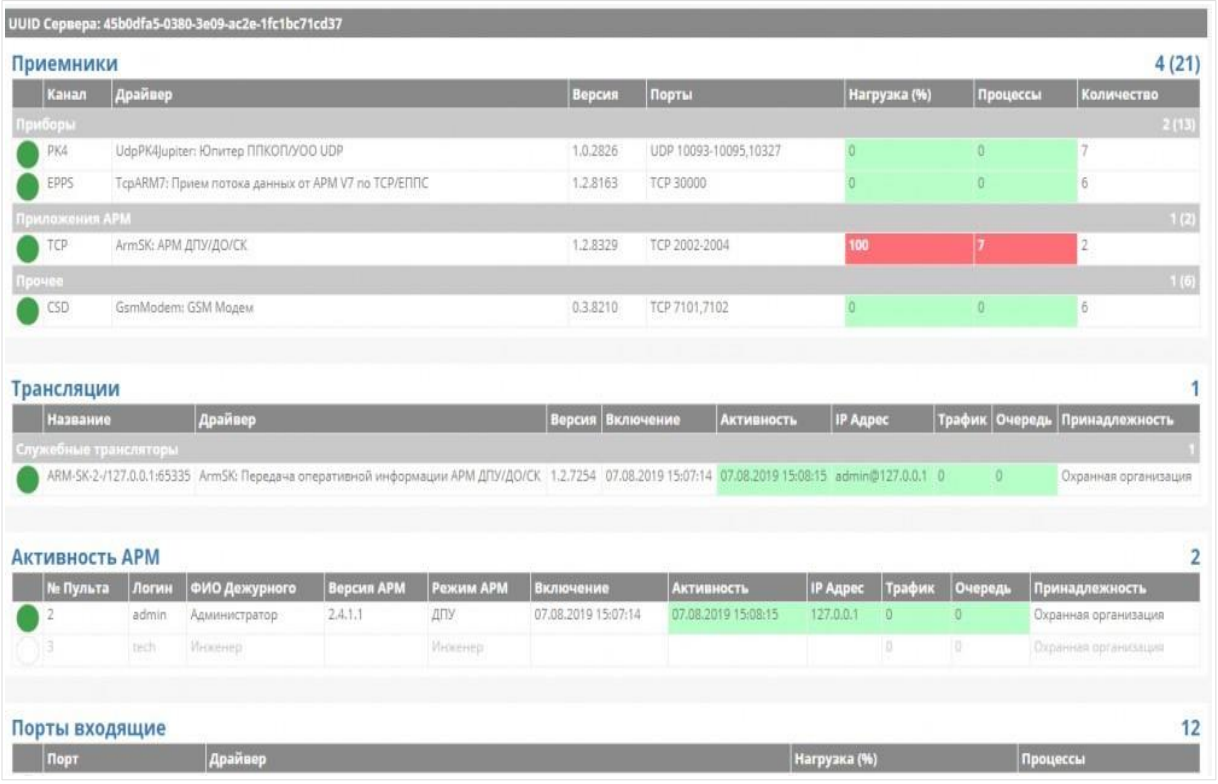


Рис. 6 Монитор

Под учетной записью Администратора Сервера (superadmin) у вкладки появляется дополнительная информация о состоянии сервера (рис. 7).



Рис. 7 Дополнительная информация вкладки «Монитор», доступная пользователю superadmin

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

5. Меню «Сервер»

Доступ к тонким настройкам тех или иных разделов определяется той ролью, которая назначена пользователю. Максимальный доступ к настройкам сервера имеет superadmin. Поэтому не стоит удивляться, если пользователь вошел в систему и не увидел раздел или в разделе присутствуют не все подразделы.

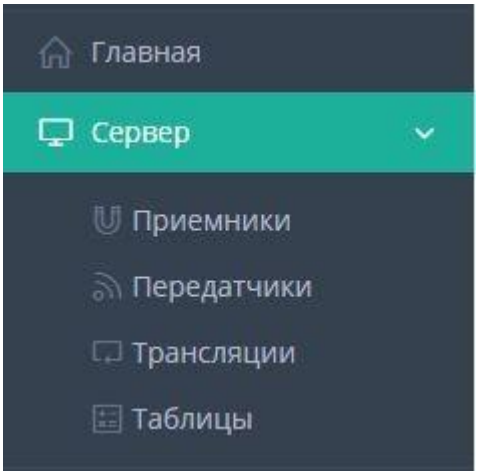


Рис. 8 Меню «Сервер»

Разделы «Приемники» и «Передатчики» могут быть не доступны администратору предприятия, если только эти разрешения не указаны в его роли.

5.1 Приемники

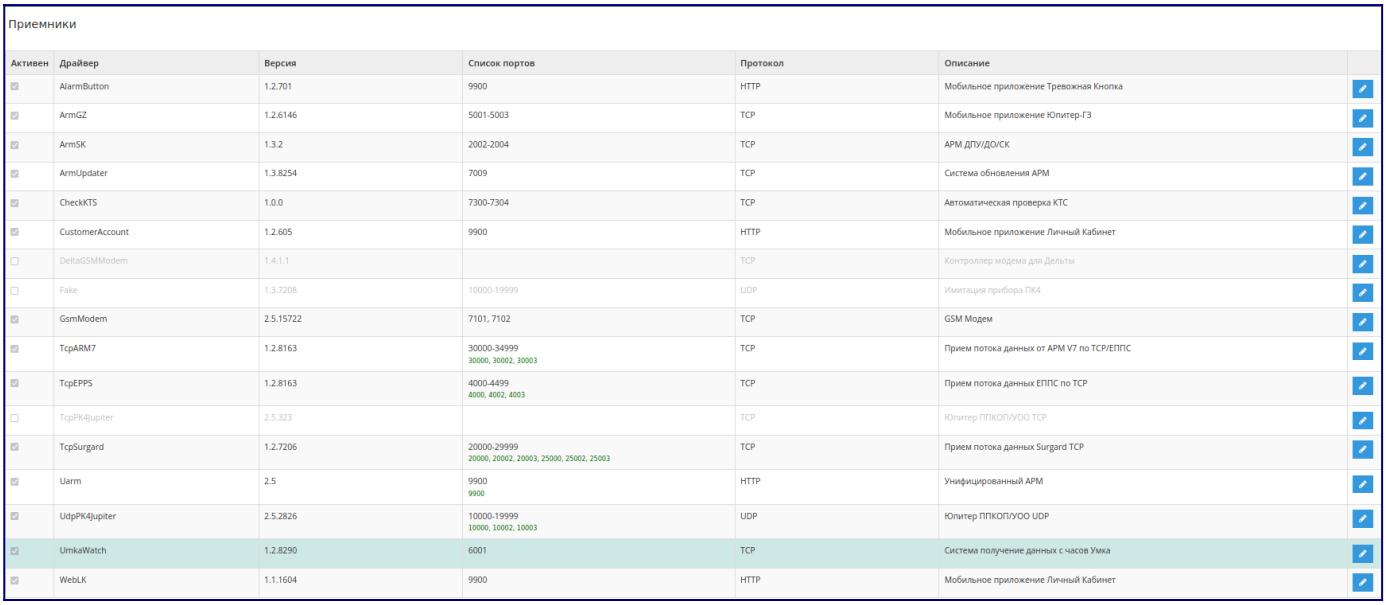
Окно **«Приемники»** доступно только **Администратору сервера**, если только не установлено разрешение в какой-либо из ролей, например **Администратор**.

Если порты в приемнике, по каким либо причинам ограничены, то в случае открытия (добавления) нового порта в настройках охранной организации (Охрана-Реквизиты-Параметры-Диапазон разрешенных портов), следует проверить, попадает ли этот порт в разрешенный диапазон в настройках приемника.

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.

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

5.1.1 Настройка приемников


Приемники

Активен	Драйвер	Версия	Список портов	Протокол	Описание
☑	AlarmButton	1.2.701	9900	HTTP	Мобильное приложение Тревожная Кнопка
☑	ArmGZ	1.2.6146	5001-5003	TCP	Мобильное приложение Юпитер-ГЗ
☑	ArmSK	1.3.2	2002-2004	TCP	АРМ ДПУ/ДО/СК
☑	ArmUpdater	1.3.8254	7009	TCP	Система обновления АРМ
☑	CheckKTS	1.0.0	7300-7304	TCP	Автоматическая проверка КТС
☑	CustomerAccount	1.2.605	9900	HTTP	Мобильное приложение Личный Кабинет
☐	DeltaGSMModem	1.4.1.1		TCP	Контроллер модема для Дельты
☐	Fake	1.3.7208	10000-19999	UDP	Имитация прибора ПК4
☑	GsmModem	2.5.15722	7101, 7102	TCP	GSM Модем
☑	TcpARM7	1.2.8163	30000-34999 30000, 30002, 30003	TCP	Прием потока данных от АРМ V7 по TCP/ЕППС
☑	TcpEPPS	1.2.8163	4000-4499 4000, 4002, 4003	TCP	Прием потока данных ЕППС по TCP
☐	TcpPK4Jupiter	2.5.323		TCP	Юпитер ППКОП/УОО TCP
☑	TcpSurgard	1.2.7206	20000-29999 20000, 20002, 20003, 25000, 25002, 25003	TCP	Прием потока данных Surgard TCP
☑	Uarm	2.5	9900 9900	HTTP	Унифицированный АРМ
☑	UdpPK4Jupiter	2.5.2826	10000-19999 10000, 10002, 10003	UDP	Юпитер ППКОП/УОО UDP
☑	UmkaWatch	1.2.8290	6001	TCP	Система получение данных с часов Умка
☑	WebLK	1.1.1604	9900	HTTP	Мобильное приложение Личный Кабинет

Рис. 9 Внешний вид таблицы параметров приёмников

Таблица 2 Характеристики драйверов приёмников КРОС

Наименование драйвера	Функции	Протокол	Порты по умолчанию	Требуется открыть, если используется
AlarmButton	Драйвер приложения Тревожная Кнопка	HTTP / HTTPS	9900 / 9800	9900 вход
ArmGZ	Драйвер поддержки АГЗ	TCP	5001-5003	вход
ArmSK	Драйвер поддержки АРМ СК/ДПУ/ДО	TCP/ SSL	2002-2004 / 3002-3004	2002 вход, Lan проброс, если сервер и АРМ в одной сети
ArmUpdater	Драйвер обновления АРМ	TCP	7009	7009 вход/выход, Lan если сервер и АРМ в одной сети-после доработки обновления с локального сервера
CheckKTS	Автоматическая проверка КТС	TCP	7300-7304	вход(Позволяет использовать функционал Автоматическая проверка тревожной кнопки с помощью модема Юпитер-7520)
CustomerAccount	Драйвер приложения Личный Кабинет	HTTP / HTTPS	9900 / 9800	9900 вход
GsmModem	Драйвер GSM Модема	TCP	7101, 7102	7101 вход, Lan проброс, если сервер и модем в одной сети

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

TcpARM7	Прием потока данных из Юпитер-7 и резервирование	TCP	30000-34999	вход – если идет поток данных из Юпитер-7 по протоколу ЕППС вход / выход – если резервирование данных
TcpEPPS	Прием потока данных по протоколу ЕППС	TCP	30000-34999	вход – если идет поток данных только на прием вход / выход – если резервирование ("Зеркалирование")
TcpPK4Jupiter	Приём данных ППКОП/УОО по протоколу TCP	TCP	10000-19999	вход
TcpSurgard	Прием потока данных в формате Surgard	TCP	20000-24999	вход выход при настройке трансляции на стороннее ПО
Uarm	Протокол - Унифицированный АРМ	TCP	9900	выход
UdpPK4Jupiter	Приём данных ППКОП/УОО по протоколу UDP	UDP	10000-19999	вход
Сервер лицензирования	Обновление сервера	TCP/ SSL	2120-2122/ 3120-3122	3120 выход
UmkaWatch	Получение данных с часов Умка	TCP	6001	вход
WebLK	Мобильное приложение Личный Кабинет	TCP/SSl	9900 / 9800	9900 вход
Карта в объекте	Доступ к геокодеру	TCP	80/443	вход/выход

Для редактирования настроек необходимо:

1. В строке приемника нажать кнопку (редактировать), для вызова окна редактирования.
2. Перейти на вкладку «Параметры»
3. Внести изменения.
4. Нажать «Сохранить».

После внесения изменений необходимо нажать на кнопку 

, либо выйти из карточки настройки драйвера без внесения изменеий, нажав кнопку 

.

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

5.1.1.1 Параметры приемников

Параметры приёмников можно посмотреть и изменить, нажав на кнопку "Редактировать"



Наименования и значения параметров в настройках драйверов могут отличаться, так как настройки зависят от назначения приёмника. В статье представлены все возможные параметры.

5.1.1.1.1 Информация

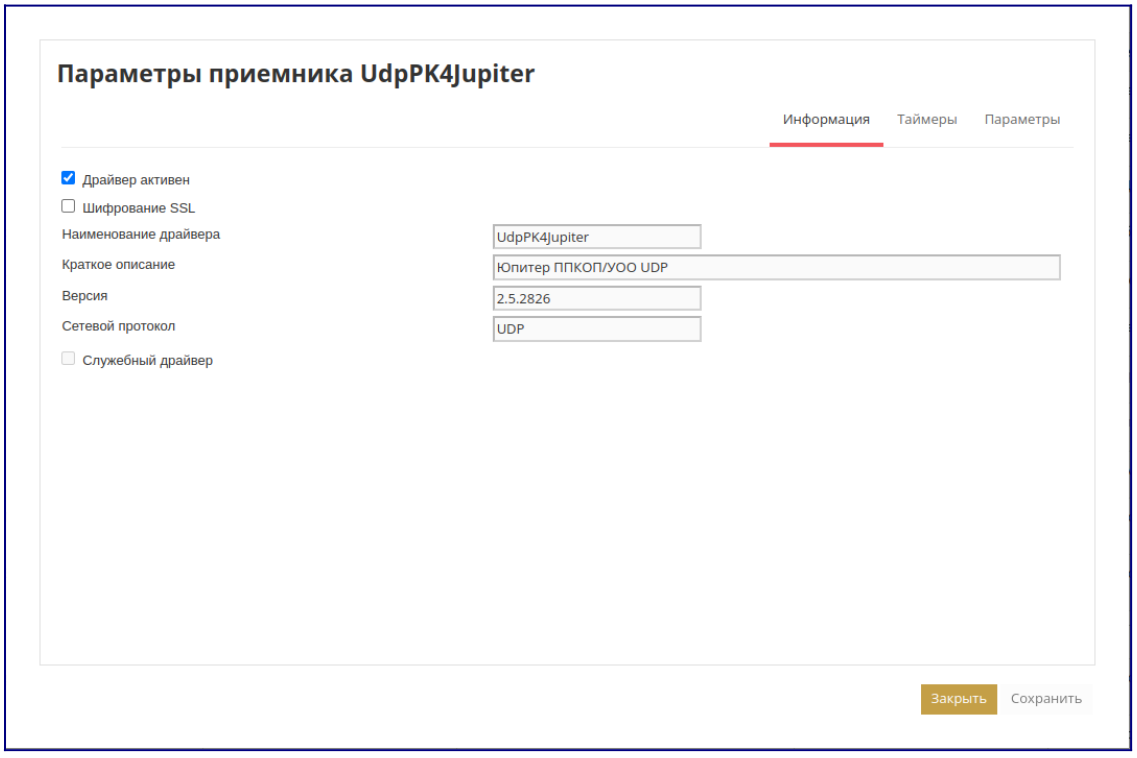


Рис. 10 Пример карточки настройки приёмника. Вкладка «Информация»

- **Драйвер активен** - разрешает или запрещает использование драйвера.
- **Шифрование SSL** - разрешает или запрещает использование шифрования на основе SSL сертификата.
- **Наименование драйвера** - наименование драйвера принятое в КРОС.
- **Краткое описание** - описание драйвера, краткая расшифровка его назначения.
- **Версия** - обновление драйверов происходит на уровне сервера лицензирования, поэтому данная информация в большей степени необходима при использовании комплекса в изолированных сетях.
- **Сетевой протокол** - отображает протокол, по которому принимается информация UDP, TCP или HTTP.
- **Служебный драйвер** - определяет драйвера, работающие в любом режиме сервера КРОС.

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

5.1.1.1.2 Таймеры

В данном разделе можно настоить время реагирования отдельного драйвера. Данный раздел может отсутствовать в настройке ряда драйверов.

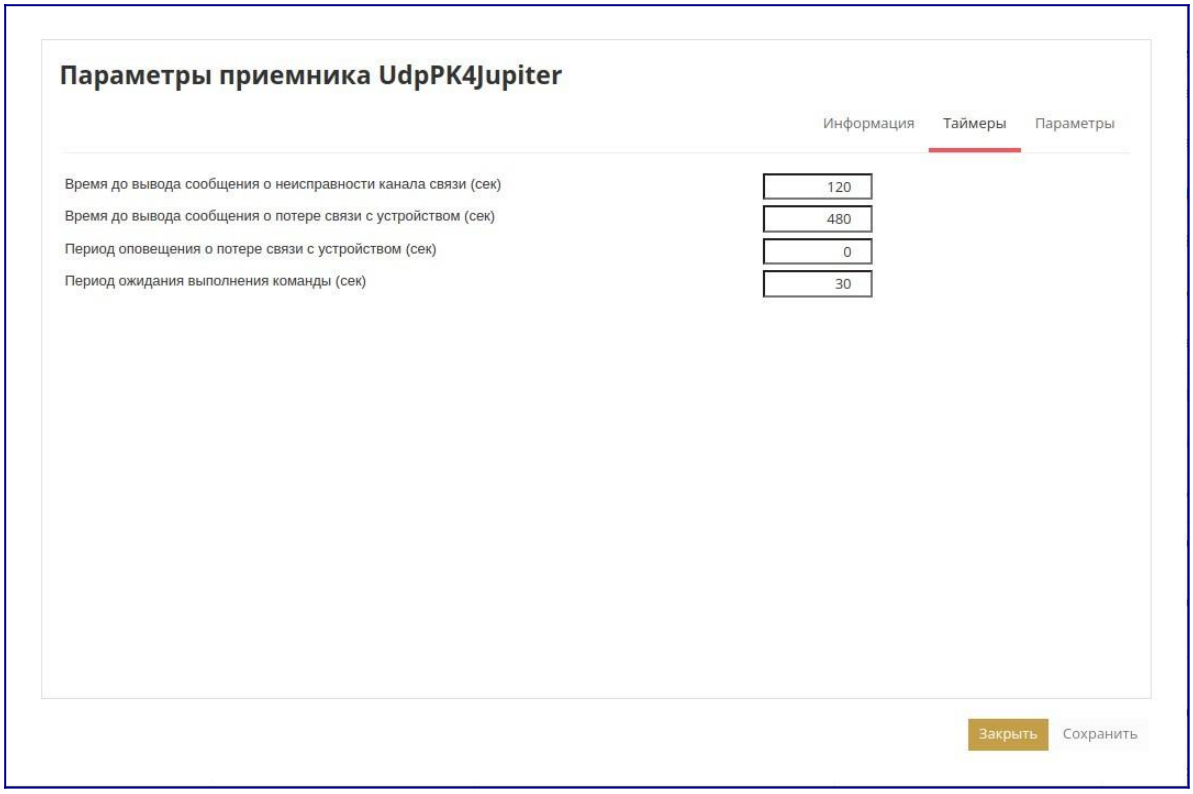


Рис. 11 Пример карточки настройки приёмника. Вкладка «Таймеры»

- **Время до вывода сообщения о неисправности канала связи (сек)** - если, в течении указанного времени, прибор или другая перефирия, не прислали информацию, КРОС генерирует сообщение о неисправности канала связи.
- **Время до вывода сообщения о потере связи с устройством (сек)** - если в течении указанного времени информация по каналу связи так и не была получена, КРОС генерирует событие - "Потеря связи".
- **Период оповещения о потере связи с устройством (сек)** - с какой периодичностью генерировать сообщение.
- **Период ожидания выполнения команды (сек)** - сколько времени КРОС ждет подтверждение о том, что прибор принял команду.

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

5.1.1.1.3 Параметры

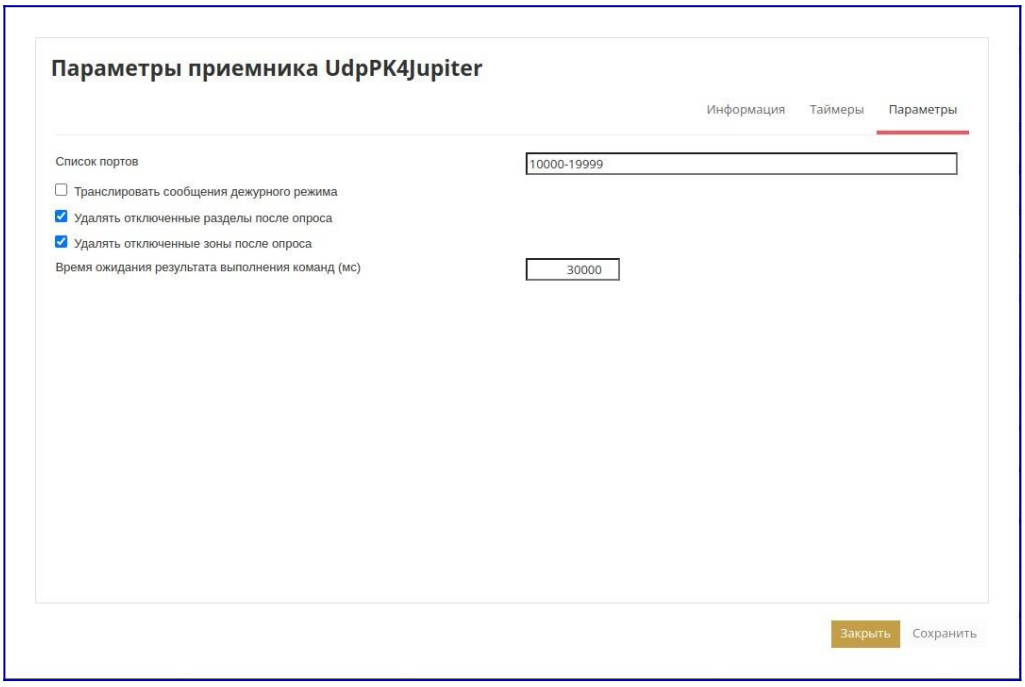
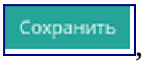


Рис. 11 Пример карточки настройки приёмника. Вкладка «Параметры»

В настройке некоторых передатчиков данный раздел отсутствует. Здесь приводится полный перечень параметров, встречающихся в разделе **параметры** при настройке приёмников.

- **Список портов** - порты назначенные драйверу для приёма информации
- **Транслировать сообщения дежурного режима** - разрешить/запретить передачу системных сообщений
- **Удалять отключенные разделы после опроса** - позволяет устанавливать текущую конфигурацию разделов прибора.
- **Удалять отключенные зоны после опроса** - корректирует состояние зон в карточке прибора.
- **Время ожидания результата выполнения команд (мс)** - время ожидания подтверждения выполнения команд.
- **TCP таймаут (мс)** - время ожидания отклика по текущему каналу связи.
- **Период контроля повторного входа (сек)** - Определяет периодичность попыток авторизации.
- **Путь к дистрибутиву** - относительный путь, где находятся модули обновления ПО "АРМ Юпитер".
- **Таблица перекодировки по умолчанию** - Таблица сообщений назначаемая при создании трансляции по-умолчанию.

После внесения изменений в настройки драйвера необходимо нажать кнопку 

, чтобы зафиксировать новые значения.

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

5.2 Передатчики

В окне **«Передатчики»** (меню **«Сервер»→«Передатчики»**) представлен список драйверов, предназначенных для передачи потока информации в реальном времени на программы и устройства, работающими с ними.

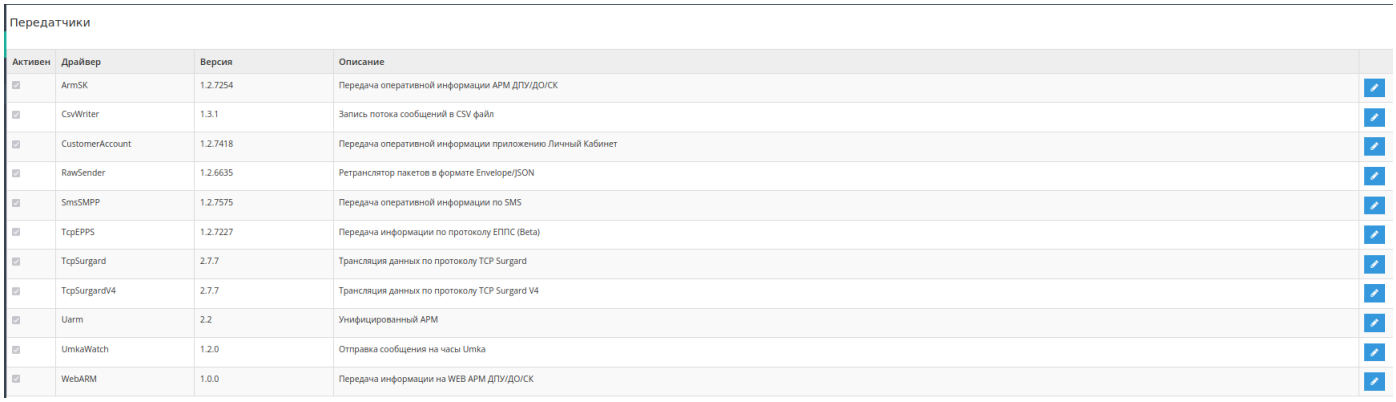


Рис. 12 Список драйверов передатчиков КРОС

5.2.1 Настройка передатчиков

Имеется возможность их редактирования , хотя их параметры уже настроены и не требуют изменения.

После внесения изменений необходимо нажать на кнопку 

, либо выйти из карточки настройки драйвера без внесения изменений, нажав кнопку 

.

5.2.1.1 Параметры передатчиков

5.2.1.1.1 Информация

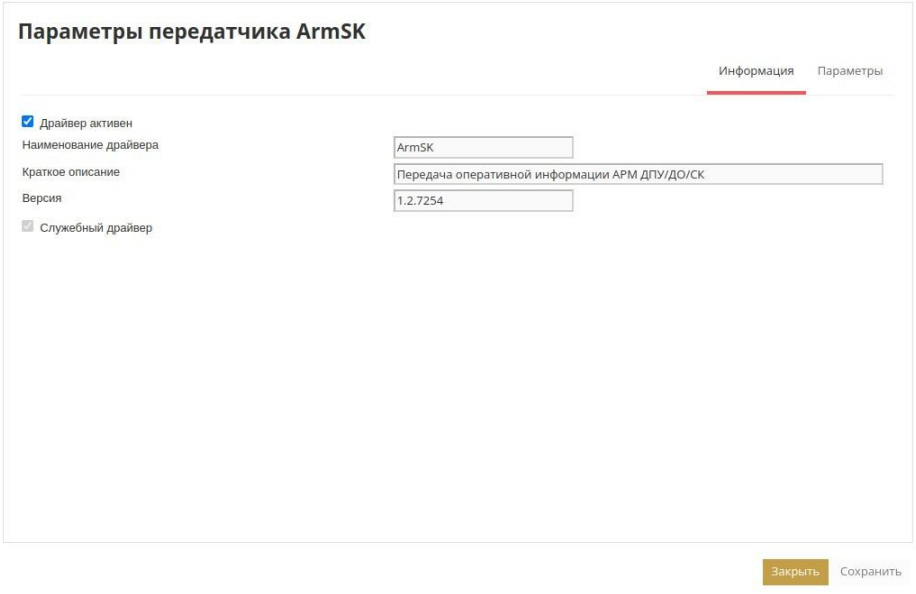


Рис. 13 Пример карточки настройки передатчика. Вкладка «Информация»

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

В той или иной форме **Информация** присутствует у всех передатчиков, поэтому здесь описаны все возможные поля.

- **Драйвер активен** - позволяет включить/отключить использование драйвера
- **Наименование драйвера** - наименование драйвера принятое в КРОС
- **Краткое описание** - наименование драйвера или описание его назначения
- **Версия** - информация необходимая для использования комплекса в изолированных средах.
- **Служебный драйвер** - указывает на то, что данный драйвер определен на системном уровне.

5.2.1.1.2 Параметры

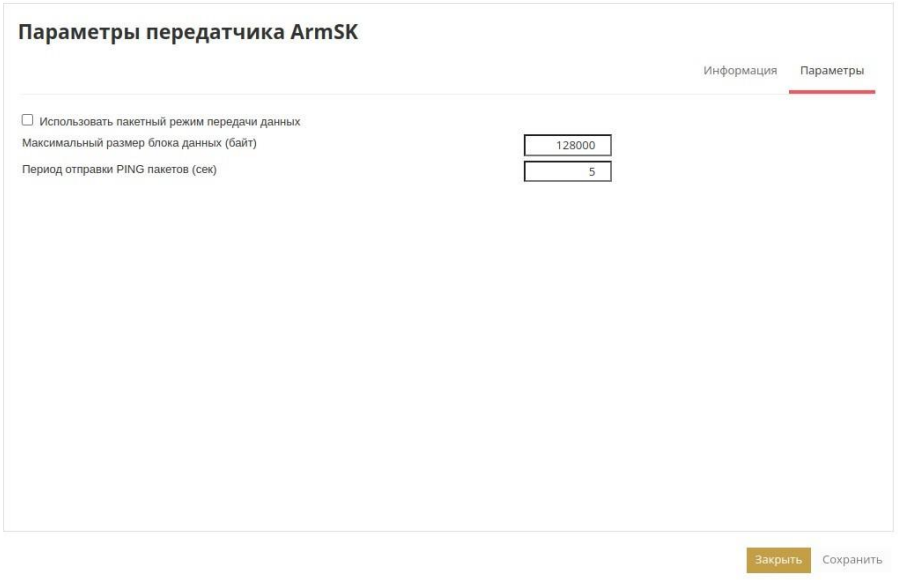


Рис. 14 Пример карточки настройки передатчика. Вкладка «Параметры»

Данная закладка может отсутствовать у ряда передатчиков. Так же количество параметров и их наименование зависит от специфики драйвера. Здесь приводится полный список используемых параметров.

- **Использовать пакетный режим передачи данных** - разрешить определять размер, передаваемых пакетов, в ручную.
- **Максимальный размер блока данных (байт)** - задать размер, передаваемого блока данных.
- **Период отправки PING пакетов (сек)** - задать максимально допустимый интервал времени в течении которого данные должны быть переданы.

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.

- Окно **«Трансляции»** по-умолчанию доступно **Администратору сервера**, **Администратору** и **Инженеру**.
- **Администратор сервера** не может добавлять новые трансляции передачи событий (кроме зеркалирования), но может редактировать и удалять существующие.

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

5.3.1 Таблица трансляций

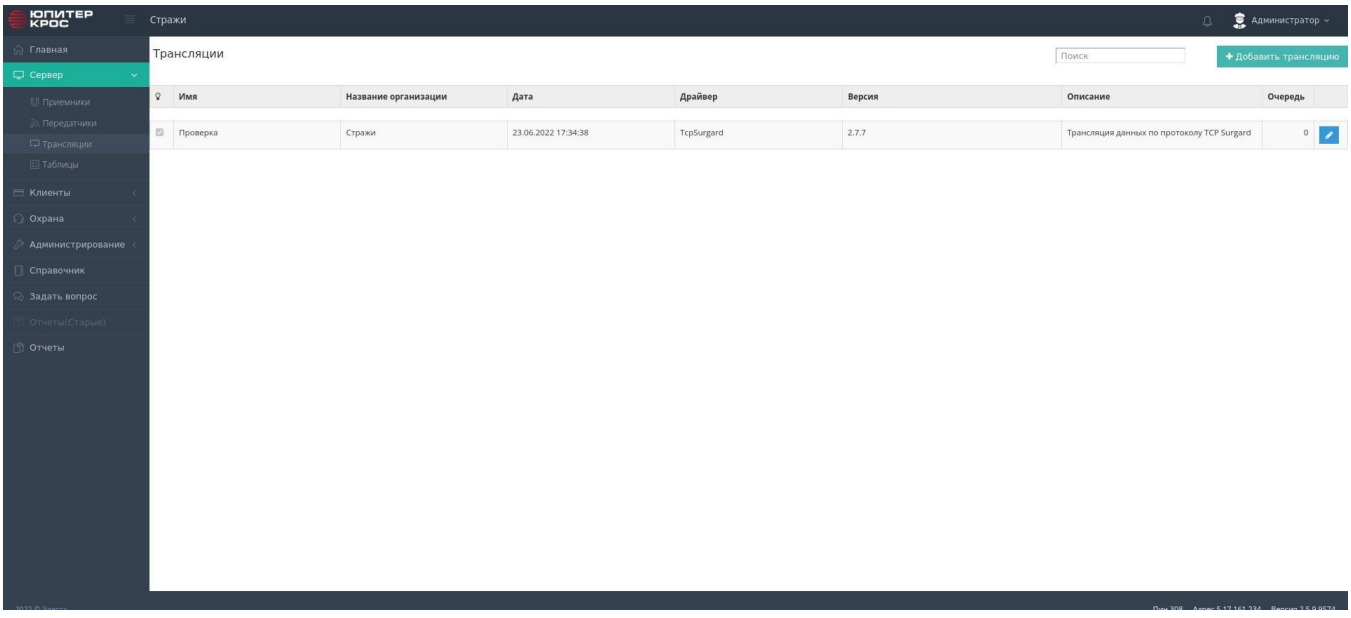


Рис. 15 Внешний вид таблицы трансляций

Для того чтобы открыть таблицу Трансляций, необходимо войти в пункт меню "Сервер" подраздел "Трансляции". Пользователь superadmin может создавать трансляции для любого ОП на сервере КРОС, используя протокол ЕППС(«Зеркалирование»), остальные протоколы ему не доступны. Пользователь с правами администратора ОО может создавать трансляции, используя любые доступные драйвера, кроме протокола ЕППС.

В таблице Трансляций приняты следующие обозначения:

 - отображает активность трансляции поле заполнено - трансляция включена, поле пустое - трансляция выключена.

Имя - наименование трансляции, которое было ей присвоено при создании. Поле можно изменить

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

в режиме редактирования.

Название организации - Наименование организации - источника сообщений. Выбирается при создании трансляции. Данное поле доступно только пользователю superadmin, так как трансляции, создаваемые под администратором ОО транслируют данные только той ОО, администратором которой он является.

Дата - Дата создания трансляции.

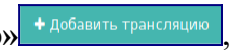
Драйвер - тип драйвера, используемого для трансляции.

Версия - Версия драйвера. Необходима для контроля актуальной версии.

Описание - Описание драйвера.

Очередь - Отображает текущее состояние передачи данных. Если значение "0", значит очереди нет и данные исправно передаются. В зависимости от состояния локальной сети или работы канала интернет, а так же от состояния принимающего сервера заполнение очереди может колебаться. Если в очереди менее 100-150 сообщений, то считается, что трансляция работает в нормальном режиме.

5.3.2 Создание трансляций

Для добавления новой трансляции передачи событий, необходимо нажать на кнопку «**Добавить трансляцию**» 

, расположенную в правом верхнем углу таблицы трансляций. Если трансляцию создает администратор предприятия, то в этом случае откроется форма создания трансляции.

5.3.1 Добавление трансляции

Форма для создания новой трансяции(рис. 16)

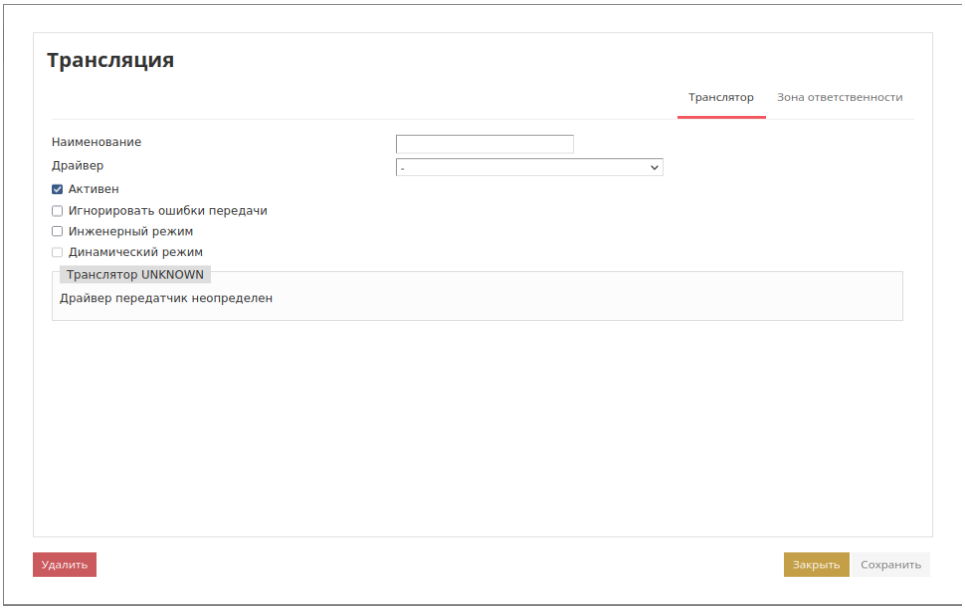


Рис. 16 Карточка создания трансляции администратором предприятия

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

Параметры, общие для всех типов трансляций:
Наименование — поле для ввода имени трансляции, что позволяет её персонализировать.
Активен - включает/выключает текущую трансляцию.
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.

5.3.1.1 Драйвер трансляции

Заполнить поле **«Наименование»** и, в выпадающем списке, выберите **«Драйвер»**. (рис. 17).

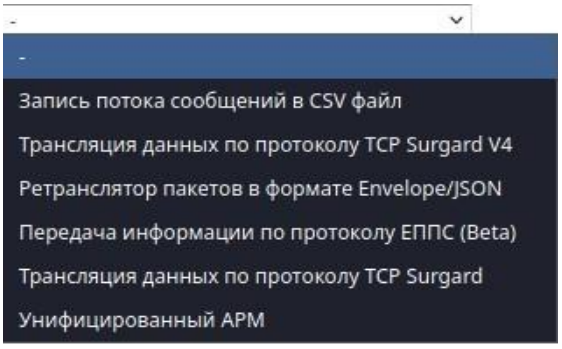


Рис. 17 Список драйверов

Требуется особо отметить - пользователь *superadmin* может создавать трансляции, использующие только протокол ЕППС.

После выбора протокола трансляции появляются расширенные настройки протокола.

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

5.3.1.1.1 Запись потока сообщений в CSV файл

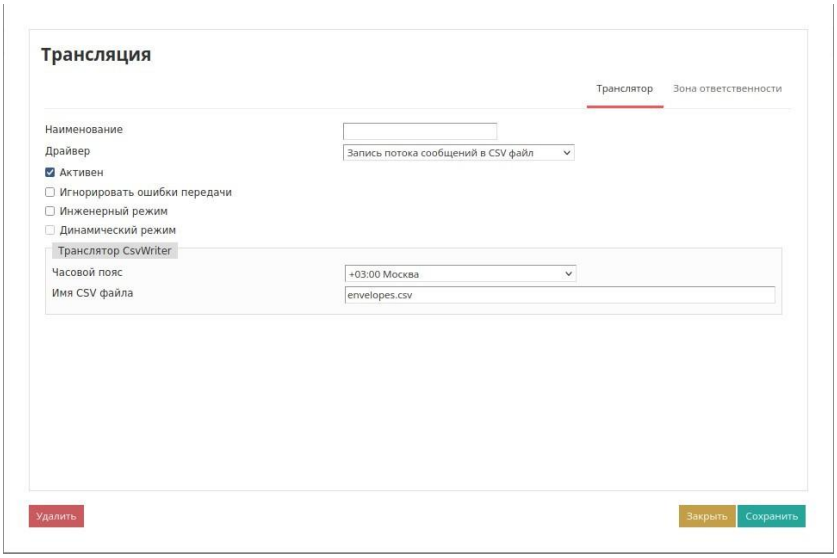


Рис. 18 Карточка настройки трансляции потока сообщений в CSV файл

Данный протокол записывает все события по объектам в текстовый файл формата CSV.

- **Часовой пояс** - часовой пояс в котором работает ОП.
- **Имя CSV файла** - указывается путь и название файла в формате той ОС, в которой установлен КРОС.

5.3.1.1.2 Трансляция данных по протоколу SurGard(SurGard V4)

Это протоколы специально разработаны для обмена информацией между производителями ПО, так как на аппаратном уровне каждый производитель ПО и приборов использует свои протоколы и шифрование.

SurGard - этот стандарт устанавливает протокол связи, который был разработан и полностью принадлежит ADEMCO Group, подразделение Pittway Corporation. Он публикуется в Security Industry Association (SIA), как промышленный стандарт безопасности де-факто. Ограничений на его использование нет.

SurGard V4 - это дальнейшее развитие протокола ***SurGard***. В настоящее время поддерживается не всеми производителями.

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

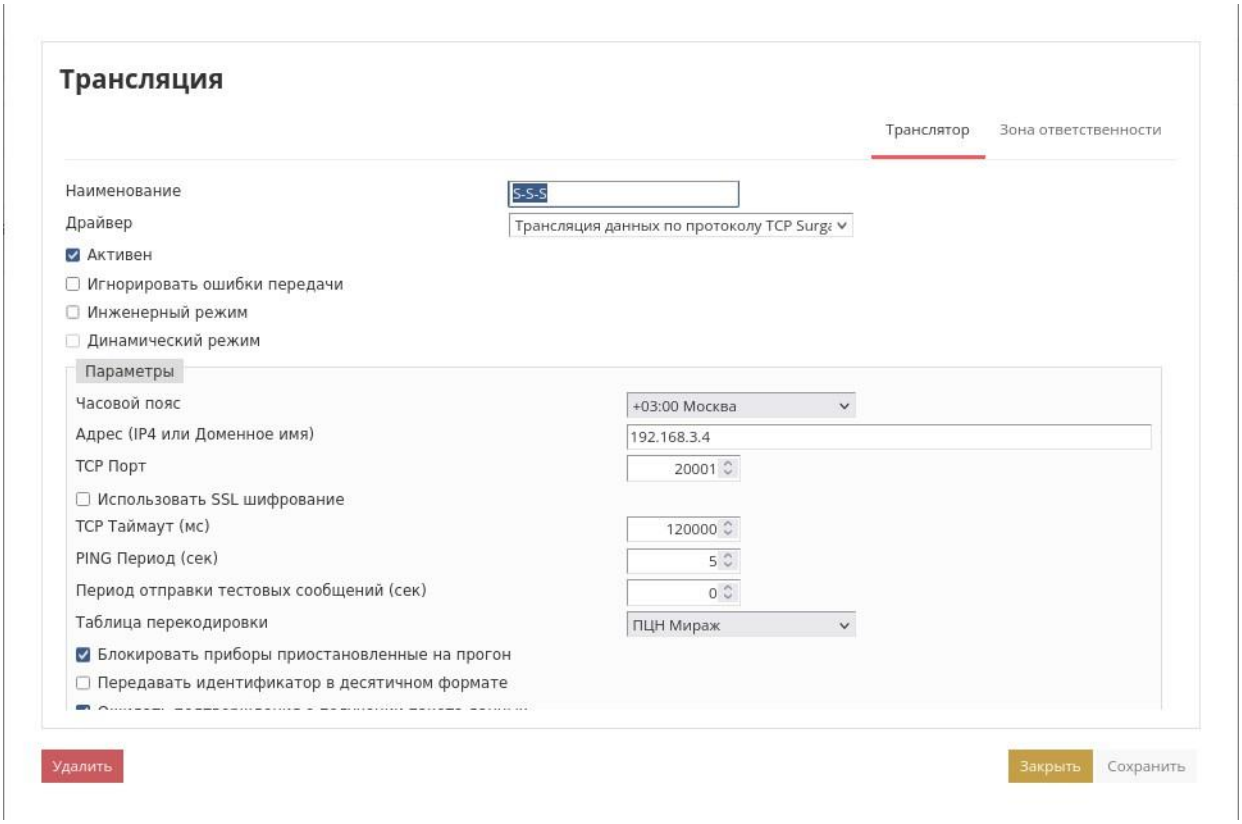


Рис. 19-1 Карточка создания трансляции по протоколу SurGard

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

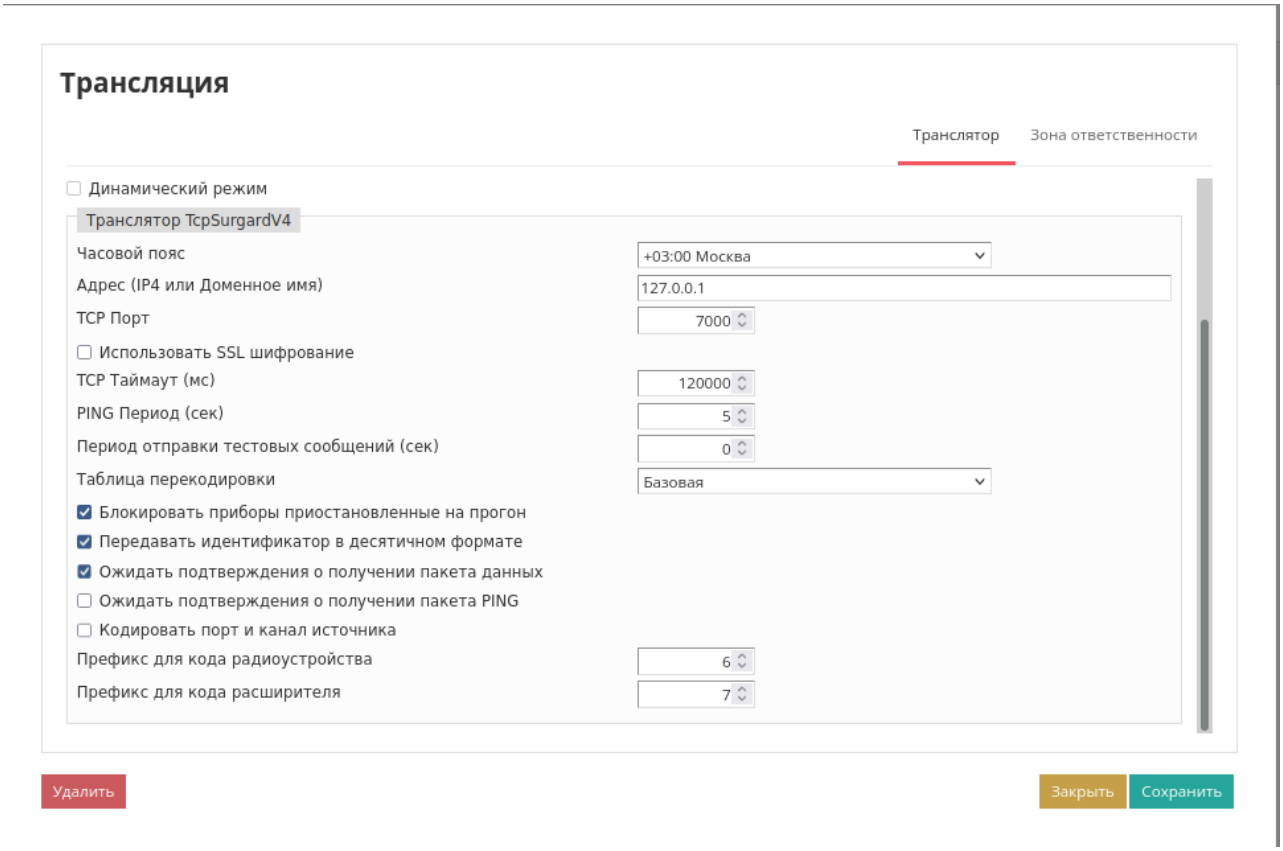


Рис. 19-2 Карточка создания трансляции по протоколу SurGard

Значение полей и параметров трансляции:

- **Часовой пояс** - часовой пояс в котором работает ОП.
- **Адрес (IP или Доменное имя)** - В этом поле необходимо указать IP-адрес(IPv4) в формате ***"aaa.bbb.ccc.ddd"*** или доменное имя компьютера или маршрутизатора, на который буден транслироваться поток данных.
- **TCP порт** - Порт по которому будет осуществляться соединение с сервером-приёмником. По-умолчанию используется порт:***7000***, но можно использовать порт указанный на принимающей стороне или порты заданные в настройках драйвера и ОО.
- **Использовать SSL шифрование** - если есть ***SSL сертификат***, то система позволяет транслировать данные по зашифрованному каналу.
- **TCP таймаут (мс)** - максимально допустимое время в миллисекундах, в течении которого должен передаваться пакет информации.
- **PING Период (сек)** - период проверки доступности сервера, принимающего сообщения.
- **Период отправки текстовых сообщений (сек)** - По-умолчанию ***"0"*** - постоянно. Можно указать периодичность отправки сообщений в секундах.
- **Таблица перекодировки** - назначение таблицы кодов сообщений, которая должна соответствовать таблице сообщений принимающей системы.
- **Блокировать приборы, приостановленные на прогон** - не передавать информацию от приборов, которые заблокированы или находятся на техническом обслуживании.

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

- **Передавать идентификатор в десятичном формате** - в комплексе КРОС идентификатор приборов передается в шестнадцатеричном формате, для совместимости с другими производителями можно изменить передачу идентификатора на десятеричный. При этом диапазон идентификаторов в первом случае ограничивается 0..65535, во втором 0..9999. Установка зависит от возможностей внешнего приемника.
- **Ожидать подтверждения о получении пакета данных** - в основном требуется при использовании нестабильных каналов связи, для проверки целостности, передаваемых 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** - желательно использовать на нестабильных каналах передачи данных, во избежание потерь при их передаче. Данный функционал проверяет наличие стабильного канала связи.
- **Кодировать порт и канал источника** - позволяет создавать зашифрованный канал передачи данных. Однако существует некоторая опасность того, что на принимающей стороне может не поддерживаться алгоритм шифрования в связи с различием версий драйверов Surgard. Параметр задает способ формирования заголовка SurGard сообщения. По умолчанию номер порта и номер канала станавливаются 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.
- **Префикс для кода радиоустройства** - параметр, позволяющий отличить проводные приборы от радиоканальных при обработке сообщений.
- **Префикс для кода расширителя** - параметр, позволяющий отличить расширитель от основного прибора при обработке сообщений.

5.3.1.1.3 Ретранслятор пакетов в формате Envelope/JSON

Протокол предназначен для передачи структурированных данных на программные комплексы способные их обработать.

- **Часовой пояс** - часовой пояс в котором работает ОП.
- **Адрес (IP или Доменное имя)** - В этом поле необходимо указать IP-адрес(IPv4) в формате ***"aaa.bbb.ccc.ddd"*** или доменное имя компьютера или маршрутизатора, на который буден транслироваться поток данных.
- **TCP порт** - Порт по которому будет осуществляться соединение с сервером-приёмником. По-умолчанию используется порт:***7000***, но можно использовать порт указанный на принимающей стороне.

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

- **TCP таймаут (мс)** - максимально допустимое время в миллисекундах, в течении которого должен передаваться пакет информации.
- **Использовать SSL шифрование** - если есть ***SSL сертификат***, то система позволяет транслировать данные по зашифрованному каналу.
- **Ожидать подтверждения** - в основном требуется при использовании нестабильных каналов связи, для проверки целостности, передаваемых данных.
- **Таблица перекодировки** - назначение таблицы кодов сообщений, которая должна соответствовать таблице сообщений принимающей системы.

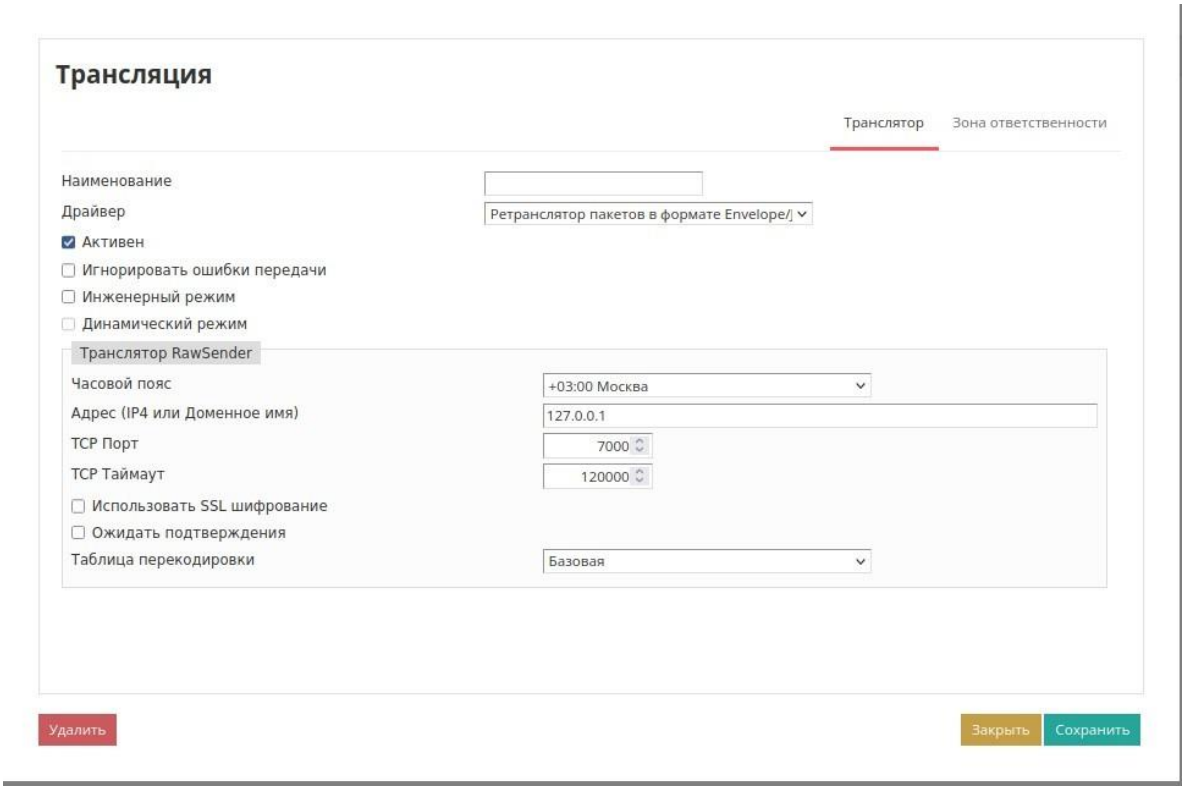


Рис. 20 Ретранслятор пакетов в формате Envelope/JSON

5.3.1.1.4 Передача информации по протоколу ЕППС(Зеркалирование)

Данный протокол разработан в ООО "ЭЛЕСТА" и является протоколом, использующим сквозное шифрование. Шифрование данных происходит на уровне драйвера. Использование протокола ЕППС позволяет связать два и более компьютеров в одну сеть и осуществлять контроль за объектами их управление, с любого из них. Удаленный доступ к прибору может осуществляться только с того сервера КРОС, к которому прибор подключен в данный момент. На остальных компьютерах будет доступен только протокол событий по приборам. Преимуществом использования данного протокола можно считать и тот момент, что ОП может использовать несколько каналов связи(например, для каждого сервера свой), соответственно и в приборах может

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

быть указано несколько адресов и портов серверов. После объединения серверов по протоколу ЕППС они обмениваются информацией в режиме реального времени.

Трансляции, с использованием протокола ЕППС, может создавать только пользователь с правами **superadmin**.

Администратор охранной организации, прав на создание трансляций, с использованием протокола ЕППС **не имеет**.

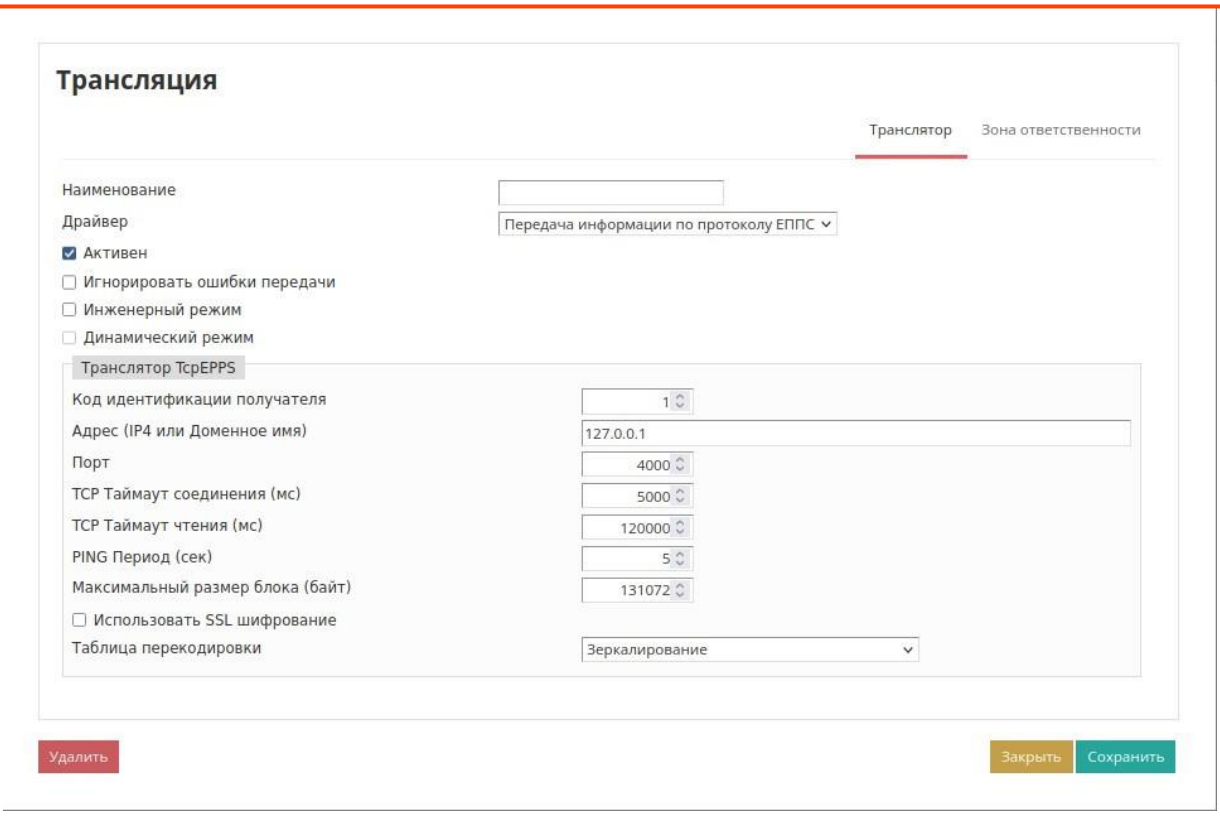


Рис. 21 Карточка создания трансляции по протоколу ЕППС

- **Код идентификации получателя** - При создании ОО каждому подразделению присваивается личный номер. На разных серверах они могут быть разными. Поэтому прежде чем создавать трансляцию необходимо выяснить какой идентификатор имеет ОО на принимающем сервере. После этого необходимо указать, полученный номер в этом поле.
- **Адрес (IP или Доменное имя)** - В этом поле необходимо указать IP-адрес(IPv4) в формате ***"aaa.bbb.ccc.ddd"*** или доменное имя компьютера или маршрутизатора, на который буден транслироваться поток данных.
- **Порт** - Порт по которому будет осуществляться соединение с сервером-приёмником. По-умолчанию используется порт:***4000***, но можно использовать порт указанный на принимающей стороне. Если трансляция настраивается на сервер вне локальной сети, необходимо обеспечить

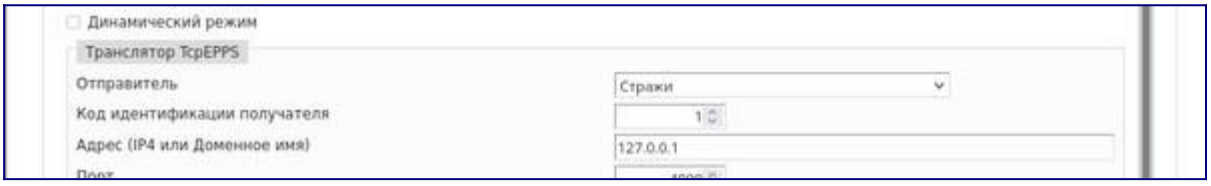
SEC.RU | Короткий путь к информации Скачано с sec.ru

доступ к удаленному серверу по этому порту. Настоятельно рекомендуется для каждой трансляции использовать отдельное значение этого параметра.

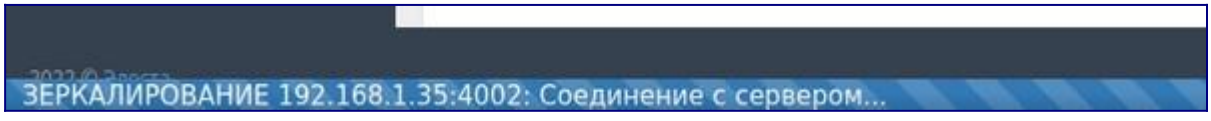
- **TCP Таймаут соединения(мс)** - максимально допустимое время в миллисекундах, в течении которого сервер ждет соединения с принимающей стороной для передачи пакета с информацией, после чего начинает формировать очередь сообщений и делать повторные попытки соединиться.
- **TCP Таймаут чтения(мс)** - максимально допустимое время в миллисекундах, в течении которого должен дойти пакет от передающего сервера. В случае если пакет не дошел, начинает формироваться очередь на прием и сервер повторяет попытки.
- **PING Период (сек)** - период проверки доступности сервера, принимающего сообщения.
- **Максимальный размер блока (байт)** - параметр, определяющий размер блока, передаваемой информации. При сильных нагрузках на локальную сеть, возможно, имеет смысл снизить это значение в два, а то и три раза. Однако, если, при описании объекта Вы используете изображения с большим разрешением, возможно имеет смысл увеличить это значение в два раза.
- **Использовать SSL шифрование** - если есть ***SSL сертификат***, то система позволяет транслировать данные по зашифрованному каналу.
- **TCP таймаут (мс)** - максимально допустимое время в миллисекундах, в течении которого должен передаваться пакет информации.
- **Максимальный размер блока (байт)** - параметр, позволяющий отличить проводные приборы от радиоканальных при обработке сообщений.
- **Таблица перекодировки** - назначение таблицы кодов сообщений, которая должна соответствовать таблице сообщений принимающей системы. При использовании протокола ЕППС, используемая таблица, "Зеркалирование"

Внимание!!!

При регистрации в системе под пользователем *superadmin* при настройке Трансляций доступен только режим **Передача информации по протоколу ЕППС**. При этом можно настроить трансляции отдельно для каждой ОО. В списке дополнительных параметров появляется:



Отправитель - наименование ОО, для которой настраивается текущая трансляция. Для одной ОО может быть настроено несколько трансляций на разные сервера, при этом для каждой трансляции рекомендуется использовать разные значения параметра **Порт**.



При регистрации на сервере КРОС нескольких ПЦО, ЧОП, ОП, в случае настройки трансляции, рекомендуется настраивать трансляции именно под пользователем *superadmin*.

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

5.3.1.1.5 Трансляция по протоколу УАРМ

Протокол для взаимодействия со сторонними системами, поддерживающими данный формат приемо-передачи. Для создания трансляции необходимо заполнить, следующие поля:

- **Наименование** - Ввести произвольное наименование.
- **Драйвер** - Выбрать в списке "Унифицированный АРМ".
- **Транслятор Uarm** - Настройки трансляции на приемо-передачу:
  - **Часовой пояс** - часовой пояс охранной организации, куда транслируются события.
  - **Токен сегмента данных приёмника** - Необходимо указать предоставленный UUID, предоставленный принимающей стороной. Необходим для унификации канала.
  - **URL приемника для трансляции данных** - Указать адрес унифицированного АРМ, того который будет принимать информацию.
  - **URL передатчика для обработки команд** - Указать адрес унифицированного АРМ, того который будет отправлять информацию.
  - **Период отправки тестовых сообщений (сек)** - Периодичность отправки пакетов. Если установлено значение "0", значит информация передаётся постоянно.

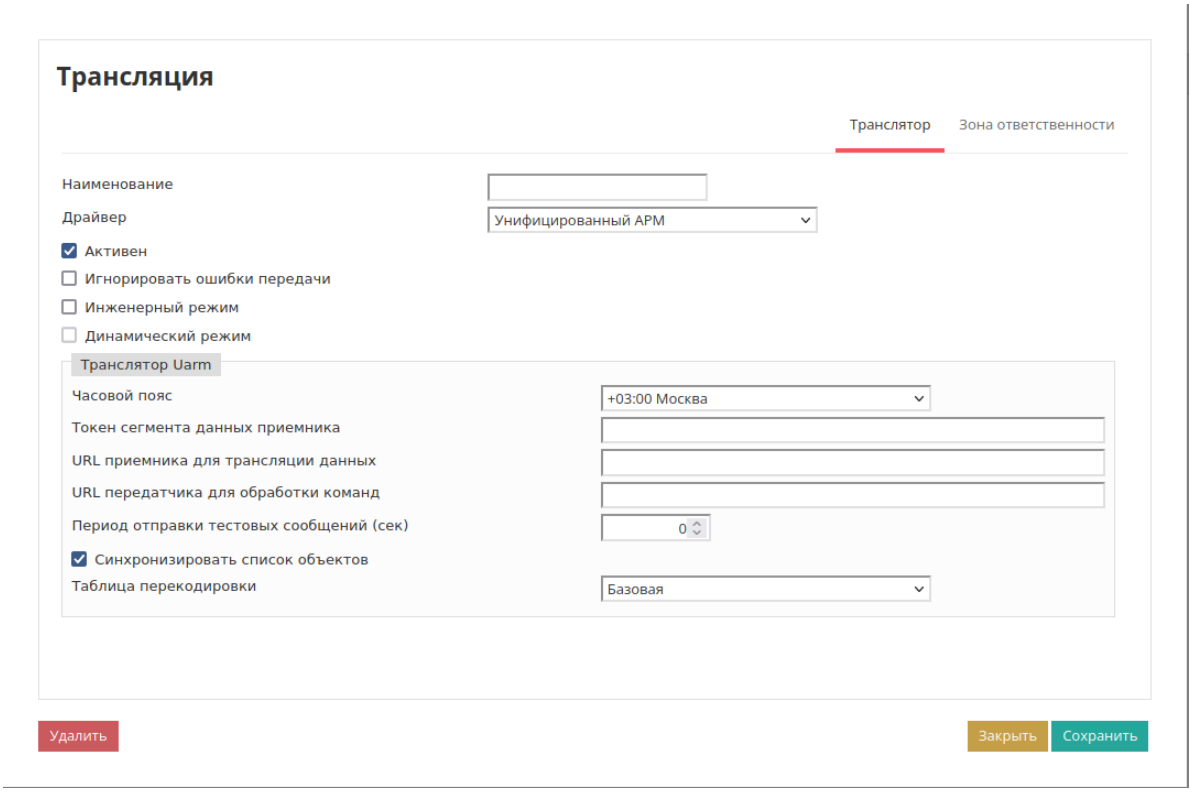


Рис. 22 Карточка создания трансляции по протоколу УАРМ

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

5.3.1.2 Таблица перекодировки

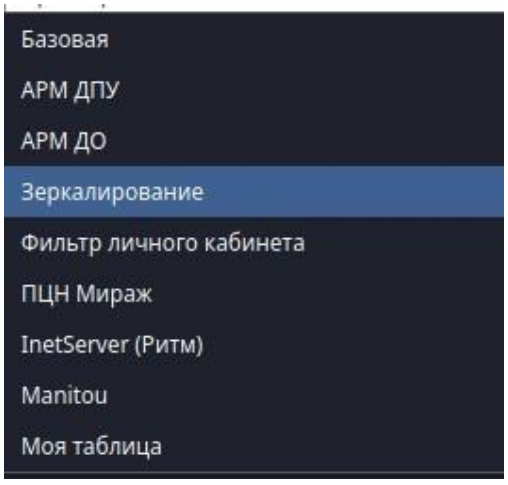


Рис. 23 Список выбора таблиц перекодировок

Выбор таблицы перекодировки осуществляется из выпадающего списка **«Таблица перекодировки»**(рис. 23), который присутствует в протоколах, требующих перекодировки кодов сообщений/извещений.
Выбор таблицы включает в себя:

Базовая - Базовая таблица, включает в себя все основные сообщения, кроме служебной информации.
АРМ ДПУ - Таблица стандартных сообщений для работы оператора пульта охраны.
АРМ ДО - Таблица сообщений для "дежурного офицера" включает в себя информацию по объектам, переданным ему на контроль.
Зеркалирование - Таблица содержит все возможные, на момент релиза, сообщения, передаваемые по протоколу ЕППС. По факту - отключение фильтра - прямая передача всего потока сообщений/извещений. Предназначен для использования в протоколе ЕППС.
ПНЦ Мираж - Таблица сообщений совместимых с ПНЦ Мираж.
InetServer(Ритм) - Таблица сообщений совместимых InetServer.
Manitou - Таблица сообщений совместимых с Manitou.
Моя таблица - Таблица созданная администратором ОП, в соответствии с требованиями и пожеланиями сотрудников ОП. Данная таблица создается самостоятельно и может иметь наименование согласно своей задаче.

О таблицах перекодировки сообщений/извещений более подробно можно прочитать в разделе **Таблицы**.

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

5.3.1.3 Зона ответственности

В том случае, когда необходимо ограничить передачу информации по объектам или, когда есть единый центр охраны и от него настраивается передача информации, не связанным между собой конечным потребителям этой информации, в этом случае можно ограничить передачу данных, задав **зону ответственности**.

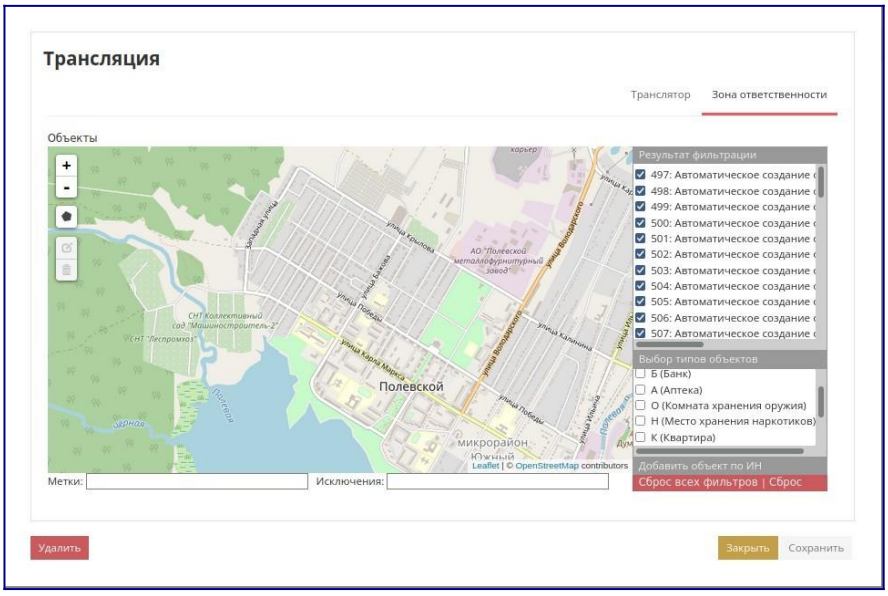


Рис. 24 Зона ответственности со списком объектов и типом объектов

Задать зону ответственности можно несколькими способами:

- **Выбор типов объектов** - использование фильтра позволит выбрать объекты по типу, который был назначен объекту при заполнении карточки объекта. При этом в окне **Результат фильтрации** будут отмечены те объекты, которые отвечают, выбранному типу или типам.
- **Метки** - Несколько объектов, помимо типа, можно объединить в группы используя метки. Если указать эту метку, то объекты с этой меткой попадут в **Результат фильтрации**.
- **Исключения** - объекты с указанной здесь меткой будут исключены из списка **Результат фильтрации**.
- **Выбрать зону ответственности, используя редактор зоны**. Для этого в левой части окна, там где расположена карта, необходимо нажать пиктограмму с пятиугольником и вызвать редактор, создания зоны. Далее, следуя подсказкам рядом с маркером вы создадите зону, после чего в окне **Результат фильтрации** будут отмечены те объекты, которые попали в эту зону. Используя знаки + и - можно увеличить или уменьшить масштаб карты. Можно создать несколько зон ответственности.
  - **Редактировать зону ответственности**. Если есть необходимость редактировать зону ответственности, то в этом случае необходимо нажать на значок **Редактировать**. На карте активируются границы зоны и появятся дополнительные точки, передвигая которые, можно

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

увеличить или уменьшить зону. После окончания редактирования, необходимо нажать надпись **"Сохранить"** или **"Отменить"**, рядом со значком **Редактировать**.

- **Редактировать зону ответственности**. Если есть необходимость редактировать зону ответственности, то в этом случае необходимо нажать на значок **Редактировать**. На карте активируются границы зоны и появятся дополнительные точки, передвигая которые, можно увеличить или уменьшить зону. После окончания редактирования, необходимо нажать надпись **"Сохранить"** или **"Отменить"**, рядом со значком **Редактировать**.

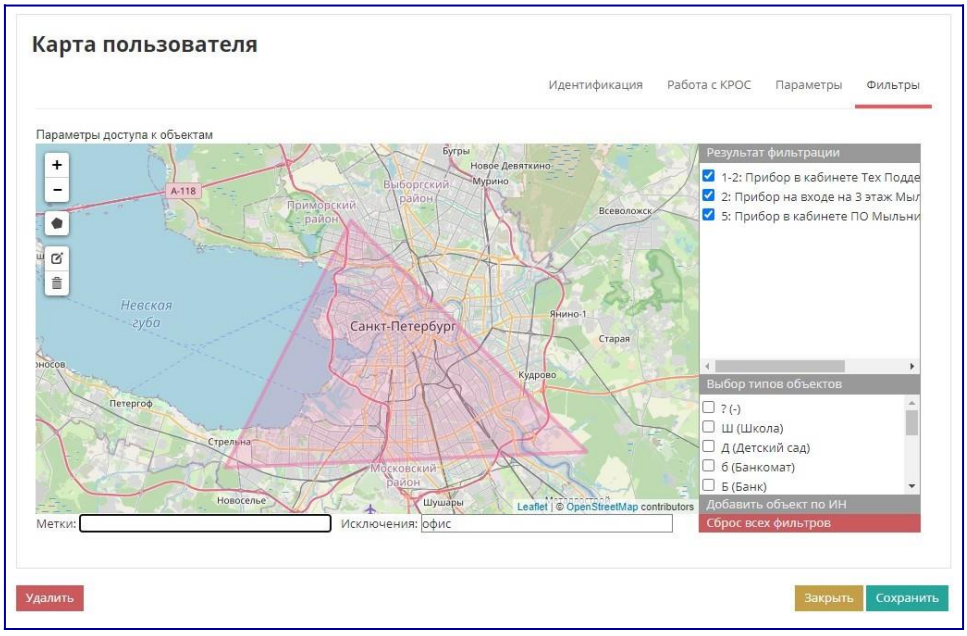


Рис. 25 Зона ответственности после редактирования

- **Удалить зону ответственности** - если возникла необходимость в удалении зоны ответственности. Необходимо выбрать значок **Удалить** и указать зону, которую надо удалить. После удаления зоны **Результат фильтрации** должен измениться.

- **Сброс всех фильтров** - сбросит все результаты фильтрации.
- **Сброс** - вернет состояние зоны ответственности на значение по-умолчанию.

При создании зоны ответственности, методы фильтрации можно комбинировать.

После задания фильтров в окне **Результаты фильтрации** можно дополнительно отметить или снять отметку выделения с объекта. В результате выполненных действий список объектов отображаемых, в АРМ, трансляциях или у пользователя будет ограничен.

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

5.3.2 Сохранение, редактирование и удаление настроек трансляции

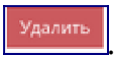
После того как все необходимые данные для создания трансляции введены, в окне "Трансляция" необходимо нажать на кнопку **«Сохранить»** 

Для редактирования настроек, а так же если необходимо удалить трансляцию необходимо:

1. Нажать на кнопку «редактировать»  трансляцию.

2. При необходимости внести изменения в трансляцию.

3. Нажать «Сохранить» 

, а при удалении - **«Удалить»** 

.

Если никаких изменений в трансляцию не вносилось или нет необходимости в их сохранении, тогда необходимо нажать на кнопку **«Закрыть»** 

5.4 Таблицы

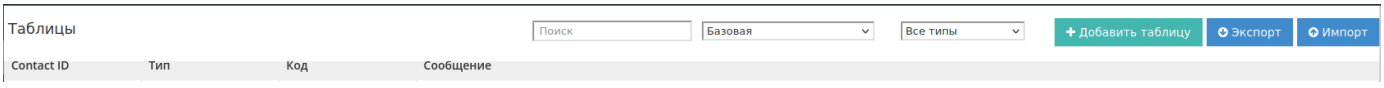
В окне **«Таблицы»** (меню **«Сервер»** → **«Таблицы»**) создаются, редактируются и удаляются таблицы перекодировки сообщений\извещений.
Окно **«Таблицы»** по-умолчанию доступно **Администратору сервера**, **Администратору** и **Инженеру**.

Редактирование таблицы доступно только **Администратору сервера.**
Администратор ОП может редактироавть и удалять таблицы только в пределах своей ОО.

Базовые таблицы редактированию и удалению не подлежат. В случае необходимости, использования своей таблицы сообщений, необходимо создать копию существующей и вносить изменения в неё, после чего можете назначать свою таблицу сообщений/извещений пользователю или указать при создании трансляции. Таблицы перекодировки сообщений/извещений служат для возможности изменения формируемых сообщений выводимых в ленту событий:

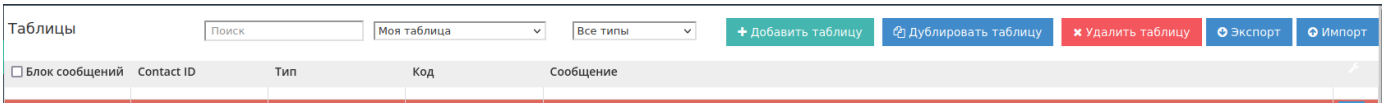
- АРМ ДПУ/ДО/Инженера, Web-АРМ
- мобильное приложение "Личный кабинет"
- трансляции в протоколе SurGard
- извещения для отправки SMS

При выборе встроенных таблиц интерфейс будет выглядеть следующим образом:



При выборе таблицы созданной администратором ОП интерфейс немного поменяется:

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

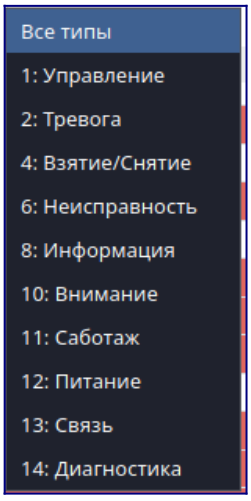


Администратор предприятия может создать свою таблицу, дублировать выбранную таблицу и редактировать сообщения уже в ней, так же есть возможность экспортировать таблицу или импортировать ранее созданную.

5.4.1 Описание раздела и полей таблиц сообщений/извещений

Поиск - Позволяет осуществлять поиск в таблице сообщений по коду, типу и наименованию сообщения.

- **Таблица перекодировки** - Фильтр позволяет выбрать таблицу для просмотра и редактирования.



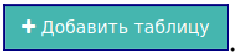
- **Фильтр типов сообщений** - После выбора типа сообщения в таблице отображаются записи, соответствующие, выбранному фильтру
  - **Все типы** - отключение фильтра сообщений. Отображаются все записи.
  - **1.Управление** - отображаются сообщения, связанные с управлением приборов.
  - **2.Тревога** - отображается список сообщений тревожных состояний.
  - **4.Взятие/Снятие** - отображает сообщения, связанные с постановкой объекта/прибора на охрану и снятие с охраны.
  - **6.Неисправность** - фильт сообщений, связанных с неисправным состоянием прибора.
  - **8.Информация** - список сообщений информирующих о работе приборов.
  - **10.Внимание** - сообщения которые требуют внимания инженерных служб.
  - **11.Саботаж** - сообщения требующие особого внимания, так как связаны с условиями эксплуатации и обслуживания приборов.
  - **12.Питание** - Информационные сообщения, отражающие состояние электропитания прибора.
  - **13.Связь** информационные сообщения, связанные с условиями эксплуатации каналов связи.
  - **14.Диагностика** - сообщения о проверки работы каналов связи и электропитании.
- **Экспорт** - позволяет экспортировать, выбранную таблицу в файл формата "xml", что позволяет перенести её на другой сервер КРОС.

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

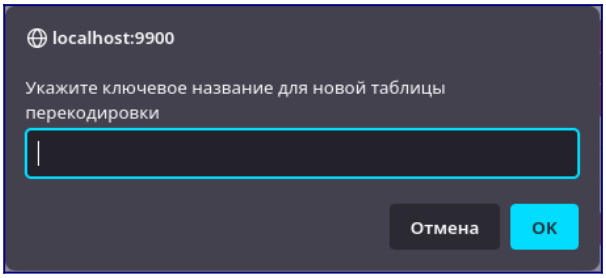
- **Импорт** - позволяет импортировать таблицу из файла формата "xml", созданного на другом сервере КРОС.
- Поля таблицы сообщений:
- **Contact ID** - это протокол передачи данных, который получил наиболее широкое распространение в охранных системах. Он был создан для того, чтобы привести процесс передачи информации к единому стандарту, чтобы устройства от различных производителей могли правильно работать друг с другом.
- **Тип** - тип сообщения. Назначается в соответствии со спецификой охранной системы.
- **Код** - внутренний код сообщения, принятый в КРОС.
- **Сообщение** - расшифровка/пояснение кода сообщения.

5.4.2 Добавление таблицы

Чтобы добавить таблицу перекодировки сообщений\извещений нужно:

1. Нажать на кнопку "Добавить таблицу" 

.
2. В появившемся окне подтверждения ввести название таблицы.



3. Нажать «ОК».

По-умолчанию таблицы сообщений создаются на основе **Базовой таблицы перекодировки**. Однако за основу можно выбрать любую из имеющихся таблиц или **"Дублировать таблицу"**

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

5.4.3 Редактирование сообщения в таблице

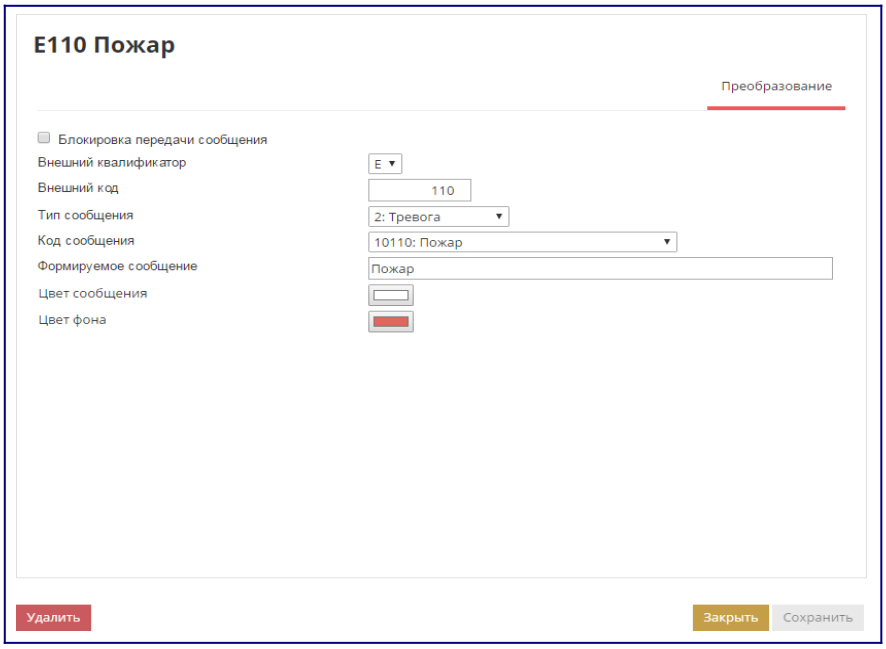


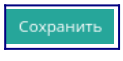
Рис. 26 Карточка сообщения таблицы извещений

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

Для редактирования сообщения в таблице:

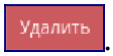
1. Через поиск найти текущее название сообщения.
2. Нажать на кнопку "редактировать" .
3. После нажатия открывается окно редактирования сообщения. В данном окне возможно задать:

- **Блокировка передачи сообщения** - запретить передачу сообщений, содержащих текущий код.
- **Внешний квалификатор** - определяет начало **"E"** или конец **"R"** события.
- **Внешний код** - код, соответствующий событию, который необходимо передать/транслировать.
- **Тип сообщения** - отределяет тип сообщени. По сути это его важность.
- **Код сообщения** - код сообщения, принятый в комплексе КРОС.
- **Формируемое сообщение** - текстовое сообщение, которое будет включено в передачу/трансляцию.
- **Цвет сообщения и цвет фона** - Пользователи имеют возможность изменить цвет фона и цвет текста в сообщении, которое будет приходить в ленту событий, только в том случае, если цветовая палитра не определена ГОСТ Р 55017—2012 и регламентными документами НИЦ «Охрана».

4. Нажать **«Сохранить»** 

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

Для закрытия без сохранения, необходимо нажать на кнопку **«Закрыть»** 

в окне редактирования сообщения. Для удаления записи из таблицы сообщений надо нажать на кнопку "Удалить" 

. Удаление сообщений нужно производить крайне осторожно, иначе есть риск потерять важные информационные сообщения.

5.4.4 Удаление таблицы сообщений

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», «АРМ ДО» и «Фильтр личного кабинета» удалить нельзя.

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

6. Меню «Клиенты»

Так как пользователь с правами **superadmin** осуществляет общее управление сервером, данный раздел ему ***недоступен***.

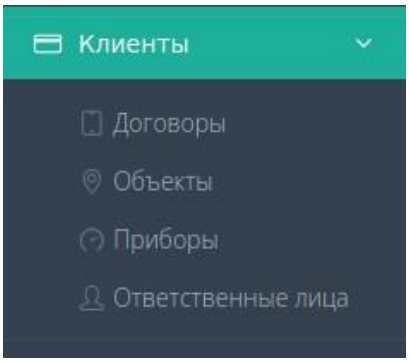


Рис. 26 Меню «Клиенты»

Раздел **"Клиенты"** доступен только пользователям в рамках ОО. Доступ к данным, возможность создавать, редактировать и удалять записи в разделе определяется Ролью пользователя.

- **Договоры** - Создание и управление договорами, с которыми связаны объекты, юридические и физические лица.
- **Объекты** - Объекты охраны, включают в себя как объекты недвижимости, так и мобильные объекты, по которым заключены договора. Так же здесь могут быть объекты не связанные договором.
- **Приборы** - Список всех приборов, с которыми работает данное ОП.
- **Ответственные лица** - *Хоз. органы* - список всех ответственных и делегированных лиц по всем объектам.

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 (рис. 27).

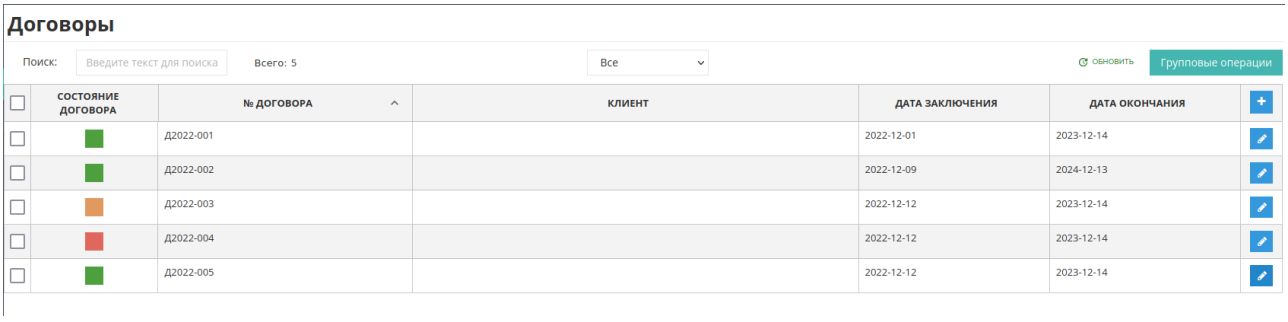
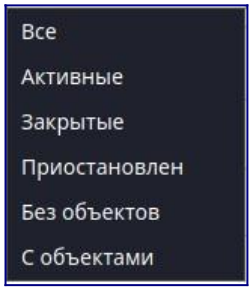


Рис. 27 Таблица договоров

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

Описание таблицы "Договоры":

- **Поиск** - позволяет осуществлять поиск договора по любому параметру.
- **Всего** - отображает общее количество договоров в данной ОО.
- **Фильтр состояния договоров** - фильтр состояния договоров:
  - **Все** - отображает все договора которые присутствуют в БД.
  - **Активные** - позволяет вывести все активные договора на текущую дату.
  - **Закрытые** - в таблице будут отображены договора, действие которых закончилось.
  - **Приостоновлен** - будут показаны договора имеющие статус **"Приостановлен"**.
  - **Без объектов** - фильтр позволяет отобрать договора не связанные с объектами.
  - **С объектами** - в список попадут только те договора, где есть объекты.



- **Обновить** -  - Сделать принудительное обновление текущей информации по состоянию договоров.
- **Групповые операции** - позволяет выполнить однотипные операции сразу с несколькими выбранными договорами .

Столбцы в таблице имеют следующее назначение:

-  - Поле выбора. При нажатии выбирает все договора. Также можно выбрать отдельные записи нажав, на значок в соответствующей строке.
- **СОСТОЯНИЕ ДОГОВОРА** - Всего существует три основных состояния договора:
  - ■ - **Активен** - Действующий договор.
  - ■ - **Закрыт** - Действие договора закончилось или неопределен срок начала действия договора.
  - ■ - **Приостановлен** - Действие договора приостановлено на время или до особого распоряжения.
- **№ ДОГОВОРА** - Наименование договора, принятое внутри ОП. Заполняется при оформлении карточки договора.
- **КЛИЕНТ** - После того, как будут заполнены реквизиты, отображает ФИО, если договор заключён с физическим лицом и ***Краткое наименование***, когда договор заключен с юридическим лицом или статус лица, с которым заключается договор ***Неопределен***.
- **ДАТА ЗАКЛЮЧЕНИЯ** - Дата заключения договора или дата начала действия договора.

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

- **ДАТА ОКОНЧАНИЯ** - Дата окончания действия договора или дата начала действия договора.
-  - Добавить новый договор.
-  - Редактировать данные, выбранного договора.

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

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

6.1.1 Добавление, редактирование и удаление договора охраны

6.1.1.1 Учётная карточка договора охраны

1. Необходимо войти в КРОС под учетной записью, имеющей право на добавление договоров. По умолчанию, добавлять договора могут пользователи, имеющие Роль - "Администратор" и "Менеджер".
2. Перейти в меню **Клиенты → Договоры → Создать новый договор**, для чего в таблице договоров нажать на кнопку "Добавить" 

6.1.1.1.1 Вкладка «Основная»

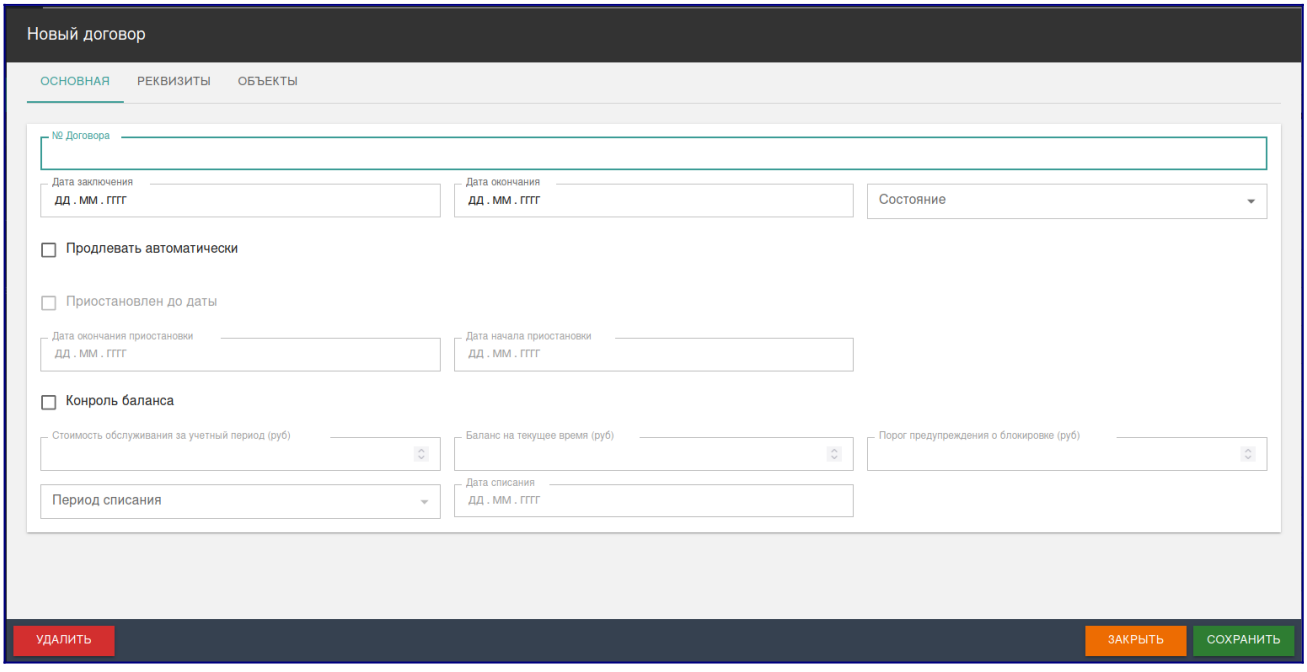


Рис. 28 Форма для регистрации нового договора. Вкладка «Основная»

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

В открывшемся окне, на вкладке **«Основная»**, необходимо заполнить поля.

- **№ Договора** - В поле вводится номер договора в соответствии с нормами учета, принятыми в данной ОО. Данное поле обязательно к заполнению. При наличии договора с таким наименованием, система выдаст предупреждение.
- **Дата заключения** - Дата заключения договора. При заполнении карточки договора, дата заключения договора, не обязательно должна совпадать с текущей датой.
- **Дата окончания** - дата окончания действия договора. По умолчанию, срок действия договора 1 год. Однако, её можно изменить, воспользовавшись встроенным календарём.
- **Продлевать автоматически** - Если по условиям договора предусмотрено продление договора, а так же в случае бессрочного договора или срок действия договора не определён, необходимо выставить данный параметр, тогда при наступлении даты окончания действия договора, пролонгация договора будет включена автоматически, сроком ещё на один год.
- **Состояние** - Всего существует три основных рабочих состояния договора и режим "ожидания":

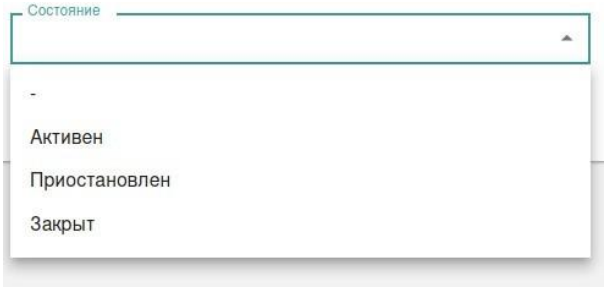


Рис. 29 Состояния договоров

- **Активен** - договор действует
- **Приостановлен** - действие договора временно приостановлено до особого решения и по времени не ограничено. В случае, когда выбирается данное состояние, возможен вариант временной приостановки действия договора. При указании ***"Приостановлен до даты"*** необходимо указать дату, до которой договор будет приостановлен - "Дата окончания приостановки". После достижения этой даты договор автоматически переходит в режим **"Активен"**. В поле "Дата начала приостановки" система информирует - с какой даты действие договора было приостановлено.
- **Закрыт** - договор не действует.
- **В ожидании** - это означает, что в карточке договора не выставлен статус, либо дата начала действия договора еще не наступила.

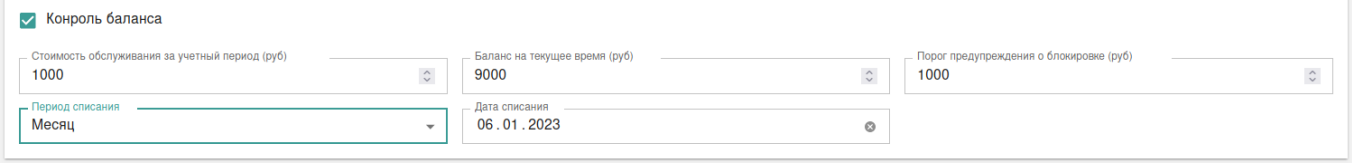


Рис. 30 Контроль баланса договора

- **Контроль баланса** - позволяет контролировать денежные средства клиента при абонентском обслуживании:

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

- *Стоимость обслуживания за учетный период (руб)* - абонентская плата до договору
- *Баланс на текущее время (руб)* - сумма остатка денежных средств по договору, после вычета абонентской платы. Здесь указывается сумма вносимая клиентом при заключении договора или же корректируется при пролонгации договора, или внесении доплаты клиентом.
- *Порог предупреждения о блокировке (руб)* - указывается сумма-порог, при достижении которой оператору/менеджеру/администратору будет сообщатся о том, что данный договор будет приостановлен в следствии отсутствия средств на обслуживание.
- *Период списания* - На данный момент предусмотрено ежемесячное списание средств или раз в полгода.
- *Дата списания* - выставляется дата оказания услуги. Если дата не указывается, то списание начинается с даты заключения договора.

- **Договор инкассации** - Данная отметка скрыта для обычных пользователей и используется при заключении договора инкассации. В этом случае, у роли пользователя, создающего договор, должен быть разрешен "Режим дежурного инкассатора", и тогда договору может быть присвоен данный статус.

После заполнения данной формы, необходимо сохранить введенную информацию, для чего следует нажать кнопку "Сохранить" 

. После этого можно продолжить заполнять информацию по договору или отложить этот процесс, нажав кнопку "Закрыть" 

.

6.1.1.1.2 Вкладка «Реквизиты»

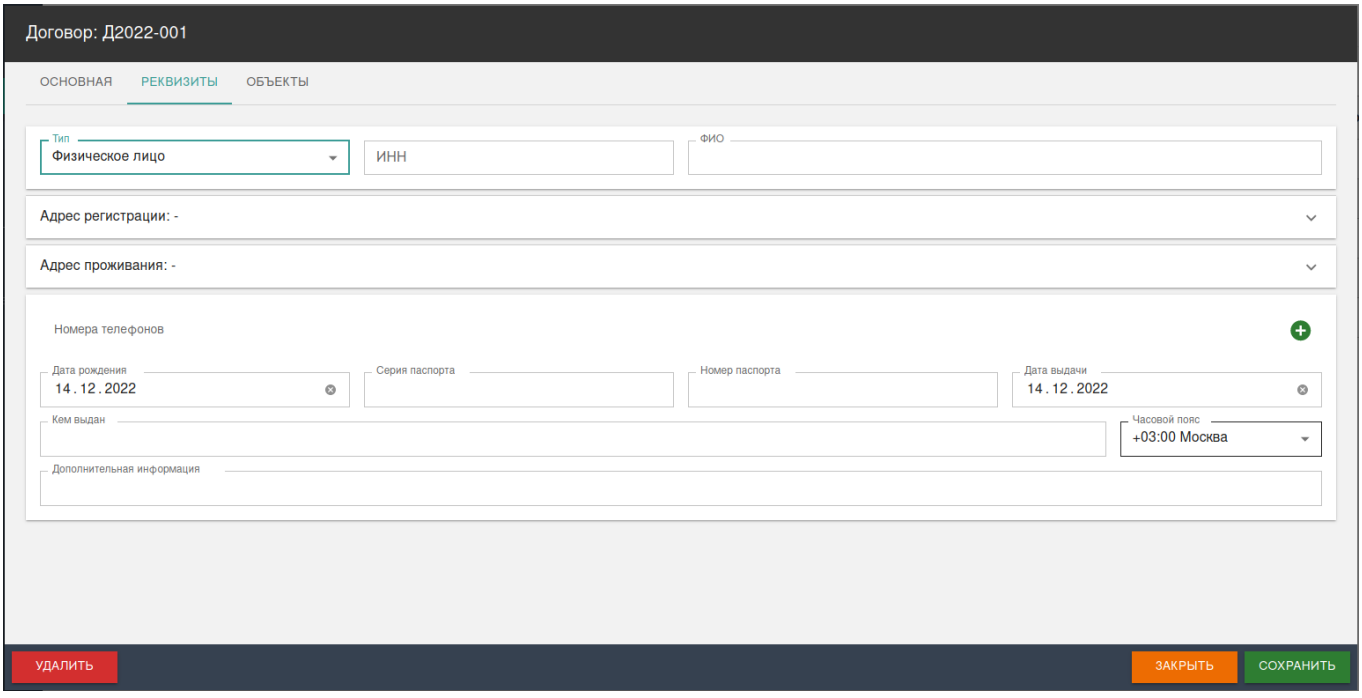


Рис.31 Форма для регистрации нового договора. Вкладка «Реквизиты» физического лица

Вкладка **«Реквизиты»** договора предназначена для ввода информации по субъекту, заключающему договор.

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

- **Тип** - выпадающий список позволяет выбрать тип субъекта - "Физическое лицо" или "Юридическое лицо". Выбор типа определяет форму для заполнения.
- **ИНН** - ввести номер ИНН. При заполнении ИНН для юридического лица, после нажатия на кнопку **Поиск** , вся доступная информация заполнит поля автоматически.

Основные данные *Физическое лицо*:

- **ФИО** - Фамилия, Имя, Отчество, заключающего договор. Данные вводятся так, как указаны в паспорте.
- **Адрес регистрации** - Данные постоянной или временной регистрации указываются так, как указаны в паспорте. Для ввода и редактирования данных, достаточно активировать запись, когда указатель изменит свой вид на .
- **Адрес проживания** - Адрес фактического проживания. Для ввода и редактирования данных, активируйте запись, когда указатель изменит свой вид на .
- **Номера телефонов** - Данная форма заполняется аналогично форме в разделе "Ответственные лица".
- **Дата рождения** - Дата рождения лица, с которым заключается договор.
- **Серия паспорта** - Необходимо указать только серию паспорта.
- **Номер паспорта** - Необходимо указать только номер паспорта.
- **Дата выдачи** - Дата выдачи паспорта.
- **Кем выдан** - Необходимо указать каким подразделением выдан паспорт, а так же указать код этого подразделения.

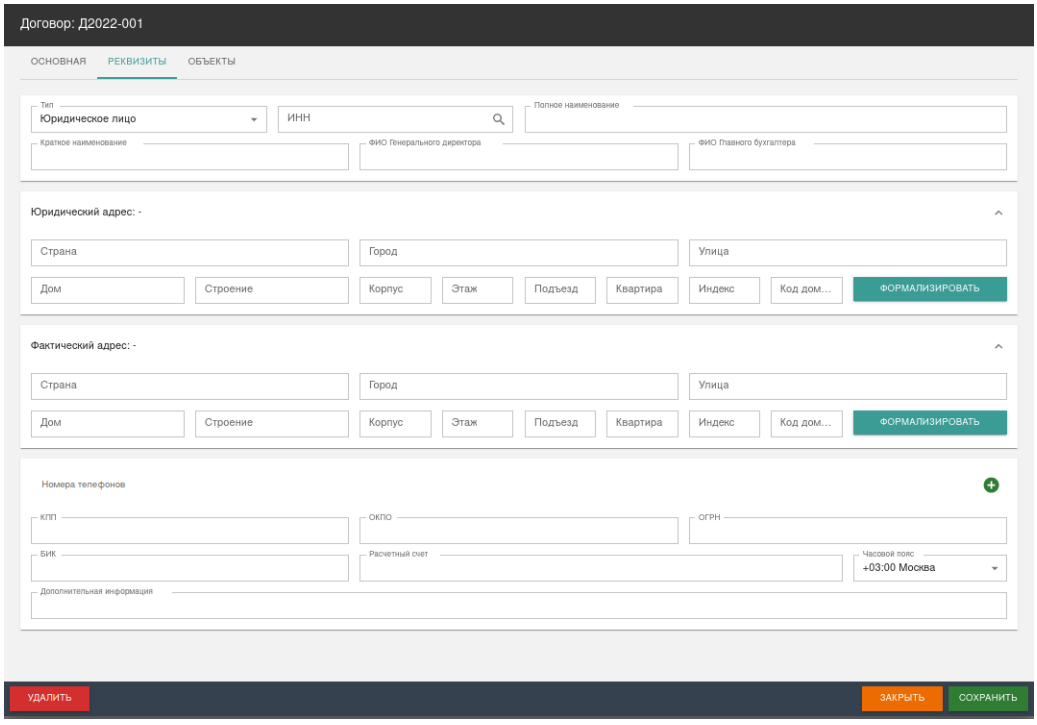


Рис.32 Форма для регистрации нового договора. Вкладка «Реквизиты» юридического лица

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

Основные данные *Юридическое лицо*:

- **Полное наименование** - Полное наименование согласно регистрационным документам.
- **Краткое наименование** - Краткое наименование юридического лица. Поле **"Краткое Наименование"** обязательно к заполнению при создании договора.
- **ФИО Генерального директора** - Указывается Генеральный директор или лицо, исполняющее его обязанности.
- **ФИО Главного бухгалтера** - Указываются данные Главного бухгалтера или лица, его заменяющего.
- **Юридический адрес** - Адрес, по которому зарегистрировано юридическое лицо.
- **Фактический адрес** - Адрес реального месторасположения юридического лица.
- Для ввода и редактирования данных Юридического и Фактического адресов, активируйте запись, когда указатель изменит свой вид.
- **Номера телефонов** - Если с договором связан какой-либо номер телефона, то его можно указать в этом поле. Для этого необходимо нажать на кнопку "Добавить"  и заполнить форму, аналогично заполнению формы в разделе "Ответственные лица".
- **Реквизиты** - Статистические данные по юридическому лицу
  - **КПП** - Код причины постановки на учет — это код, который дополняет ИНН и содержит информацию об основании постановки на учет в налоговом органе.
  - **ОКПО** - общероссийский классификатор предприятий и организаций. Состоит он из 8 или 10 цифр. Каждой фирме Росстат присваивает уникальный ОКПО, его обязана иметь любая организация.
  - **ОГРН**(для ИП – **ОГРНИП**) – это основной государственный регистрационный номер юридического лица, который присваивается при его создании и после записи о нем в ЕГРЮЛ (или ЕГРИП для ИП). Указывается ОГРН в свидетельстве, которое официально выдается налоговой службой и свидетельствует о постановке на налоговый учет.
- **Банковские реквизиты**
  - **БИК** - Банковский идентификационный код – девятизначный уникальный код кредитной организации. Он предназначен для идентификации участников расчетов и является обязательным элементом реквизитов любого банка. БИК используется в платежных документах на территории России.
  - **Расчетный счет** — это специальный счет в банке, который открывается для индивидуальных предпринимателей и юридических лиц. Он используется для безналичных расчетов с контрагентами, выплаты заработной платы, уплаты налогов и сборов.

Так же можно установить :

- **Часовой пояс** - Часовой пояс в котором расположен субъект, заключающий договор.
- **Дополнительная информация** - Поле для ввода дополнительной и справочной информации по лицу, заключающему договор.

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

6.1.1.1.3 Вкладка «Объекты»

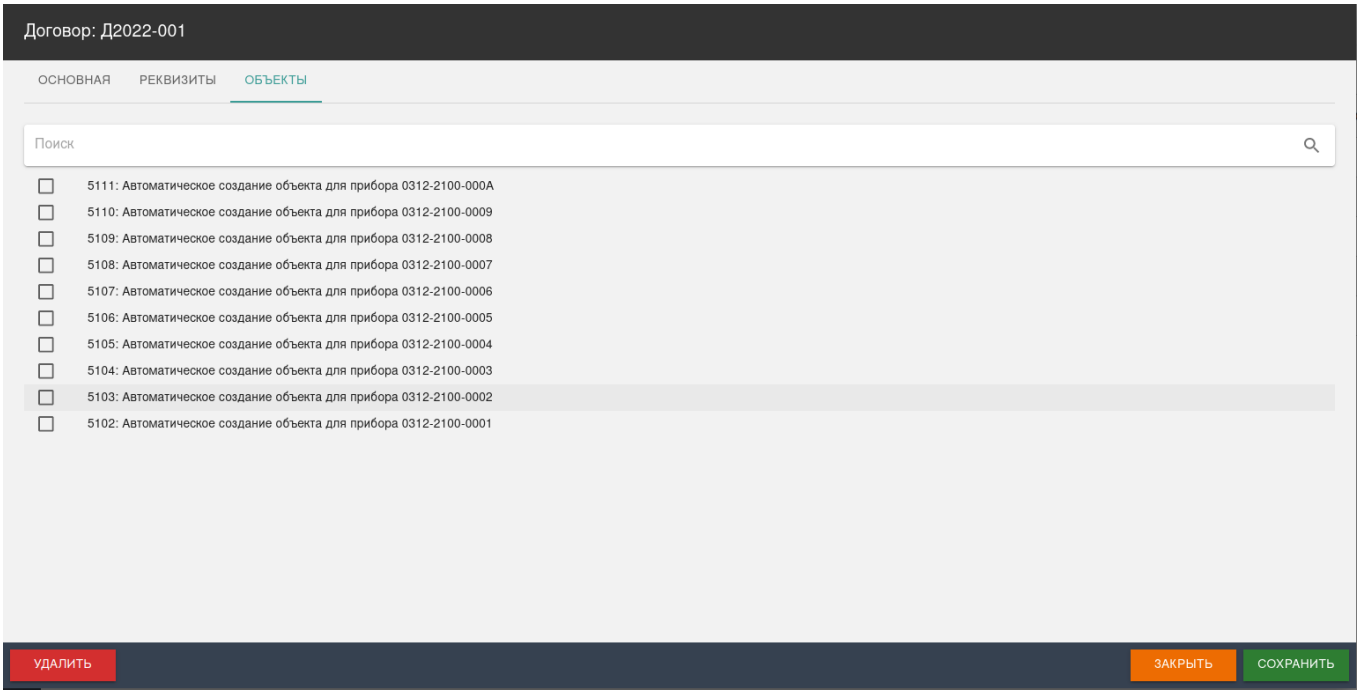


Рис.32 Форма для регистрации нового договора. Вкладка «Объекты»

Для того, чтобы прикрепить объект(ы) к договору, необходимо перейти на вкладку «Объекты».

В открывшемся окне, появится список доступных объектов. Необходимо выбрать один или несколько объектов, которые связаны с данным договором.

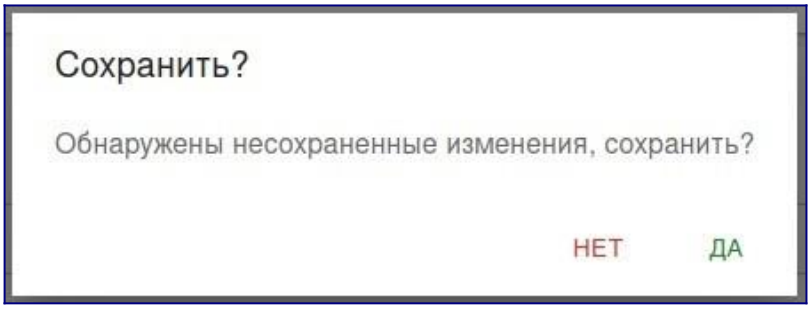
Во вкладке "Объекты" можно привязать объект только в том случае, если он был заранее создан во вкладке Клиенты → Объекты , в ином случае привязка происходит через карточку объекта или здесь, но после создания Объекта. Подробнее про привязку объекта к договору: **Добавление объекта**

6.1.1.2 Сохранение, редактирование и удаление договора охраны

Для сохранения договора охраны, нужно нажать кнопку **«Сохранить»** 

в окне **«Договор»**, чтобы не сохранять, нужно нажать кнопку **«Закрыть»** 

в окне **«Договор»**. Если в карточке договора были произведены какие-либо действия, то при закрытии данной



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

карточки ПО выдает предупреждение
необходимо подтвердить изменения или отказаться от них.

Для редактирования договора необходимо нажать на кнопку «Редактировать»  договор охраны, которая находится в строке с информацией о договоре справа. Затем внести изменения в договор охраны и нажать кнопку «Сохранить» 

.

Для закрытия договора охраны без сохранения, нажать **«Закрыть»** 

в окне **«Договор»**.

При удалении договора, необходимо войти в режим "Редактировать" и нажать кнопку "Удалить" 

После чего, подтвердить свое действие, нажав "ДА" или, отказавшись — "Нет".

6.1.2 Групповые операции с договорами охраны

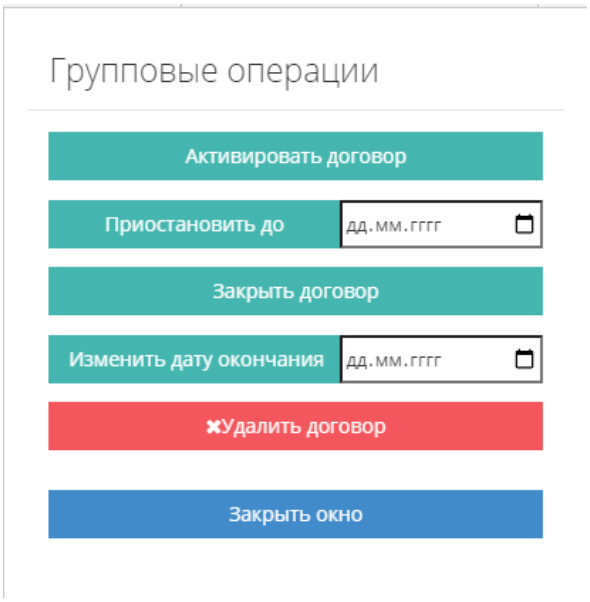


Рис. 33 Допустимые групповые операции с договорами

Групповые операции - позволяет выполнить однотипные операции сразу с несколькими выбранными договорами.

- **Активировать** - Активировать сразу несколько договоров, имеющих статус **Неопределен** или **Приостановлен**.
- **Приостановить до [** дд.мм.гггг **]** - указать дату, до которой приостанавливается действие одного или нескольких договоров.
- **Закрыть договор** - остановить действие договора(ов).
- **Изменить дату окончания [** дд.мм.гггг **]** - указать новую дату окончания договора(ов).
- **Удалить договор** - удалить, отмеченные договора.

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

♦ **Закрыть окно** - Закрыть, без выполнения групповых операций.

6.1.3 Иерархия

Комплекс КРОС учитывает следующую иерархию построения охранной деятельности:

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

↓

Объект охраны состоит из ***разделов*** одного или нескольких ***приборов***.Так же может быть ***мобильным объектом***.

↓

Прибор - устройство, устанавливаемое на ***объект***. Последством которого осуществляется управление режимами охраны. **Мобильный объект** - ***Мобильная тревожная кнопка***, **Мобильное приложение "Тревожная кнопка"**, **GPS-трекер "УМКА**.

↓

Раздел состоит из ***зон***. На одном приборе может быть настроено несколько разделов, каждый из которых может отвечать за отдельный объект. Один раздел может включать в себя несколько зон. Количество разделов и зон определяется констуктивной особенностью прибора, а так же возможностью подключения ***Расширителей***

↓

Зона — это часть охраняемого ***объекта***, контролируемого одним ***шлейфом*** охранной организации. На одном шлейфе может быть несколько оконечных устройств(датчиков).

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

6.2 Объекты

Для управления объектами необходимо осуществить переход меню **«Клиенты»** → **«Объекты»**.

В результате открывается таблица управления объектами в рамках одной охранной организации, поле для поиска объекта охраны и кнопка сортировки.

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

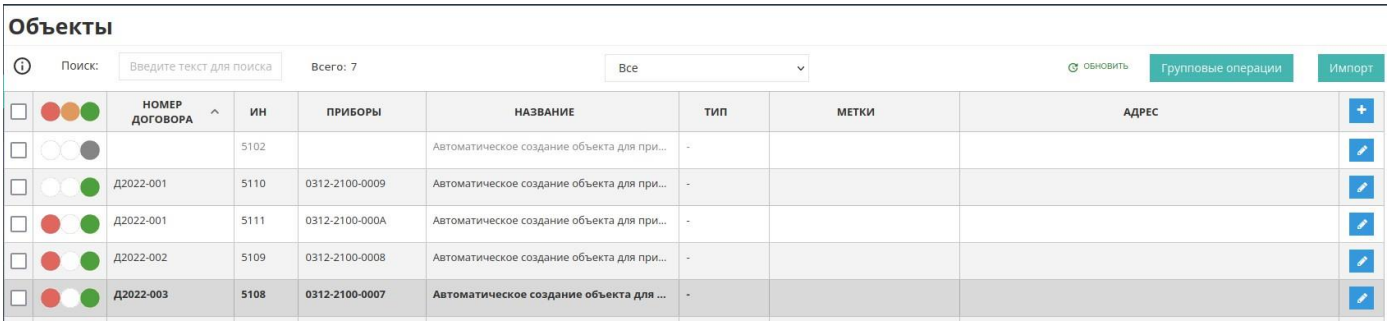
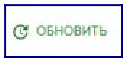


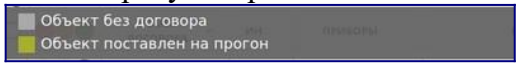
Рис.34 Таблица объектов

Основное управление объектами:

- **Поиск** - строка поиска объекта по любым известным признакам.
- **Всего** - отображает общее количество объектов в рамках текущей ОО.
- **Фильтр** - фильтр состояния объектов:
  - ***Все*** - все объекты(без фильтра)
  - ***Взят*** - отображаются объекты, которые находящиеся под охраной
  - ***Снят*** - отображает объекты, которые не находятся под охраной
  - ***Частично взят*** - отображаются объекты, которые частично взяты под охрану
  - ***В тревоге*** - отображаются объекты, на которых зафиксировано тревожное состояние
  - ***В неисправности*** - отображаются объекты на которых зафиксирована неисправность.
  - ***С договорами*** - будут показаны только те объекты, которые указаны в договорах
  - ***Без договора*** - будут показаны объекты без договоров
  - ***Приостановленные объекты*** - отображаются объекты действие договоров на которых приостановлено
  - ***Импортированные объекты*** - объекты имеющие статус импортированных, как правило это объекты перенесенные из "Юпитер-7". В связи с тем, что **Иерархия** взаимодействия объектов и субъектов в "Юпитер-7" и "КРОС" отличаются, при переносе данных, связанных с одним объектом, могут быть интерпретированы, как два объекта. При этом формат записи объекта будет выглядеть следующим образом - ***"(номерключа)"***, а связанные с ним разделы ***"(номерключа)=01"***, ***"(номерключа)=02"*** и т.д. Для объединения данных одного объекта необходимо воспользоваться функционалом - **Групповые операции**.
- **Обновить** - 

- Сделать принудительное обновление текущей информации по состоянию объектов.

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

- **Групповые операции** - Однотипные операции, выполняемые над одним и более объектами.
- **Импорт** - Импорт данных по объектам из других источников, представленных в файле формата "xml".
- Значение полей в таблице Объектов:
-  - Позволяет выделить все объекты или отдельные построчно для выполнения групповых операций.
-  - Отображает статус объекта/прибора(*Состояние тревоги, Состояние неисправности, Состояние охраны*):
  -  - Тревога
  -  - Ошибка канала связи
  -  - Неисправное состояние
  -  - Переход на резервный канал связи
  -  - Объект/Прибор взят под охрану
  -  - Объект/Прибор частично взят под охрану
  -  - Объект/Прибор снят с охраны
  -  - Статус не определен, ошибки и тревожные состояния отсутствуют.
- **НОМЕР ДОГОВОРА** - Отображается номер договора, к которому прикреплён объект(ы).
- **ИН** - Индивидуальный номер, идентификатор объекта, назначаемый ему при регистрации.
- **ПРИБОРЫ** - перечень приборов и устройств, установленных на объекте или закреплённых за ним.
- **НАЗВАНИЕ** - Наименование объекта, в формате принятом в ОО. Формат должен быть удобен для визуального восприятия оператором и дежурным.
- **ТИП** - Тип объекта назначается при регистрации объекта и выбирается из справочника(справочник можно редактировать, добавляя свои типы).
- **МЕТКИ** - Особые отметки, позволяют объединять объекты по особым признакам(помимо типа). Например, по операторам связи.
- **АДРЕС** - Адрес фактического местонахождения объекта или же адрес регистрации мобильного объекта.
-  - Добавить новый объект.
-  - Редактировать данные, выбранного объекта.
- Так же предусмотрена цветовая индикация инженерных режимов объекта:


, легенду можно посмотреть, наведя курсор на значок 

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

6.2.1 Добавление, редактирование и удаление объекта охраны

После того, как была нажата кнопка "Добавить" или "Редактировать", открывается карточка объекта, в которую вносится информация, необходимуя для осуществления охранной деятельности, а так же для обслуживания аппаратной части.

6.2.1.1 Учётная карточка объекта

6.2.1.1.1 Вкладка «Основная»

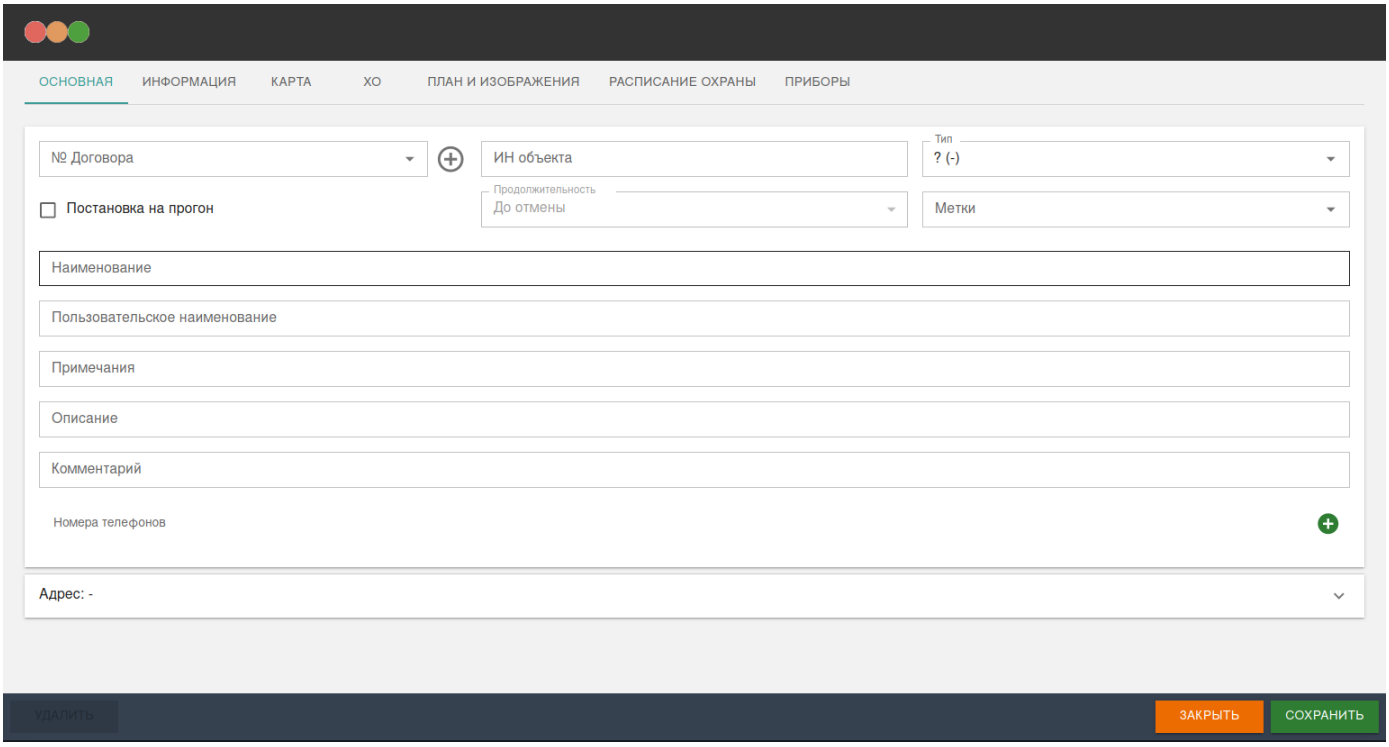


Рис. 35 Добавление объекта. Вкладка «Основная»

Данная вкладка в форме предназначена для для ввода и последующего отображения в АРМ(Web-АРМ) информации по объекту, облегчающей восприятие информации по его состоянию. Если карточка объекта уже существует, то при её открытие в левом верхнем углу будет отображаться состояние объекта

- **№ Договора** - В случае, когда договор уже существует, в выпадающем списке можно выбрать договор, к которому будет прикреплён объект. Один объект может быть прикреплен только к одному договору. В случае, если договор ещё не существует его можно создать нажав на кнопку ***"Создать новый договор"***. Выбранный договор можно отредактировать нажав на кнопку ***"Редактировать договор"*** расположенную рядом с номером договора.

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

- **ИН объекта** - Индивидуальный номер объекта, назначается согласно принятой в ОО структуры. Может быть как цифровым, буквенным, так и представлять из себя комбинацию букв, цифр и символов. Как правило, объекту присваивается ИН, облегчающий понимание его специфики.
- **Тип** - тип позволяет классифицировать объекты по признаку принадлежности к определённой группе. Правами редактирования таблицы типов обладает администратор ОО. Для редактирования таблицы типов объектов Необходимо войти в раздел меню "Администрирование"→"Справочники"→Вкладка "Типы объектов". В том случае, если необходимо следить за местонахождением объекта: объекту назначается тип "Мобильный объект" или "Мобильная тревожная кнопка", а также объекту назначается прибор "Мобильное приложение ТК v2.0", либо мобильная тревожная кнопка "Юпитер-6422"("Юпитер-6423").

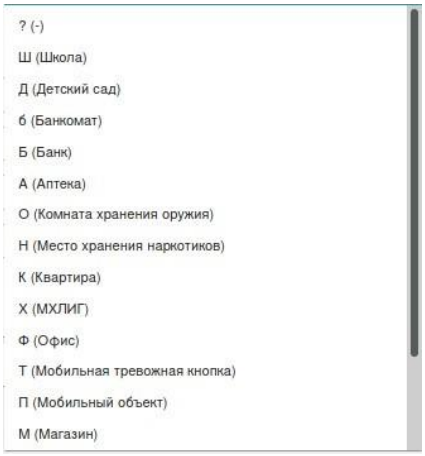


Рис. 36 Список стандартных типов объектов

- **Постановка на прогон** - позволяет поставить в режим ***Инженерного обслуживания*** весь объект. Информация с приборов будет приходить в "Ленту событий", но в окно "Тревог" события попадать не будут. После автивации этого пункта станет активым **"Продолжительность"**, где в выпадающем меню можно выбрать временной диапазон действия режима.
- **Метки** - Позволяет создать признак по которому можно объединить объекты, помимо типа. Одному объекту может быть назначено несколько меток. Если метки уже существуют, их можно выбрать из выпадающего списка.
- **Наименование** - Полное наименование объекта.
- **Пользовательское наименование** - Наименование объекта принятое для сокращения, так же можно указать местное его наименование или наименование, облегчающее понимание, местоположения или структуры объекта.
- **Примечание** - дополнительная информация, которая касается специфики объекта.
- **Описание** - описание объекта
- **Комментарий** - добавдение расширенной информации по объекту
- **Номера телефонов** - для ввода данной информации необходимо нажать на символ "Добавить" . После чего, откроется форма(рис. 37) для заполнения, где указывается:

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



Рис. 37 Форма заполнения номера телефона

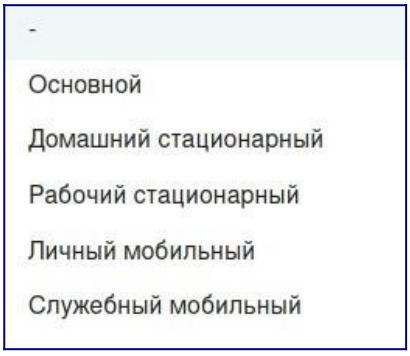


Рис. 38 Список типов номеров телефона

- **Номер телефона** - в формате - +7XXXXXXXXX, либо 8XXXXXXXXXX. Допускается использование разделителей. Необходимо учитывать, что номера телефонов "Ответственных лиц", "Договора", "Объекта" могут быть не связаны между собой.
- **Комментарий** - Информация служебного или личного характера, которая связана с данным телефонным номером. Например, время в которое можно звонить на этот номер или его территориальное расположение на объекте.
- **Тип** - Определяет специфику телефонного номера. В выпадающем списке(рис. 38) можно выбрать тип номера телефона:
  - - - тип не указан.
  - ***Основной*** - главный номер телефона для связи с ответственным.
  - ***Домашний стационарный*** - Личный номер городской телефонной линии.
  - ***Рабочий стационарный*** - Служебный/Рабочий номер городской телефонной линии.
  - ***Личный мобильный*** - Личный номер, предоставленный оператором мобильной связи.
  - ***Служебный мобильный*** - Служебный/Рабочий номер, предоставленный оператором мобильной связи.

  Если возникла необходимость в удалении записи, нажмите символ "Удалить"  и согласитесь с действием.

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

- **Адрес** - Адрес регистрации или фактического местонахождения/расположения, указанного выше субъекта. Форма для заполнения открывается при активации строки, маркер меняет форму, например . Для более точной формализации адреса, желательно указывать полный почтовый адрес(рис. 39).

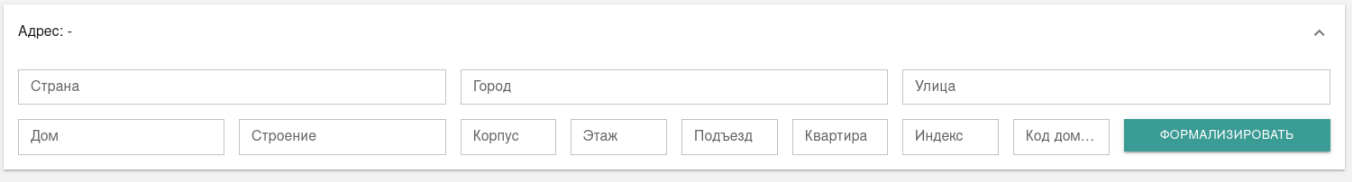


Рис. 39 Форма для заполнения адреса

Если известен и введен населенный пункт и адрес можно уточнить его данные, нажав кнопку ФОРМАЛИЗИРОВАТЬ система попытается связаться с КЛАРД и уточнить данные, связанные с указанным адресом.

6.2.1.1.2 Вкладка «Информация»

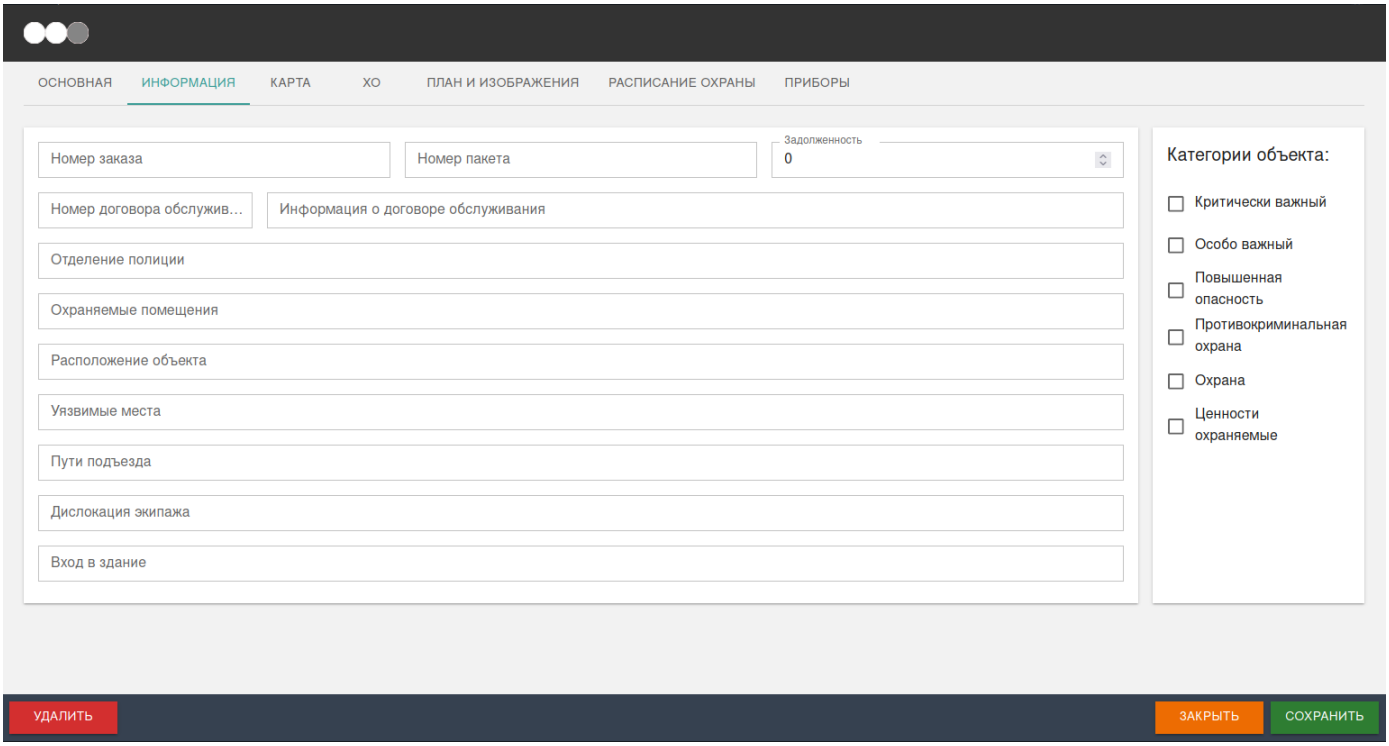


Рис. 40 Добавление объекта. Вкладка «Информация»

В данной вкладке вводится информация по обслуживающей организации, службам реагирования и критерии особой важности объекта.

- **Номер заказа** - Номер заказ-наряда по установке оборудования.

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

- **Номер пакета** - Как правило, обозначает комплектацию, устанавливаемого оборудования, определяется внутреней спецификой обслуживающей организации.
- **Задолженность** - заполняется, если на объекте есть задолженность по установке или обслуживанию.
- **Номер договора Обслуживания** - Заполняется в том случае, когда на монтаж и обслуживание оборудования составляются разные договоры.
- **Информация о договоре обслуживания** - Поле для ввода информации об обслуживающей организации и/или информации по монтажу/обслуживанию оборудования и т.п.
- **Отделение полиции** - Отделение/отдел полиции, к которому территориально относится объект.
- **Охраняемые помещения** - Так как охраняться может не весь объект, а только отдельные помещения, здесь указываются какие помещения включены в договор охраны.
- **Расположение объекта** - Описание топографической картины расположения объекта.
- **Уязвимые места** - описание мест, где не установлены оконечные устройства, либо зон не попадающих под их контроль.
- **Пути подъезда** - Описание возможных путей подъезда к объекту
- **Дислокация экипажа** - Описание маршрутов патрулирования и/или месторасположение экипажа, за которым закреплен объект, при стационарном базировании.
- **Вход в здание** - описание возможных вариантов входа в объект.

6.2.1.1.3 Вкладка «Карта»

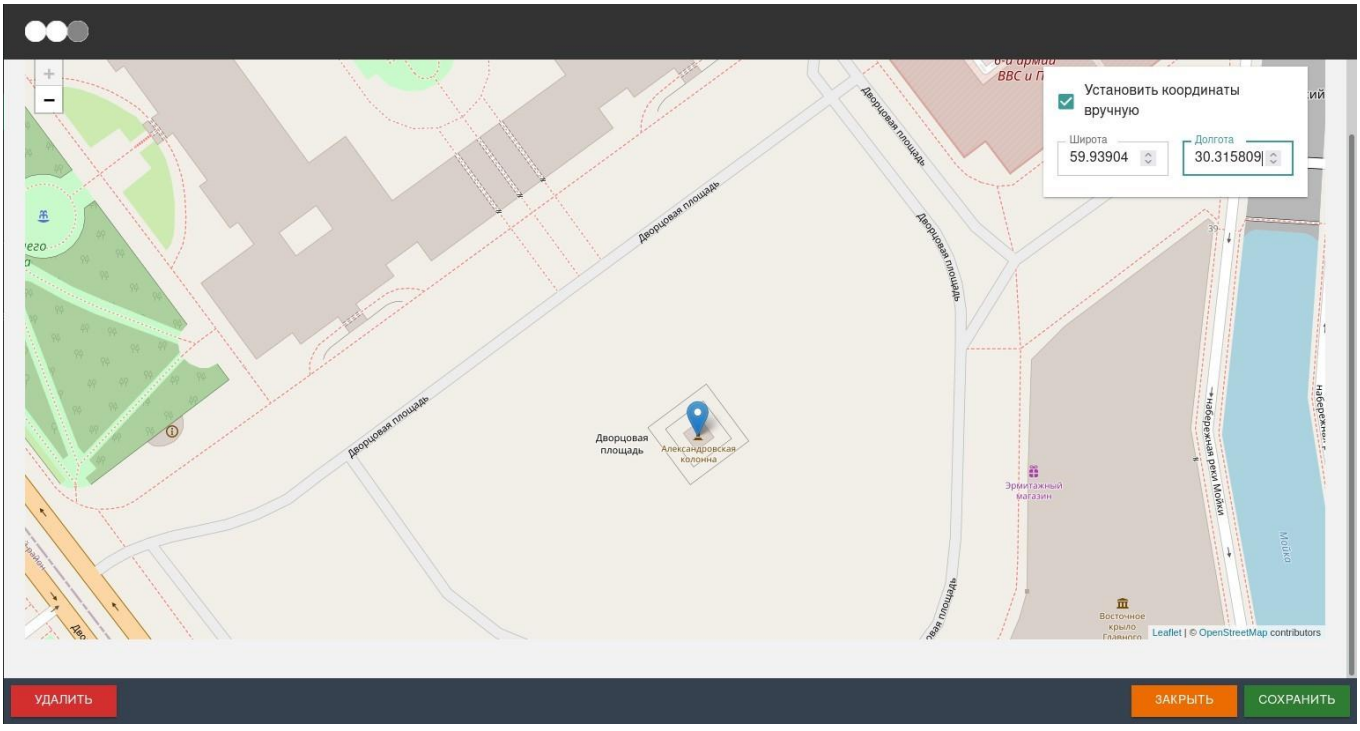


Рис. 41 Добавление объекта. Вкладка «Карта»

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

В данной вкладке показан объект, как он изображается на карте. При разработке данного функционала использовались карты разработки OpenStreetMap, а так же механизм определеня координат по адресу Leaflet

- +/- - позволяют увеличить или уменьшить масштаб карты
- **Установить координаты вручную** - Позволяет игнорировать координаты, предоставленные системой расчета координат, по почтовому адресу.
  - **Широта** и **Долгота** - Географические координаты объекта в десятичном формате. Например, объект Александровская колонна в Санкт-Петербурге, её координаты: ***59,93904° северной широты*** и ***30.31581° восточной долготы***.

При заполнении адреса объекта, во вкладке "Основная", автоматически вычисляется геопозиция объекта, что отображается в форме с географическими координатами.

6.2.1.1.3 Вкладка «ХО»

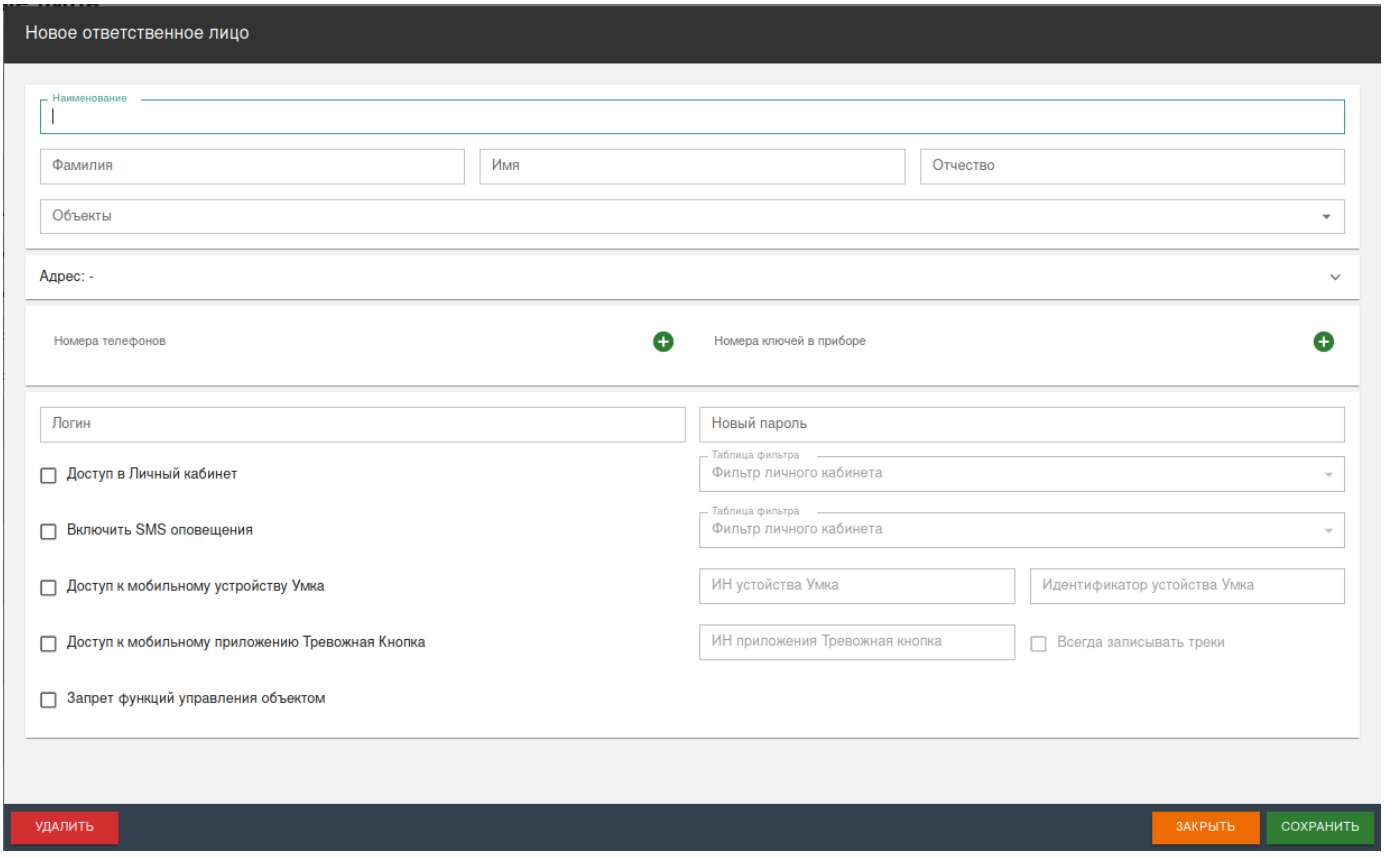


Рис. 42 Добавление объекта. Вкладка «ХО»

В данной вкладке можно ввести ответственных/делегированных лиц. При этом обратите внимание на тот момент, что ХО можно прикрепить к одному или нескольким объектам, а в договоре указывается лицо, с которым заключен договор.

- Если в договоре указано Физ.лицо, являющееся Хоз.органом, то его необходимо указать в этом списке.

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

- Если при создании записи Хоз.органа не указан объект, запись ХО удаляется. Вариант сохранения "пустого" ХО не предусмотрен.

- Для регистрации записи ХО необходимо нажать значок "Добавить" 

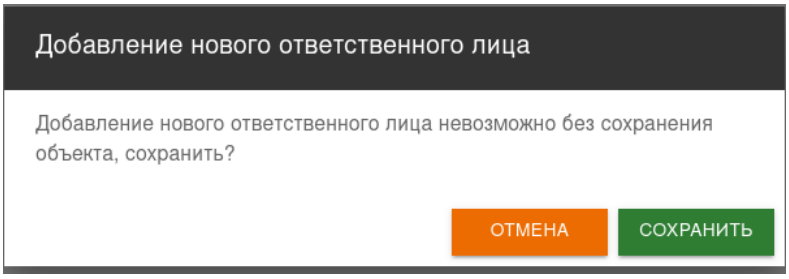


Рис. 43 Запрос на сохранение записи об ответственном лицензии

При этом если в карточке объекта были произведены какие-либо действия система выдаст предупреждение(рис. 43).

Можно закрыть окно, нажав "ОТМЕНА" и продолжить вносить изменения в другие разделы, либо нажать "СОХРАНИТЬ" и перейти к вводу информации по Хоз.органам.
Для добавления информации об ответственном лице необходимо заполнить соответствующую форму. Поля в, предлагаемой форме имеют следующие значения:

- **Наименование** - Здесь можно указать должность или информацию, связанную с персонализацией ХО.
- **Фамилия**, **Имя**, **Отчество** - ФИО лица , включенного в договор, либо имеющего доверенность, либо имеющего право на действия, связанные с охраной объекта(постановка, снятие, КТС и т.п.)
- **Объекты** - Так как в договоре может быть указано несколько объектов, а ХО может быть указан в разных договорах, при создании карточки ХО, ему можно назначить конкретный объект или несколько объектов. В выпадающем списке отображаются все доступные объекты. Нажав на один из них, можно закрепить объект за ответственным лицом. Таким образом можно указать несколько объектов. Для удаления объектов из списка необходимо нажать на кнопку удаления , расположенную справа от наименования объекта. Список объектов, прикреплённых к договору, задается во вкладке **"Объекты"**.

- **Адрес** - Адрес регистрации или фактического местонахождения/расположения, указанного выше субъекта. Форма для заполнения открывается при активации строки, маркер меняет форму, например . Для более точной формализации адреса, желательно указывать полный почтовый адрес(рис. 39).

Если известен и введен населенный пункт и адрес можно уточнить его данные, нажав кнопку 

система попытается связаться с кладром и уточнить данные, связанные с указанным адресом.

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

!!!ВНИМАНИЕ!!! Обратите особое внимание на то обстоятельство, что основным критерием уникальности **Ответственного лица**, выступает его номер телефона. Таким образом, нельзя создать разные ХО с одним номером телефона.

- **Номера телефонов** - для ввода данной информации необходимо нажать на символ "Добавить" . После чего, откроется форма для заполнения(рис. 37), где указывается:
- **Номер телефона** - в формате - +7XXXXXXXXX, либо 8XXXXXXXXXX. Допускается использование разделителей. Необходимо учитывать, что номера телефонов "Ответственных лиц", "Договора", "Объекта" могут быть не связаны между собой.
- **Комментарий** - Информация служебного или личного характера, которая связана с данным телефонным номером. Например, время в которое можно звонить на этот номер или его территориальное расположение на объекте.
- **Тип** - Определяет специфику телефонного номера(рис. 38). В выпадающем списке можно выбрать тип номера телефона:
  - - - тип не указан.
  - ***Основной*** - главный номер телефона для связи с ответственным.
  - ***Домашний стационарный*** - Личный номер городской телефонной линии.
  - ***Рабочий стационарный*** - Служебный/Рабочий номер городской телефонной линии.
  - ***Личный мобильный*** - Личный номер, предоставленный оператором мобильной связи.
  - ***Служебный мобильный*** - Служебный/Рабочий номер, предоставленный оператором мобильной связи.

Если возникла необходимость в удалении записи, нажмите символ "Удалить"  и согласитесь с действием.

На одного ответственного может быть зарегистрировано несколько номеров телефонов.

- **Номера ключей в приборе** - Как правило, у каждого ответственного за объект, в приборе есть ключи, при вводе которых объект ставится под охрану или снимается с охраны. В том случае, если указаны данные на каком приборе какой номер ключа привязан к данному ответственному лицу, дежурный или оператор на ПЦО в ленте событий может увидеть персонализированные данные. За одним ответственным может быть закреплено несколько ключей, как на одном приборе, так и на нескольких. Для добавления ключа необходимо нажать "Добавить" . В открывшейся форме необходимо заполнить, следующие поля:
  - **Прибор** - Из выпадающего списка выбрать необходимый прибор.
  - **Ключ доступа** - Указать номер ключа в приборе, закрепленный за ответственным лицом.
  - **PIN** - численный пароль, задаётся автоматически при сохранении ХО. Данный код необходим при автоматической проверке ТК. Если при записи PIN не сформирован, то это означает, что в приборе отсутствует данный ключ.

Если возникла необходимость в удалении записи, нажмите символ "Удалить"  и согласитесь с действием.

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

Дальнейшие параметры определяют доступ к системе - Данные для авторизации в мобильных приложениях - ***"Личный кабинет"*** и ***"Тревожная кнопка v 2.0"***.

Логин - Генерируется автоматически при создании записи ответственного лица, но может быть задан вручную.

- **Новый пароль** - Необходимо задать самостоятельно. Позволяет изменить пароль при утере или компроментации.
- **Доступ в Личный Кабинет** - Разрешает/Запрещает доступ пользователя к сервису "Личный кабинет".
- После активации сервиса открывается "Таблица фильтра" для Личного Кабинета, которая позволяет выбрать фильтр сообщений, что позволяет сократить трафик.
- **Включить SMS оповещения** - Разрешить отправку SMS-сообщений этому пользователю по событиям на объектах, включенных в договор. Данный функционал имеет смысл использовать при настроенном SMPP сервере.
- После активации сервиса открывается "Таблица фильтра" для SMS уведомлений, которая позволяет выбрать фильтр сообщений.
- **Доступ к мобильному устройству "Умка"** - Разрешает/Запрещает доступ к сервису взаимодействия с носимым GPS-трекером "Умка". При активации данного сервиса необходимо заполнить поле ***"Идентификатор мобильного устройства "Умка"***. Идентификатор устройства обычно расположен на ярлыке, с обратной стороны устройства. После этого данное устройство идентифицируется сервером КРОС как прибор, поэтому в дальнейшем все действия аналогичны операциям с обычным прибором. Инструкция по настройке GPS-трекера расположена в разделе Часы "УМКА"
- **Доступ к мобильному приложению "Тревожная Кнопка"** - Разрешает/Запрещает доступ к сервису "Тревожная кнопка". При включении этого сервиса в разделе Приборы автоматически создаётся прибор, использующий драйвер мобильного приложения. Таким образом, сервер КРОС работает с мобильным приложением, как с обычным прибором. Описание приложения расположено в разделе Мобильные приложения
  - ♦ Для корректного определения местоположения мобильного объекта, когда разрешен **Доступ к мобильному приложению "Тревожная Кнопка"** и/или **Доступ к мобильному устройству "Умка"**, рекомендуется включить параметр **Всегда записывать трек перемещения**, что позволит оперативно определить местонахождение ответственного лиц. При этом после сохранения данных в списке приборов автоматически создается прибор, связанный с приложением "Мобильная ТК" или часами "УМКА".
- **Запрет функций управления объектом** - данная опция не позволяет пользователю управлять объектом. Пользователь получает информацию в режиме мониторинга.

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

- **Инкассатор** - специальный режим, который необходимо активировать, в случае договора по охране инкассаторов. Данный атрибут указывает, что ответственное лицо является инкассатором.

При создании объекта ХО можно создать во Вкладке **ХО**. Необходимо учитывать то обстоятельство, что вводимый ХО может уже присутствовать в **списке ответственных**. В этом случае, для включения ХО в список ответственных на объекте, необходимо в списке ответственных найти необходимый ХО и в его карточке выбрть необходимый объект.

6.2.1.1.4 Вкладка «План и Изображения»

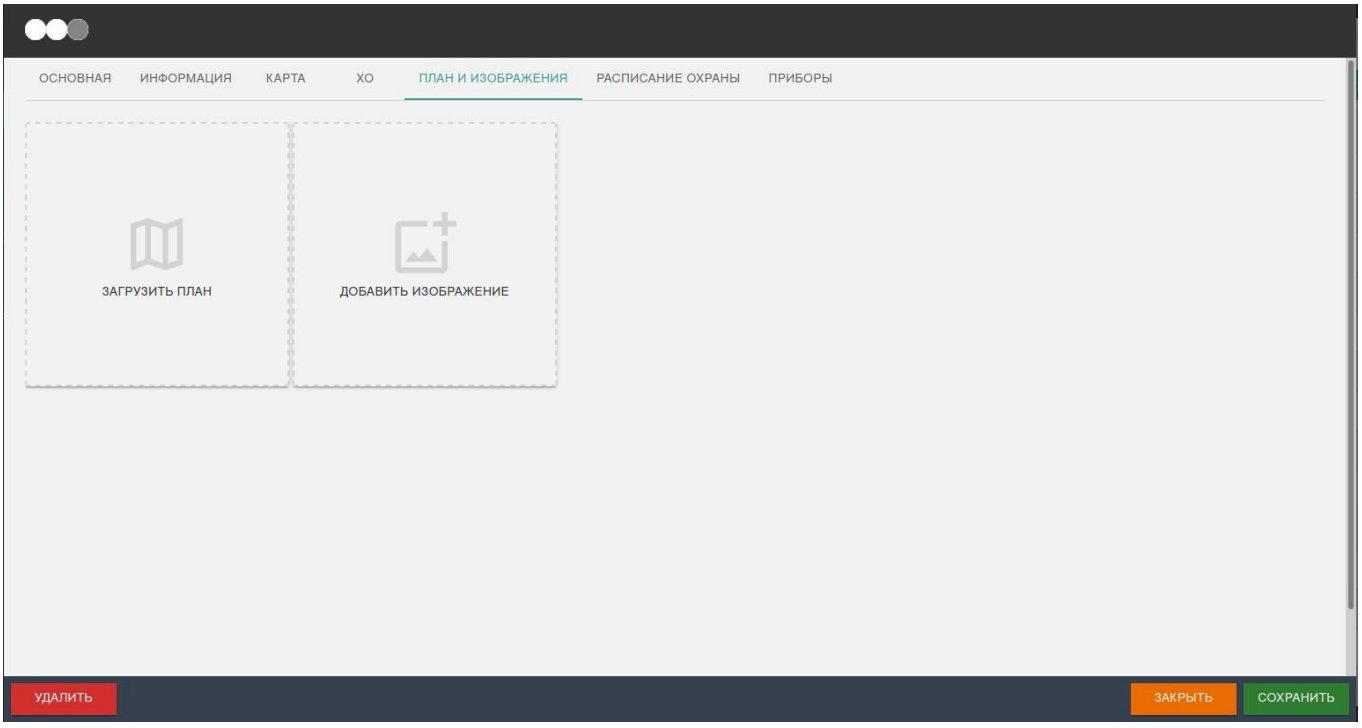


Рис. 42 Добавление объекта. Вкладка «План и Изображения»

!!!ВНИМАНИЕ!!! Для оптимизации скорости отображения изображений и воизбежание ошибок отображения, настоятельно рекомендуем не использовать файлы формата - PDF, BMP, CDR, PPD и им подобные. Для оптимальной работы рекомендуется использовать файлы с расширением - JPG, JPEG, PNG, SVG и размером, желательно, не более 3 Мбайт

Для уточнения данных по объекту можно ввести графическую информацию:

- **План объекта** - Отсканированное изображение плана или чертежа объекта, так же здесь может быть размещен план с отметками расположения прибора и датчиков. Для загрузки плана необходимо нажать на иконку с надписью **"ЗАГРУЗИТЬ ПЛАН"** и выбрать файл, отвечающий требованием плана.

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

- **Изображение обекта** - Позволяет загрузить изображения объекта, а так же любую дополнительную графическую информацию по объекту. Для загрузки файла необходимо нажать на иконку с надписью **"ДОБАВИТЬ ИЗОБРАЖЕНИЕ"** и выбрать необходимый файл.

После того, как будут загружены все необходимые изображения внешний вид закладки будеть выглядеть примерно так

Если необходимо удалить изображение, нужно нажать значок "Удалить" 

6.2.1.1.4 Вкладка «Расписание охраны»

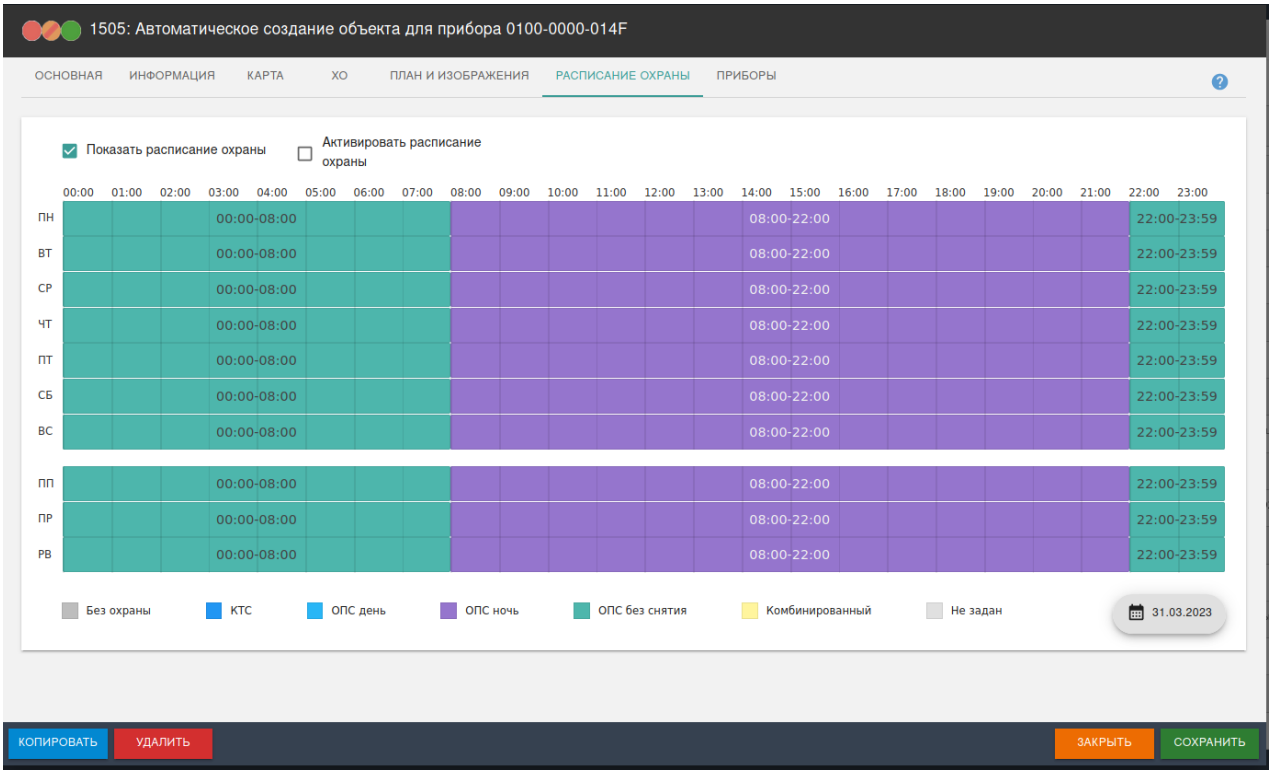


Рис. 43 Добавление объекта. Вкладка «Расписание охраны»

Расписание создается для контроля взаимодействия ОП и объекта. После создания расписания оператор или дежурный может проверить, обслуживается ли данный объект в этот временной интервал или нет и в каком режиме(рис. 43).

При составлении расписания используются следующие режимы охраны:

- **Не задан** - режим охраны не определен. Строго говоря, не является режимом охраны, а лишь показателем отсутствия остальных режимов. Появляется при первоначальном включении расписания охраны и при удалении какого-либо режима. При попытке сохранения карточки объекта все интервалы с режимом "не задан" будут превращены в интервалы "без охраны".
- **Без охраны** - Временной интервал, исключенный из времени охраны. Тревоги приходящие в это время отображаются в "Ленте событий", но обрабатываются частично, например, если разрешено генерирование тревоги по потере связи, то это сообщение появится в окне тревог.

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

- **КТС** - Указывается временной интервал в течении которого обрабатывается состояние **К**нопки **Т**ревожной **С**игнализации. Если в расписании не указано - КТС, то в этом случае тревоги могут не обрабатываться. Если этот режим назначен, то тревожные сообщения будут обрабатываться без задержки.
- **ОПС День** - Обслуживание **О**хранно-**П**ожарной **С**игнализации по тарифу **"День"**. Это 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** - Обслуживание **О**хранно-**П**ожарной **С**игнализации по тарифу **"Ночь"**. При этом режиме, 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** - Обслуживание **О**хранно-**П**ожарной **С**игнализации по тарифу **"Без снятия"**, постоянная охрана без **КТС**. Это режим, во время которого тревожные сообщения будут обрабатываться без задержки, а постановка объекта на охрану проводится с отсчетом времени на выход.
- **Комбинированный** - Переходный режим, используется при смене режимов охраны, когда временные рамки перехода из одного режима охраны в другой жёстко определить невозможно. Например, примерное время прихода ХО на объект или переход из **ОПС Ночь** в режим **КТС** можно обозначить как раз этим режимом. Поведение объекта в течение этого режима будет таким же как поведение объекта без включенного расписания охраны.

- **Показать расписание охраны** - Если не активировать данный параметр,то расписание на объекте будет не доступно. Для редактирования расписания необходимо выбрать данный пункт. При этом откроется график охраны со значениями по умолчанию и режим специальной отметки.

  - **Активировать расписание охраны**- параметр доступен при включеннном параметре **Показать расписание охраны** и переводит расписание охраны в активный режим.
    - **Уехали до** - при активации данного пункта будет доступен режим ввода даты, после её ввода посередине графика охраны появится информационное сообщение формата: **УЕХАЛИ ДО HH:MM DD.MM.YYYY**. При этом на пульт будут поступать все тревожные сообщения, вне зависимости от того взят объект под охрану по расписанию или снят с охраны по расписанию. Использование данного функционала определяется условиями договора. Данный параметр доступен после выбора **Активировать расписание охраны**.
    - **Копировать расписание для объектов** - Позволяет назначить одинаковое расписание охраны нескольким объектам. Выбор объектов производится из ниспадающего списка.

При активации расписания охраны предлагается график по умолчанию, однако, его можно изменить. Для изменения графика расписания, необходимо выбрать день и войти в режим редактирования, нажав левую клавишу "мышки"(для левшей правую)(рис. 44). Текущий график охраны можно распространить на несколько дней:

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

- **ПН** - Понедельник
- **ВТ** - Вторник
- **СР** - Среда
- **ЧТ** - Четверг
- **ПТ** - Пятница
- **СБ** - Суббота
- **ВС** - Воскресенье
- **ПП** - Предпраздничный день
- **ПР** - Праздничный день
- **РВ** - Рабочий выходной день

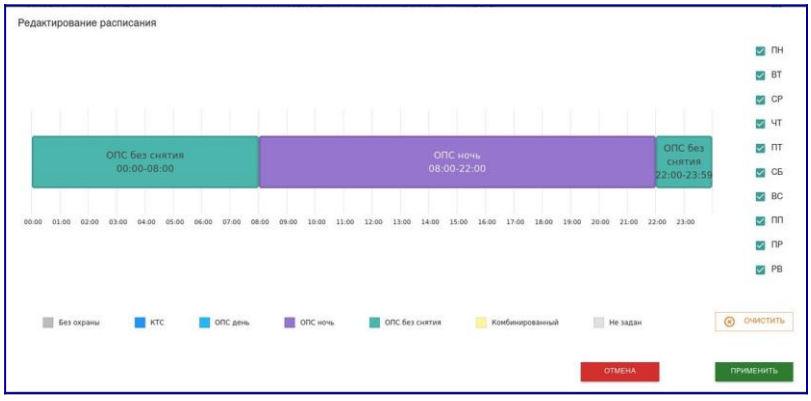


Рис. 44 Редактирование режимов временных интервалов

Для активации расписания по определенным дням необходимо установить/снять отметки на необходимых днях(список дней расположен справа в форме редактирования расписания).

Для настройки списка ***предпраздничных***, ***праздничных*** и ***рабочих выходных*** дней необходимо отредактировать . "Календарь".

Перед созданием своего временного интервала, можно удалить уже установленный, для этого необходимо нажать кнопку "Очистить" 

. После очистки расписания можно задать новое.

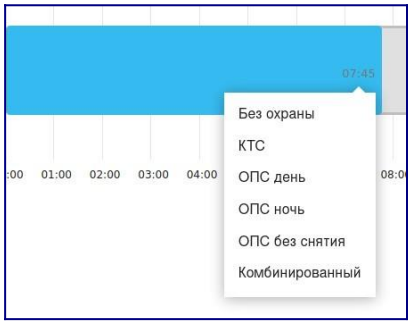


Рис. 45 Список режимов охраны

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

При создании нового расписания, необходимо подвести указатель "мыши" к левому краю временного диапазона и, нажав левую клавишу(для левшей правую) "зацепить" край временного диапазона, переместить его до времени окончания его действия. После чего откроется список выбора режима охраны. В открывшемся списке, необходимо выбрать режим охраны(рис. 45), соответствующий временному интервалу, описанному в договоре. После этого можно перейти к созданию следующего временного интервала. При создании последнего временного интервала охраны, с окончанием в "23:59", по факту временой диапазон действует до 24:00, не следует

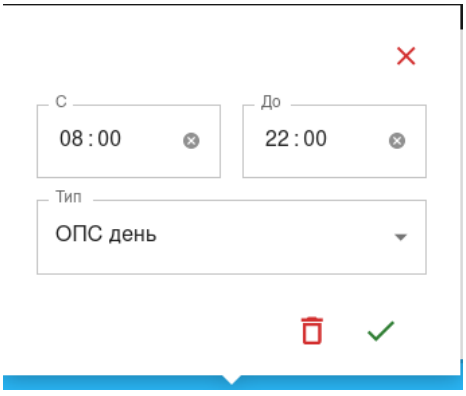


Рис. 46 Форма редактирования временного интервала и типа охраны

Каждый временной интервал можно отредактировать, нажав на него. При этом откроется форма редактирования временного интервала и режима охраны. После окончания редактирования, необходимо принять изменения, нажав на кнопку "Подтвердить" , либо закрыть форму редактирования диапазона без изменения, нажав "Закрыть" . Так же, можно удалить временной интервал, нажав кнопку "Удаления" . После удаления, временной диапазон получит статус охраны - **"Не задан"**.

Создать новый временной интервал можно так же, как и при создании нового расписания, даже если новый диапазон создается между уже существующих.

В настройках расписания предусмотрена возможность корректировки выходных и праздничных дней.

Все объекты наследуют календарь из настроен календаря, выполненных в карточке ОО и эти данные изменить нельзя. Имеется возможность изменить значение только тех дней, которые не отредактированы в календаре ОО.

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

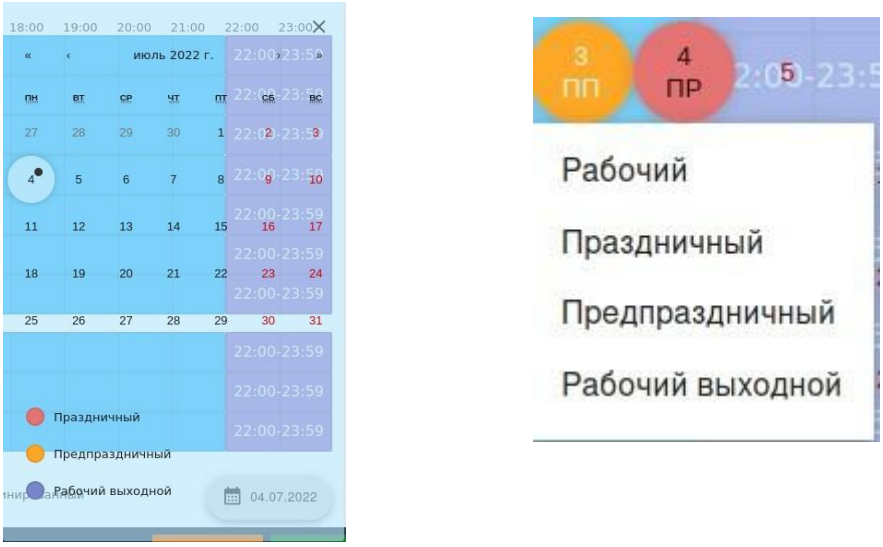


Рис. 47 Календарь и значения дней для корректировки

Для редактирования календаря необходимо его открыть, нажав на символ . Текущая дата отмечена кругом голубого цвета и точкой "•"(рис. 47).

Используя символы "‹" и "›", можно переключаться между месяцами, а при нажатии на символы "«" и "»", появляется возможность сменить год. При нажатии на название месяца, откроется список месяцев, где можно сделать необходимый выбор. При двойном клике на значении года, можно сделать выбор определенного значения в диапазоне.

При выборе определённой даты открывается возможность назначить этот день: Рабочим, Праздничным, Предпраздничным или Рабочим выходным. Для визуализации используются цветовые обозначения.

6.2.1.1.5 Вкладка «Приборы»

Во вкладке "Приборы" отображаются приборы не прикреплённые к объектам, а также виртуальные приборы, связанные с приложением "Мобильная Тревожная кнопка". Таким образом, здесь можно отметить прибор или приборы, которые находятся в "Инженерном режиме", и их можно закрепить за объектом. Если есть необходимость в переназначении прибора другому объекту, вначале его необходимо исключить из объекта, сняв отметку, а затем зайти в учётную карточку необходимого объекта и отметить нужный прибор в данной вкладке. Если необходимо откорректировать информацию связанную с прибором, то в этом случае необходимо нажать кнопку "Редактировать" , расположенную справа от наименования прибора(рис. 48).

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

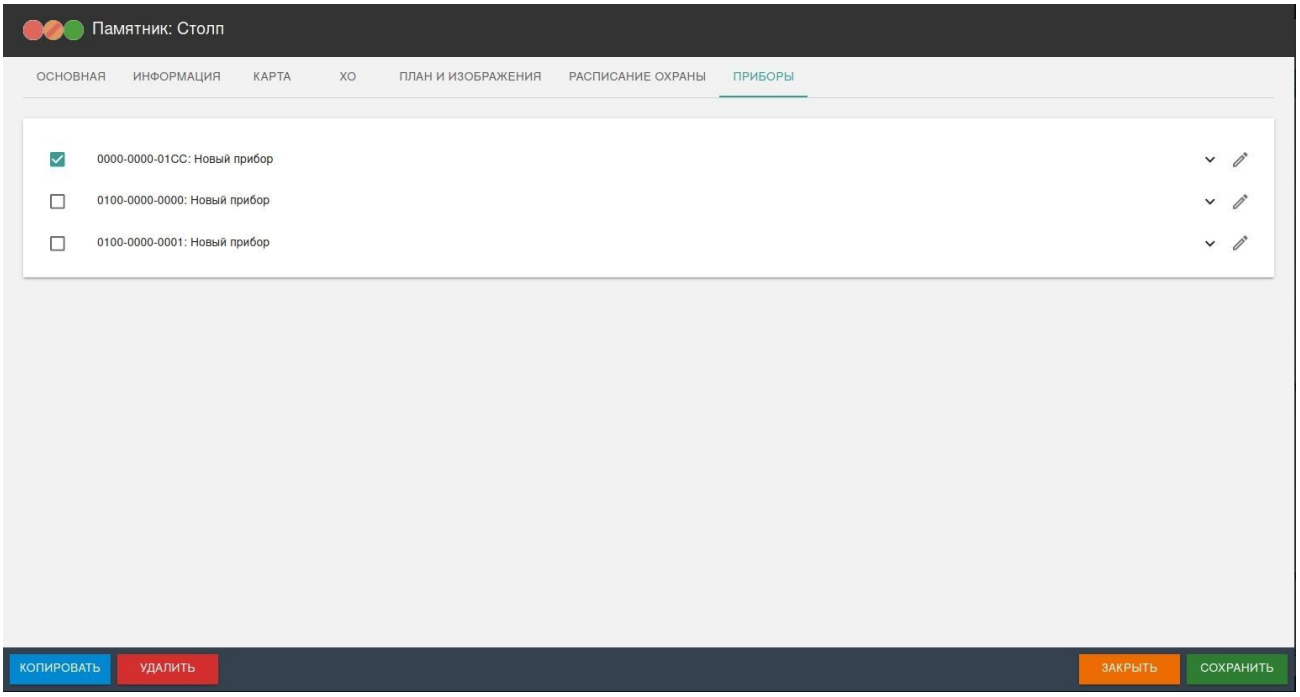


Рис. 48 Добавление объекта. Вкладка «Приборы»

При активации записи прибора, раскрывается его структура, где отображаются все разделы. В открывщейся структуре, появляется возможность "привязать" к объекту не весь прибор, а его конкретный раздел. Это позволяет экономить приборы и использовать один прибор, когда, например, в одном здании находятся несколько организаций(юридических или физических лиц) и с каждым заключен договор на охрану, тогда за каждым субъектом закрепляется отдельный раздел, при этом прибор конфигурируется соответственным образом.

6.2.1.2 Сохранение, редактирование и удаление данных карточки объекта

Для сохранения введённой информации по объекту необходимо нажать кнопку "Сохранить" 

. Если корректировка данных по объекту не производилась или нет необходимости сохранять измененные данные, то в этом случае нажмите "Закрыть" 

.

Если в каких-либо полях производились действия, то в этом случа ПО выдаст предупреждение. В этом случае, необходимо подтвердить изменения или отказаться от них.

Для удаления карточки объекта нажмите кнопку "Удалить" 

.

ХО, указанные в объекте, после удаления объекта, так же будут удалены, если только они не указаны в других объектах.

Иногда возникает необходимость в создании объекта с аналогичными данными в этом случае можно воспользоваться кнопкой "Копировать" 

. В этом случае в списке объектов появится запись идентичная текущей, но с цифровым "ИН", а так же без изображений и "прикрепленных" приборов.

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

6.2.2 Групповые операции с объектами охраны

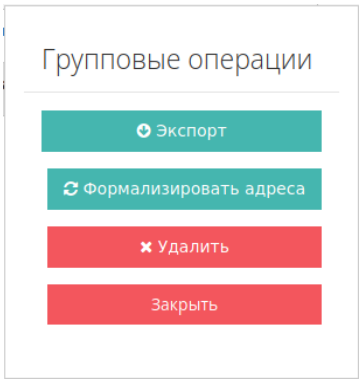


Рис. 49 Возможные варианты групповых операций с объектами

Для обработки однотипных операций предусмотрен режим "Групповые операции"(рис. 49). Перед их выполнением необходимо выбрать один или несколько объектов, после чего нажать кнопку 

.

- **Экспорт** - позволяет экспортировать, связанную с объектом или объектами, информацию в файл формата "xml", для переноса на другой сервер или для обработки другими программами.
- **Формализировать адреса** - Процедура уточнения адресов объектов по введённому почтовому адресу, вычисление почтового индекса, а также географических координат объекта или объектов.
- **Удалить** - Удаление выбранных объектов.
- **Закрыть** - Завершить работу с групповыми операциями.

В случае когда необходимо обработать данные, перенесённые из "Юпитер-7", например объединить ключи одного объекта, необходимо в "Фильтре объектов" выбрать ***"Импортированные объекты"***. В таблице объектов будут отображены только объекты, переведенные из "Юпитер-7". После этого необходимо отметить объекты требующие объединения и нажать кнопку "Групповые операции" 

. В открывшейся форме появится дополнительный пункт - **"Объединить объекты"**. После выбора этой операции, откроется форма в которой надо выбрать тот объект, который будет считаться основным и "Сохранить" изменения. После этой операции все, выбранные записи по объекту, объединятся и, открыв карточку объекта, можно изменять и дополнять записи по объекту в новом формате.

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

6.3 Приборы

Чтобы попасть в раздел управления приборами, необходимо осуществить переход **Меню «Клиенты»→«Приборы»**.

Изначально, доступ к таблице приборов(рис. 50) имеют пользователи с ролью **"Администратор"** и **"Инженер"**. Так же могут быть назначены пользователи, которым разрешен только просмотр настроек приборов, например, **"Менеджер"** или **"Оператор"**.

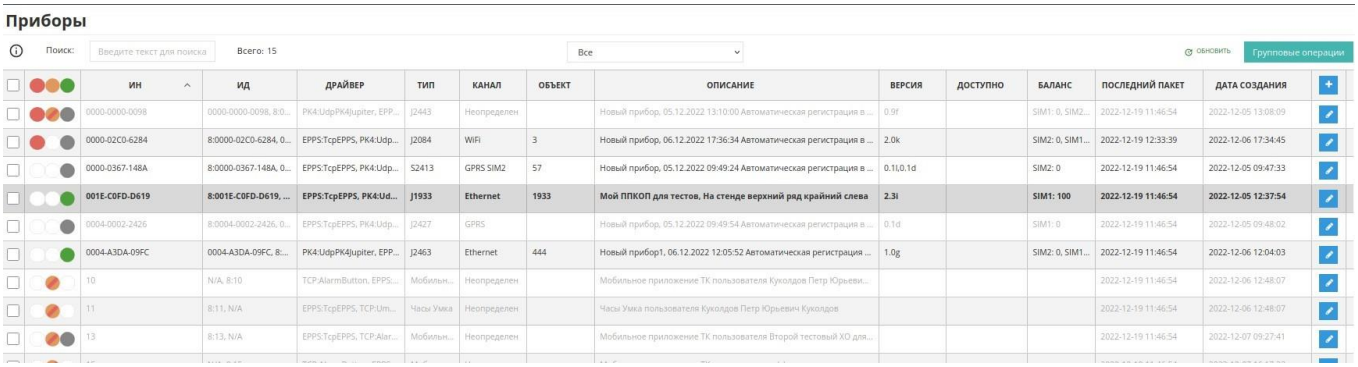


Рис. 50 Таблица состояния приборов

 - При наведении на данное изображение появляется расшифровка **Цветового обозначения** записей(рис. 51), связанных с приборами.



Рис. 51 Цветовые обозначения записей приборов

- **Поиск** - Поиск приборов по известной информации.
- **Всего** - Отображается общее количество приборов, в не зависимости от их состояния
- **Фильтр состояния приборов** - Позволяет выбрать приборы согласно их состояния(рис. 52).

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

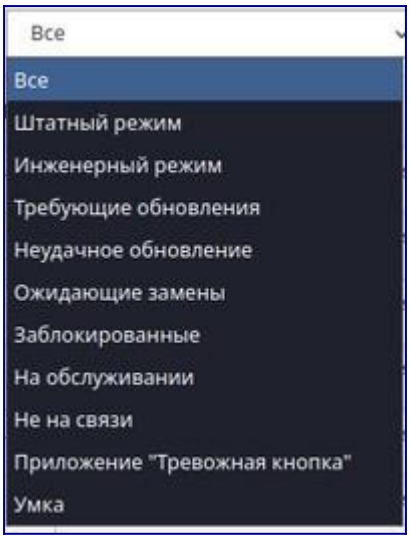
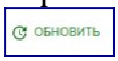


Рис. 52 Фильтр состояния приборов

- **Все** - Выставляется по-умолчанию. Отображает все приборы, вне зависимости 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.
- **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.
- **Требующие обновления** - В таблице выводятся только те приборы, для которых доступна новая версия прошивки. Проверка прошивки приборов возможна в том случае, если настроен локальный репозиторий на сервере КРОС или проверка осуществляется на сайте призводителя(локальный репозиторий отключен), при условии, что в приборе разрешена проверка наличия новой прошивки.
- **Неудачное обновление** - Позволяет отобразить приборы у которых не удалось обновить ПО.
- **Ожидающие замены** - Отображаются приборы заблокированные по признаку "Подмена". Данный признак формируется, когда некоемому прибору задаются параметры идентичные параметрам, ранее установленного, прибору, но его идентификатор не соответствует идентификатору зафиксированному ранее. В этом случае требуется решение **Администратора** ОП или **Инженера** - **Разрешить замену**.
- **Заблокированные** - В список попадут только те приборы, у которых выставлен параметр ***"Блокировка работы прибора (запрет на подключение)"***.
- **На обслуживании** - Отображаются приборы, находящиеся на "Техническом обслуживании", выставлен параметр ***"Постановка на прогон"***.
- **Не на связи** - Список приборов с ошибкой канала связи или не имеющие соединение с сервером.
- **Приложение "Тревожная кнопка"** - Позволяет выбрать только те приборы, которые ассоциированы с мобильным приложением "Тревожная кнопка".

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

- ♦ **Умка** - Отображаются приборы ассоциированные с GPS-текером "УМКА".

- **Обновить** - 

- Сделать принудительное обновление текущей информации по состоянию приборов. Необходимо учитывать, что в таблице отображается состояние приборов на момент открытия страницы. Обновление состояний происходит достаточно медленно, поэтому для ускорения процесса обновления информации можно воспользоваться данной кнопкой.
- **Групповые операции** - Однотипные операции, выполняемые над одним и более приборами.

Описание полей в таблице приборов(рис. 50):

-  - Позволяет выделить все приборы или отдельные, построчно, для выполнения групповых операций.

-  - Отображает статус объекта/прибора(*Состояние тревоги, Состояние неисправности, Состояние охраны*):
  - ♦  - Тревога
  - ♦  - Ошибка канала связи
  - ♦  - Неисправное состояние
  - ♦  - Переход на резервный канал связи
  - ♦  - Объект/Прибор взят под охрану
  - ♦  - Объект/Прибор частично взят под охрану
  - ♦  - Объект/Прибор снят с охраны
  - ♦  - Статус не определен, ошибки и тревожные состояния отсутствуют.
- **ИН** - Индивидуальное наименование прибора, принятое в рамках ОП, для облегчения восприятия информации.
- **ИД** - Идентификатор прибора. Необходимо учитывать, что при конфигурировании прибора, в ряде моделей, имеется возможность самостоятельно устанавливать значение идентификатора. При этом необходимо обратить внимание на то что в рамках действия одного сервера, особенно при базировании нескольких ОО на одном сервере, **ИД** приборов должны быть строго индивидуальны.
- **ДРАЙВЕР** - наличие драйверов определяет каналы передачи информации.
- **ТИП** - Отображает тип/модель прибора в соответствии с ПО, установленным в приборе(или согласно таблице совместимости ПО). Например, прибор ***Юпитер 4IP/GPRS***, после обновления ПО, может отображаться, как ***J2443***.
- **КАНАЛ** - Отображает основной канал связи на момент подключения прибора.
- **ОБЪЕКТ** - Объект, к которому прикреплён прибор.
- **ОПИСАНИЕ** - Поле для описания прибора. Необходимая краткая информация по прибору, например, место монтажа на объекте.

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

- **ВЕРСИЯ** - Версия, установленного на приборе ПО.
- **ДОСТУПНО** - Версия ПО, доступного для обновления на приборе. Иногда встречаются ситуации, когда в репозитории версию ПО ещё не обновили, а на приборе уже установлено ПО, версии более старшей. В этой ситуации менять прошивку на более раньюю **не рекомендуется**.
- **БАЛАНС** - Отображается состояние баланса на СИМ-картах операторов сотовой связи, установленных в приборах. Данный функционал работает в том случае, если он поддерживается ПО прибора. Чаще всего встречается ситуация, когда после задания минимума баланса, при конфигурации прибора, прибор присылает сообщения - "баланс в норме" или "недостаточно средств".
- **ПОСЛЕДНИЙ ПАКЕТ** - Дата и время получения последнего пакета информации от прибора.
- **ДАТА СОЗДАНИЯ** - Дата регистрации прибора в системе.
-  - Добавить прибор в ручную.
-  - Редактировать карточку прибора.

6.3.1 Учётная карточка прибора. Регистрация прибора в ручном режиме

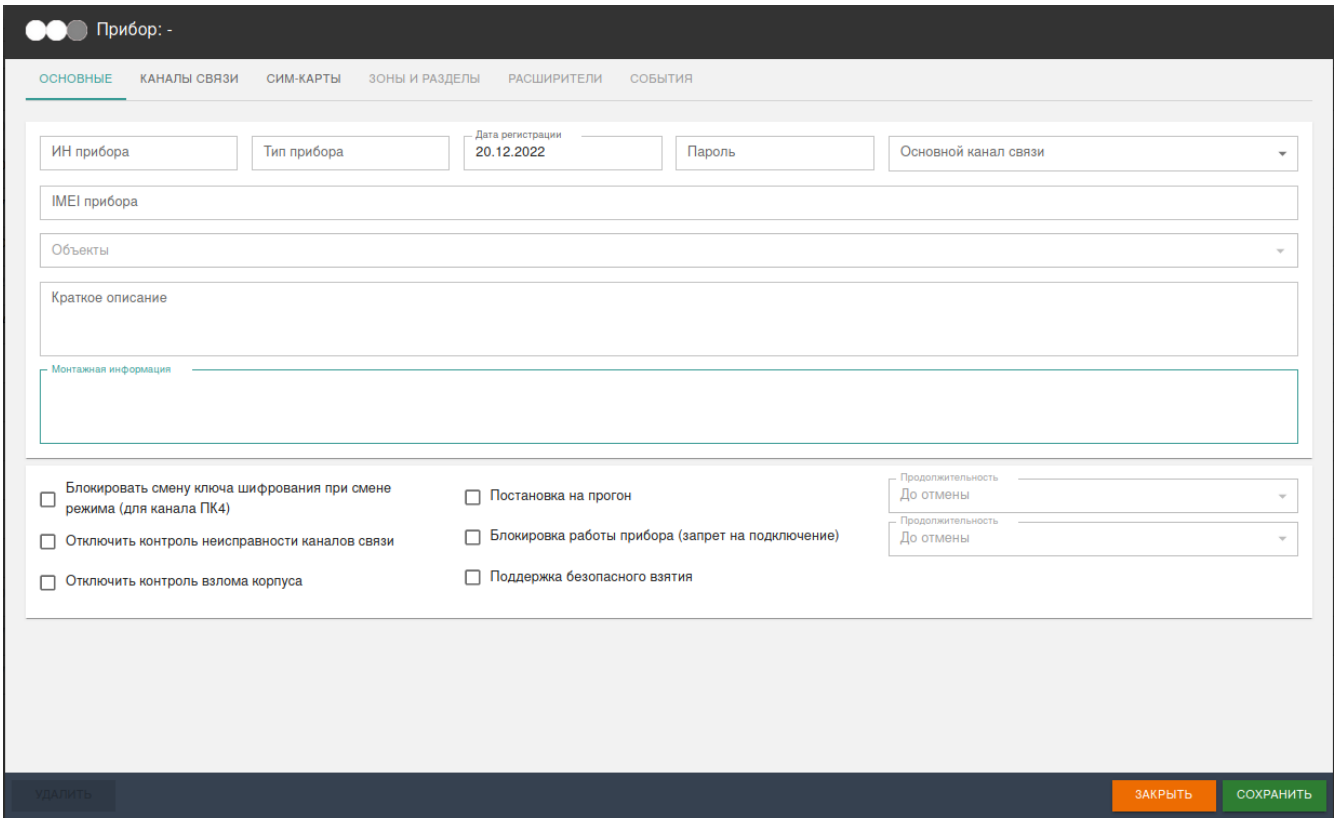


Рис. 53 Форма для регистрации прибора в ручном режиме

Для ввода информации в ручном режиме необходимо открыть карточку прибора, нажав кнопку "Добавить" (рис. 53)

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

Ручной режим - Данный режим можно использовать только в том случае если прибор был удален из БД и возникла необходимость вернуть его в работу, но при этом с прибором нет физического контакта, но есть все необходимые данные для его подключения. Основные данные для подключения прибора ручным методом включают в себя:

- Вкладка «Основные»

- **ИН прибора** - Индивидуальное наименование прибора, принятое в рамках данной ОО. Можно не указывать и изменить позже.
- **Тип прибора** - серия прибора. Например, J2443, J1833, J2024 и т.п. Указывать не обязательно, но желательно. Эти данные должны обновиться после того, как прибор выйдет на связь и передаст в КРОС свою конфигурацию.
- **Пароль** - необходим для контроля и внесения изменений в конфигурацию приборов "Сатурн" и "Юпитер" 208х серии.
- **ИН объекта** - Идентификатор объекта, к которому был подключен прибор ранее. В карточке объекта надо будет указать прибор, после его создания или выбрать объект из предложенного списка(список будет доступен после сохранения карточки прибора).

- Вкладка «Каналы связи»

Для добавления протокола во вкладке "Каналы связи" надо нажать кнопку "Добавить"  и заполнить форму.

- Необходимо указать «Тип драйвера» - По-умолчанию приборы должны работать по протокоу ***Юритер ППКОП/УОО UDP/TCP***.
- «Идентификатор ID6» прибора - Идентификатор прибора, установленный при его настройке или определенный при подключении прибора к серверу КРОС ранее.
- «Ключ шифрования» - Устанавливается при назначении прибора объекта, что обеспечивает шифрование передачи данных между сервером КРОС и прибором.

Фактически этих данных должно хватить для подключения прибора в ручном режиме. Прочие данные в карточке прибора изменятся после его подключения и получения КРОС данных о конфигурации прибора.

6.3.2 Учётная карточка прибора. Регистрация прибора в штатном 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.

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

Для облегчения поиска приборов, требующих активации можно воспользоваться фильтром "Инженерный режим".

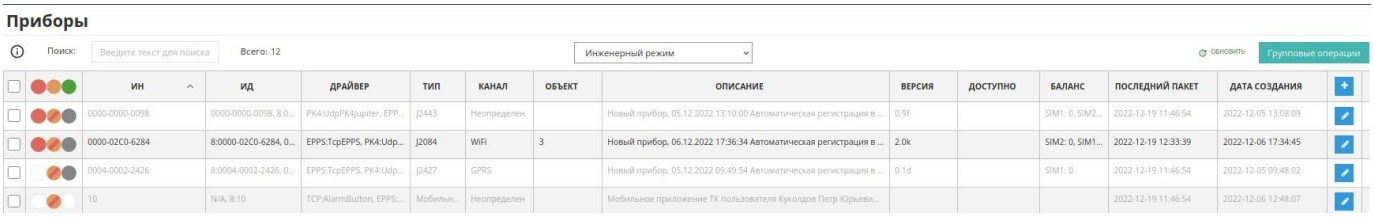


Рис. 54 Примерный вид таблицы приборов при использовании фильтра «Инженерный режим

Приборы в инженерном режиме имеют в таблице цветовую индикацию - они прописаны светло-серым цветом(рис.54). Для внесения изменений в карточку прибора необходимо перейти к режиму редактирования, нажав на кнопку "Редактировать"  Состояние прибора напрямую не связано с его карточкой, поэтому карточку можно редактировать даже если прибор взят, в тревоге или не на связи. При необходимости все связанные данные будут переданы в прибор после того как он выйдет на связь или уйдет тревожное состояние.

6.3.2.1 Вкладка «Основные»

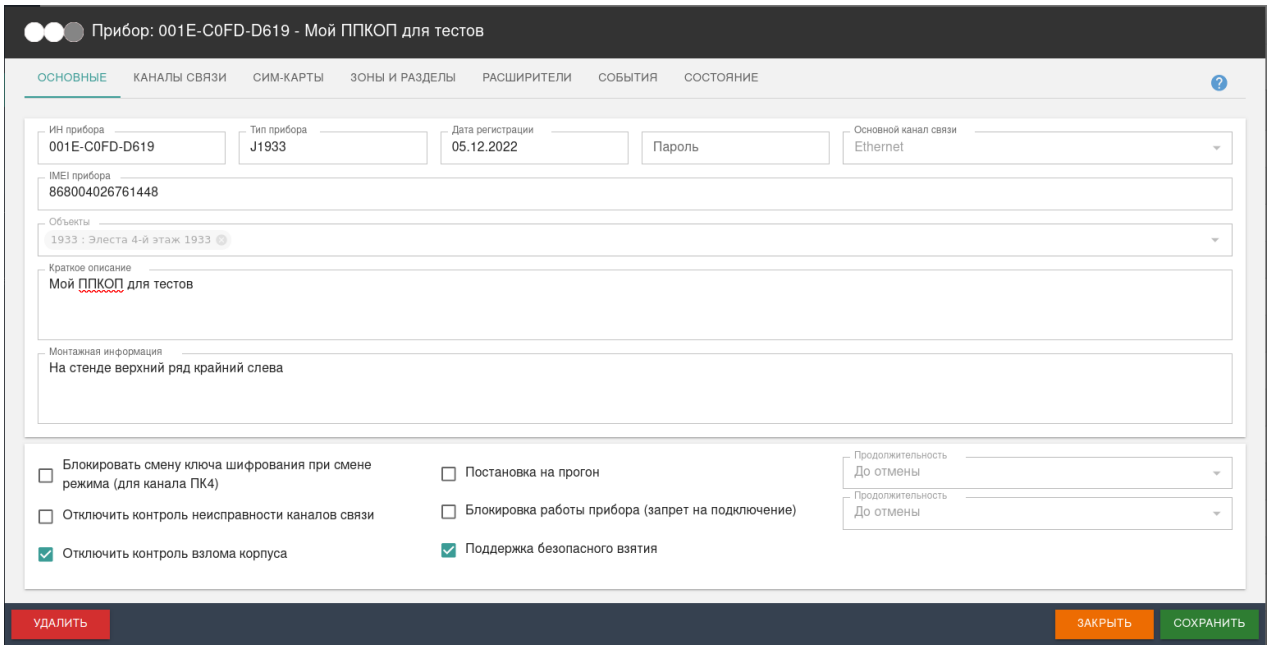


Рис. 55 Добавление прибора. Вкладка «Основные»

Основные поля данной вкладки содержат следующую информацию(рис. 55):

- **ИН прибора** - Индивидуальное наименование прибора, принятое обозначение прибора в рамках ОО, что может облегчить воспринимаемую от прибора информацию, в некоторой степени может определять индивидуальность прибора/объекта.

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

- **Тип прибора** - информация, описывающая конструктивную особенность прибора. Обычно эта информация заполняется автоматически, после того как сервер обменяется информацией с прибором и получит от него данные по конфигурации прибора.
- **Дата регистрации** - Фиксирует дату, когда прибор впервые подключился к серверу. Поле можно отредактировать.
- **Пароль** - Пароль для изменения сетевых настроек прибора. Данный пароль потребуется при прямом подключении к прибору, в том случае, если потребуется изменить сетевые настройки. При использовании удаленного конфигуратора, данный пароль не используется, так как прибор считает, что с сервером он общается по защищённому каналу.

!!!Внимание!!! В приборах "Сатурн" и радиоканальных приборах "Юпитер", при привязке прибора к объекту, генерируется пароль для изменения настроек прибора. Данный пароль необходим при переводе прибора на другие сервера.

Другие типы приборов, перед сменой IP-адресов серверов приема сообщений, необходимо перевести в инженерный режим. Для этого необходимо "отвязать" прибор от объекта.



Рис. 56 Список допустимых каналов связи

- **Основной канал связи** - определяет основной надежный канал связи, который определен в настройках прибора(рис.56). Если канал не выставлен или "Неопределен", то его можно выбрать в ручную:

  - **Неопределен** - сервер ещё не получил информацию по основному каналу связи. Так же это состояние может быть указано, если ПО прибора не передаёт эту информацию.
  - **Ethernet** - Подключение прибора по локальной сети имеющей коммутацию по проводам.
  - **GPRS** - Подключение использует каналы мобильной связи, мобильный интернет.
  - **CSD** - Канал управления по дозвону. Действия прибора определяются командами от GSM модема, которые в свою очередь зависят от того на какой номер был совершен звонок.
  - **SMS** - Канал управления прибором посредством текстовых сообщений. Может быть использован, при условии, что на приборе разрешено управление посредством SMS-сообщений.

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

- **Радиоканал** - Выставляется при условии использования радиопередающих модулей в качестве канала связи.
- **ЕППС** - Единый Протокол Передачи Сообщений. Формирует сквозную передачу данных по прибору между серверами с настроенной трансляцией в режиме "Зеркалирование". Что позволяет динамически получать информацию и управлять прибором.
- **WiFi** - Приборы, имеющие WiFi-модуль, могут передавать информацию, посредством безпроводных сетей.

- **IMEI прибора** - (англ. International Mobile Equipment Identity) - международный идентификатор мобильного оборудования — как правило это уникальный номер, предназначен для идентификации телефонов и мобильных устройств связи. Имеет либо 15 цифр в десятичном представлении, либо 16, где две последние цифры - это версия программного обеспечения мобильного устройства.
- **Объекты** - Отображает объекты к которым привязан прибор или его разделы. Включить или исключить прибор или его разделы в объект можно в разделе "Объекты" вкладка "Приборы".
- **Краткое описание** - Описание прибора, его конструктивных особенностей или иная информация требующая внимания операторов, дежурных или инженеров.
- **Монтажная информация** - Информация по монтажу и обслуживанию прибора и оконечных устройств. Так же, может быть указана информация, связанная со спецификой монтажа, необходимая для техников и ГЗ.
- **Блокировать смену ключа шифрования при смене режима (для канала ПК4)** - При отвязывании прибора от одного объекта и привязывания его к другому объекту ключ шифрования остается прежним. Так же при конвертации данных из Юпитер 7 в КРОС этот параметр устанавливается по-умолчанию, что позволяет избежать сброса ключа шифрования.
- **Отключить контроль неисправности каналов связи** - Сервер не будет передавать в протокол событий информацию о состоянии каналов связи, что при неустойчивом канале связи позволит избежать тревог по потере канала связи.
- **Отключить контроль взлома корпуса** - сервер не будет информировать оператора о тревоге по взлому корпуса. Имеет смысл использовать если датчик открытия крышки вышел из строя или присутствует, так называемый, "дребезг контактов".
- **Постановка на прогон** - Перевод прибора в "Режим обслуживания", на сервер будут доходить пакеты данных, но будут попадать только в протокол событий. Все тревожные состояния будут игнорироваться. После активации станет доступно поле "Продолжительность", что позволит установить фиксированный временной интервал действия режима. Данный режим используется при ремонте и/или отладке работы прибора, когда необходим контроль со стороны оператора пульта.
- **Блокировка работы прибора (запрет на подключение)** - Полностью блокировать информацию от прибора, прекратить передачу информации в ленту событий. Можно установить "Продолжительность" действия блокировки. Используется при, когда работа прибор требует ремонта и мешает работе операторов пульта, либо по каким-то иным причинам.

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

- **Поддержка безопасного взятия** - Если хоть один шлейф в приборе находится в тревоге или присутствует какая-либо неисправность, данный параметр позволяет избежать взятия прибора под охрану или снятия с охраны, что позволяет исключить ложные срабатывания.

6.3.1.2 Вкладка «Каналы связи»

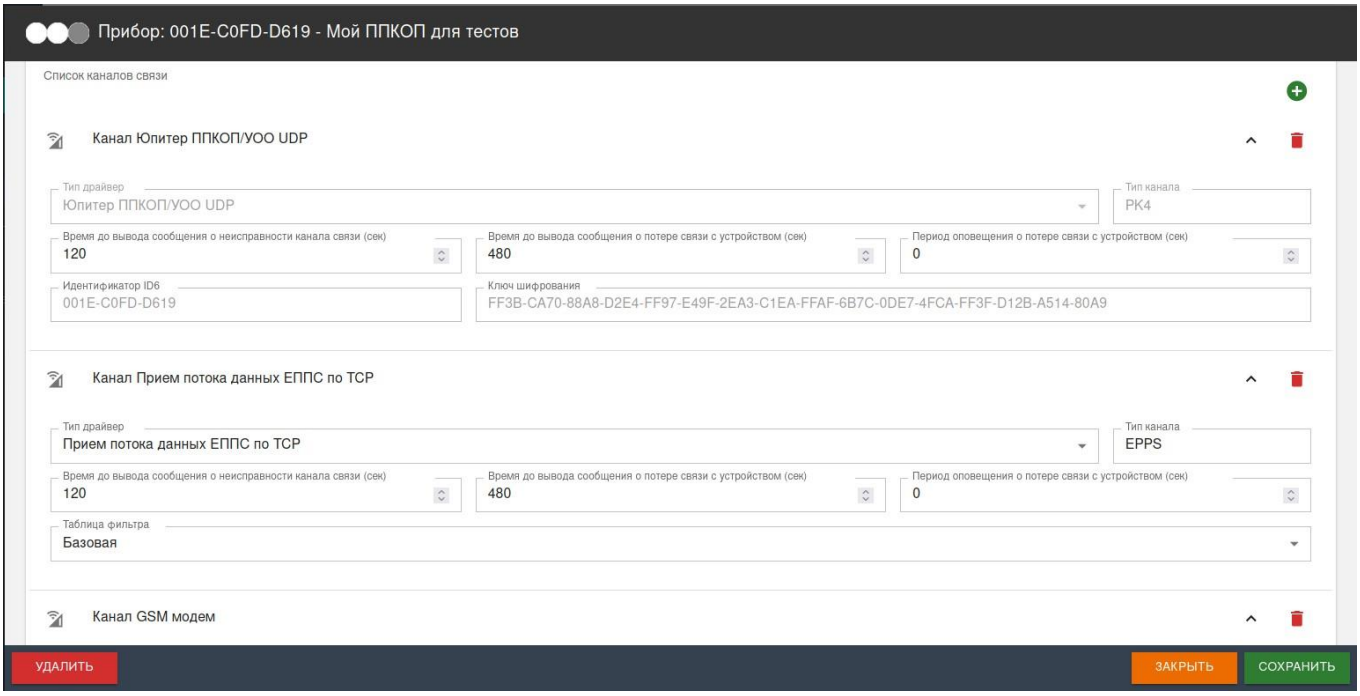


Рис. 57 Добавление прибора. Вкладка «Каналы связи»

При выходе прибора на связь в "Инженерном режиме" или после импорта данных из внешних источников в карточке прибора будут отображены каналы связи, по которым прибор может выйти на связь с сервером(рис. 57).

Для обеспечения работы каналов связи можно использовать следующие «Типы драйверов» и их настройки:

6.3.1.2.1 Канал PK4

Протокол поддерживает стандартный канал связи для приборов "Юпитер"/"Сатурн"

- **Юпитер ППКОП/УОО UDP(TCP)** - Тип **PK4** - поддержка UDP-протокола позволяет передавать информацию без проверки целостности пакетов, что значительно уменьшает время передачи. При использовании TCP-протокола увеличивается время передачи пакетов, но при этом повышается надёжность их передачи.
  - **Идентификатор ID6** - персональный идентификатор прибора в шестнадцатеричном формате. Задается либо при конфигурировании прибора, либо автоматически при подключении прибора в инженерном режиме - приборы "Сатурн" и радиоканальные приборы "Юпитер".
  - **Ключ Шифрования** - При первичном подключении прибора, в конфигураторе необходимо сбросить ключ шифрования. После привязки прибора к объекту ключ шифрования изменится. После удаления прибора из объекта ключ шифрования должен измениться на значение по-

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

умолчанию, если только в настройках прибора не установлен параметр "Блокировать смену ключа шифрования при смене режима (для канала ПК4)".

6.3.1.2.2 Канал EPPS

Канал связи формируемый на основе протокола ЕППС и предназначен для обмена информацией между серверами КРОС и "Юпитер-7".

- **Приём потока данных ЕППС по TCP** Тип **EPPS** - определяет параметры канала связи при использовании режима "Зеркалирование".
- **Приём потока данных от АРМ V7 по TCP/ЕППС** Тип **EPPS** - Определяет параметры канала связи при настройке передачи данных из "Юпитер-7".
- **Таблица фильтра** - позволяет выбрать таблицу сообщений для передачи/приёма информации.

6.3.1.2.3 Канал CID

Канал определяет соединение и прием информации по конкретному прибору из ПО сторонних производителей.

- **Приём потока данных Surgard TCP** Тип **CID** - позволяет настроить приём трансляции по протоколу Surgard от сторонних производителей.
- **Идентификатор Contact ID** - идентификатор прибора принятый в стантдарте передачи информации по протоколу Surgard.
- **Порт** - порт для канала связи, закрепленный за конкретным прибором.
- **Таблица фильтра** - позволяет выбрать таблицу соответствия сообщений между принимаемыми сообщениями и используемыми в КРОС.

6.3.1.2.4 Канал UARM

Канал приема сообщений по протоколу поддерживающему систему команд API

- **Унифицированный АРМ** Тип **UARM** - Унифицированный протокол передачи данных по API

6.3.1.2.5 Канал CSD

Канал связи поддерживающий возможность управления прибором посредством GSM-модема, установленного на ПЦО.

- **Автоматическая проверка КТС** Тип **CSD** - Система автоматической проверки реагирования КТС.
- **GSM модем** Тип **CSD** - канал управления и контроля за прибором, с использованием системы дозвона. При создании канала, автоматически, создаётся один раздел, включающий в себя одну зону.
- **Код удаленного управления** - Код для подтверждения авторизации пользователя, при удаленной настройке модема "Юпитер-7520".

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

6.3.1.2.6 Канал TCP

Протокол необходим для обеспечения подключения устройств:

- Мобильное приложение ТК(«Тревожная кнопка»)
- GPS-трекер «УМКА»

6.3.1.2.7 Настройка параметров сообщений о потере канала связи

Параметры могут настраиваться индивидуально для каждого канала связи. Сообщение формируется только в случае, если прибор не имеет соединения с сервером не по одному из каналов связи. При переключении каналов связи формируется сообщение - "Переход на резервный канал связи" или "Переход на основной канал связи".

- **Время до вывода сообщения о неисправности канала связи (сек)** - определяет интервал, через которые сервер генерирует ***сообщение*** о неисправности канала связи.
- **Время до вывода сообщения о потере связи с устройством (сек)** - определяет интервал, через который в системе бутет сгенерировано ***событие*** опотере связи с устройством
- **Период оповещения о потере связи с устройством (сек)** - определяет интервал, через который система будет отправлять событие о потере связи повторно. При указанном значении "0" сообщение будет сгенерировано единоразово.

6.3.1.2.8 Удаление канала связи

Для удаления записи канала связи необходимо нажать на кноку "Удалить" , расположенную справа от записи канала связи.

6.3.1.3 Вкладка «СИМ-карты»

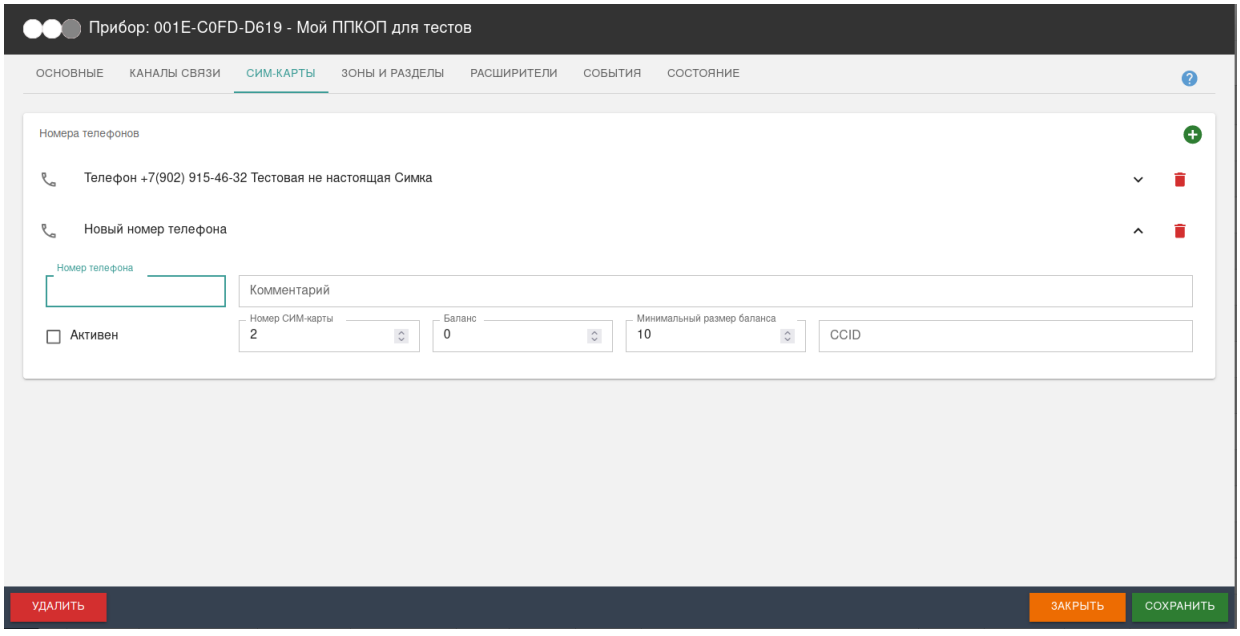


Рис. 58 Добавление прибора. Вкладка «СИМ-карты»

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

При подключении прибора информация о СИМ-картах отображается во вкладке "СИМ-Карты"(рис. 58), но также можно добавить дополнительные записи нажав кнопку "Добавить" .

В форме "Номера телефонов" предусмотрены следующие поля:

-  - В данной строке отображается информация актуальная на настоящий момент. При нажатии на строку раскрывается/скрывается ***"Форма редактирования номера телефона"***:
  - **Номер телефона** - Формат номера телефона фиксированный и записывается в формате с кодом страны - ***"+7(***) ***-**-****"***. Не пытайтесь изменить формат записи. Код страны подставляется автоматически.
  - **Комментарий** - Дополнительная информация но номеру телефона, например, оператор сотовой связи.
  - **Активен** - Показывает статус активности СИМ-карты на текущий момент. Если возникает проблема с определением основного канала передачи информации, при использовании нескольких СИМ-карт, можно выставить статус "Активен" на всех, при последующем получении конфигурации прибора, система сама должна определить, какая из СИМ-карт является основной и выставит статус "Активен" той, по которой передается информация в настоящий момент.
  - **Номер СИМ-карты** - Порядковый номер опроса СИМ-карты, определен в приборе, но можно изменить, откоррректировав порядок опроса внутри КРОС.
  - **Баланс** - Информация о состоянии баланса СИМ-карты, Информация корректируется информацией, получаемой от прибора.
  - **Минимальный размер баланса** - Состояние баланса при котором в системе начинает генерироваться сообщение, что баланс минимален.
  - **CCID** - Индивидуальный номер СИМ-карты, аналог IMEI для телефона/модема. Информация получается от прибора, поле не редактируемое.

При использовании GSM-модемов, в данный список можно внести номера телефонов ХО, с которых возможно управление прибором(поставить прибора на охрану, снять прибор с охраны, отправка тревожного сообщения).

При необходимости запись "Номера телефона" можно удалить нажав на кнопку 

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

6.3.1.4 Вкладка «Зоны и разделы»

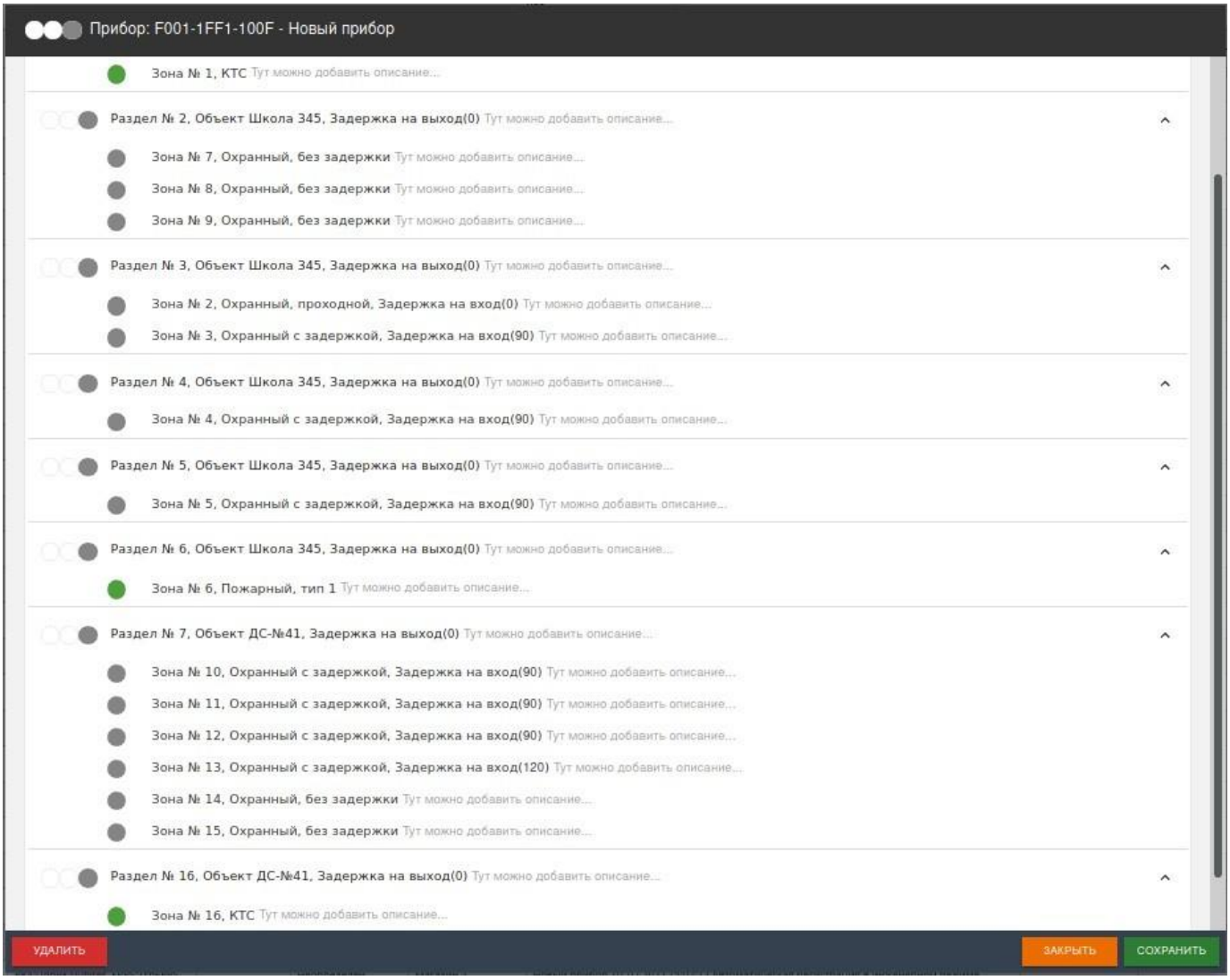


Рис. 59 Добавление прибора. Вкладка «Зоны и разделы»

Во вкладку «Зоны и разделы»(рис. 59) выводится список разделов охраны, текущее состояние раздела (взят/снят), а также ИН объекта, к которому подключен данный раздел охраны, а так же зоны, входящие в разделы и их назначение. Для того, чтобы скрыть информацию по разделу необходимо нажать на стрелочку "Вверх" . Чтобы получить доступ к подробной информации по разделу, нужно нажать стрелочку "Вниз".
Структура разделов и назначение зон задается при конфигурировании прибора. Данная вкладка позволяет осуществлять только контроль за работой разделов и зон. Вместо надписи ***"Тут можно добавить описание"*** - можно ввести описани раздела или зоны, если требуется дополнительная информация по конфигурации.

Так же предусмотрена возможность установить/снять инженерный режим зоны для её технического обслуживания. Для этого на требуемой зоне необходимо нажать правую(для левшей левую) клавишу "мыши" и выбрать необходимое действие(рис. 60).

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

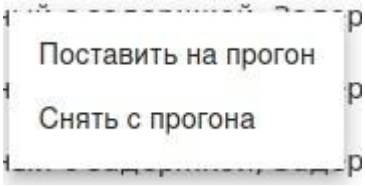


Рис. 60 Выбор режима технического обслуживания

6.3.1.5 Вкладка «Расширители»

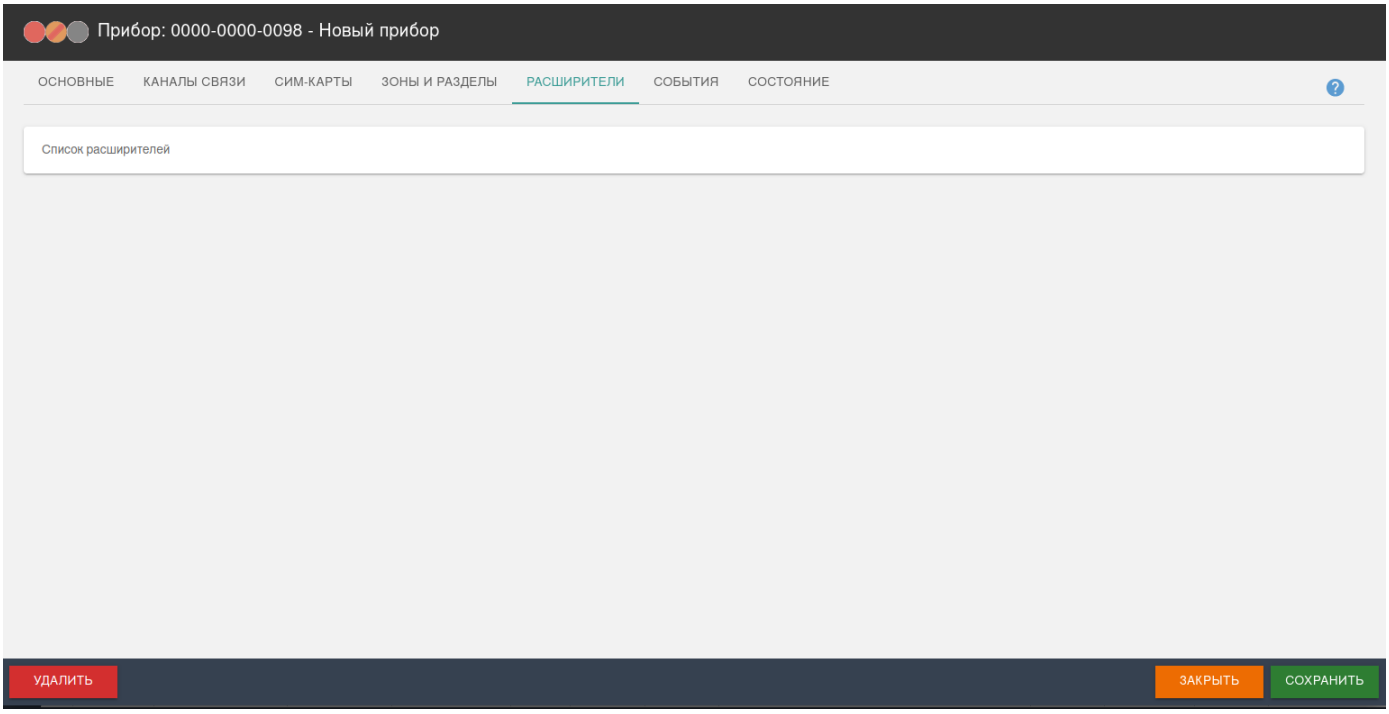


Рис. 61 Добавление прибора. Вкладка «Расширители»

При использовании Расширителей(рис. 61) в списке будут отображаться аппаратные расширители, подключенные к прибору. Список разделов и зон будет отображаться во вкладке «Зоны и разделы».

Для того, чтобы скрыть информацию по расширителю необходимо нажать на стрелочку "Вверх" . Чтобы получить подробную информацию по засширителю, нужно нажать стрелочку "Вниз" .

Здесь можно добавить краткое описание и пользовательское наименование, а также посмотреть список зон охраны данного расширителя.

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

6.3.1.6 Вкладка «События»

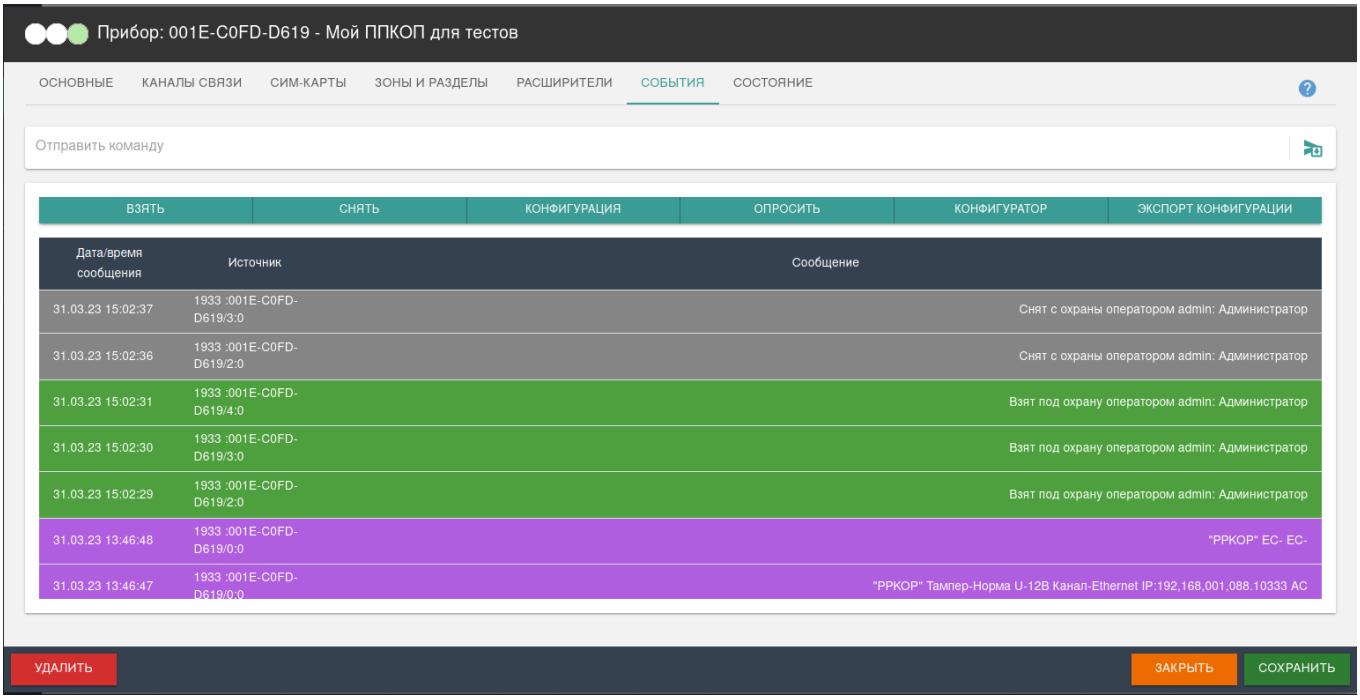


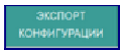
Рис. 62 Добавление прибора. Вкладка «События»

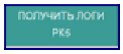
Доступ к функционалу вкладки(рис. 62) определяется ***ролью пользователя***, ***типом прибора*** и ***протоколом'***, *по которому работает прибор.*

- **Команда** - ***Отправить команду*** - Строка позволяющая отправить команду в прибор напрямую, аналогично отправке SMS-сообщения. Так как, между сервером и прибором формируется шифрованный канал, ввод пароля для удаленного управления не требуется. Список команд удаленного управления можно найти на сайте, в статье, посвященной конкретной моделе прибора. После ввода команды необходимо нажать на кнопку "Выполнить"
- ВЗЯТЬ - Позволяет отправить на прибор команду постановки на охрану всего прибора.
- СНЯТЬ - Позволяет отправить на прибор команду снятия с охраны всего прибора.
- КОНФИГУРАЦИЯ - Отправляет на прибор запрос полной копвигурации прибора.
- ОПРОСИТЬ - Отправляет на прибор запрос малой конфигурации. Как правило используется для проверки связи с прибором.
- СОСТОЯНИЕ ШЛЕЙФОВ - Отправляет команду на опрос состояния оконечных устройств, при настроенной трансляции с "Юпитер-7".
- КОНФИГУРАТОР - Загрузка модуля удаленного конфигуратора приборов. Если кнопка не активна, значит, либо прибор не поддерживает режим удаленной конфигурации, либо конфигурация прибора

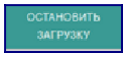
SEC.RU | Короткий путь к информации Скачано с sec.ru

загрузилась не полностью. В этом случае нужно, либо подождать пока конфигурация прибора загрузится, либо сделать запрос, нажав кнопку "Конфигурация".

- 

- Позволяет сделать запрос конфигурации прибора и сохранить её в отдельный текстовый файл.
- 

- При подключенном приборе типа "Сатурн" позволяет скопировать файлы логирования за определенную дату. В форме 

необходимо выбрать дату и время, до которого необходимы события, после чего нажать на кнопку "Выполнить" 
- 

- Остановить процесс загрузки Лог-файлов.
- 

- Загрузить все события по прибору, с момента запуска сервера, в текстовый файл.
- **Протокол событий** - Таблица предоставляет информацию о событиях по прибору, в реальном времени
- **Дата/время сообщения** - Форма сообщения: ***"День:Месяц:Год Час:Минуты:Секунды"***, что облегчает поиск сообщения по временному интервалу.
- **Источник** - Сообщение выводится в формате: ***"ИН объекта:ИН прибора/Раздел:Зона"***. Данный формат позволяет локализовать сообщения по разделам/зонам, а также определить принадлежность сообщения объектам, в том случае, когда разным объектам назначены разделы одного прибора.
- **Сообщение** - Текстовое сообщения, которое выводится согласно таблице сообщений, принятой в рамках КРОС и назначенной ОО. Для текстовых сообщений определена так же цветовая градация:
  - ♦ - Информационное сообщение.
  - ♦ ■ - Прибор на объекте снял с охраны один, несколько или все разделы. В случае снятия с охраны отдельного раздела, информация придет только по этому разделу. Прибор переходит в режим "Частично взят".
  - ♦ ■ - Прибор на объекте взял под охрану один, несколько или все разделы. В случае взятия под охрану отдельного раздела, информация придет только по этому разделу. Прибор переходит в режим "Частично взят".
  - ♦ ■ - Сообщение о тревоге или тревожном состоянии.
  - ♦ ■ - Сообщение о неисправности. Как правило - неисправен канал связи.
  - ♦ ■ - Служебная/техническая информация, предназначена для служб технических поддержки.

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

6.3.1.6 Вкладка «Состояние»

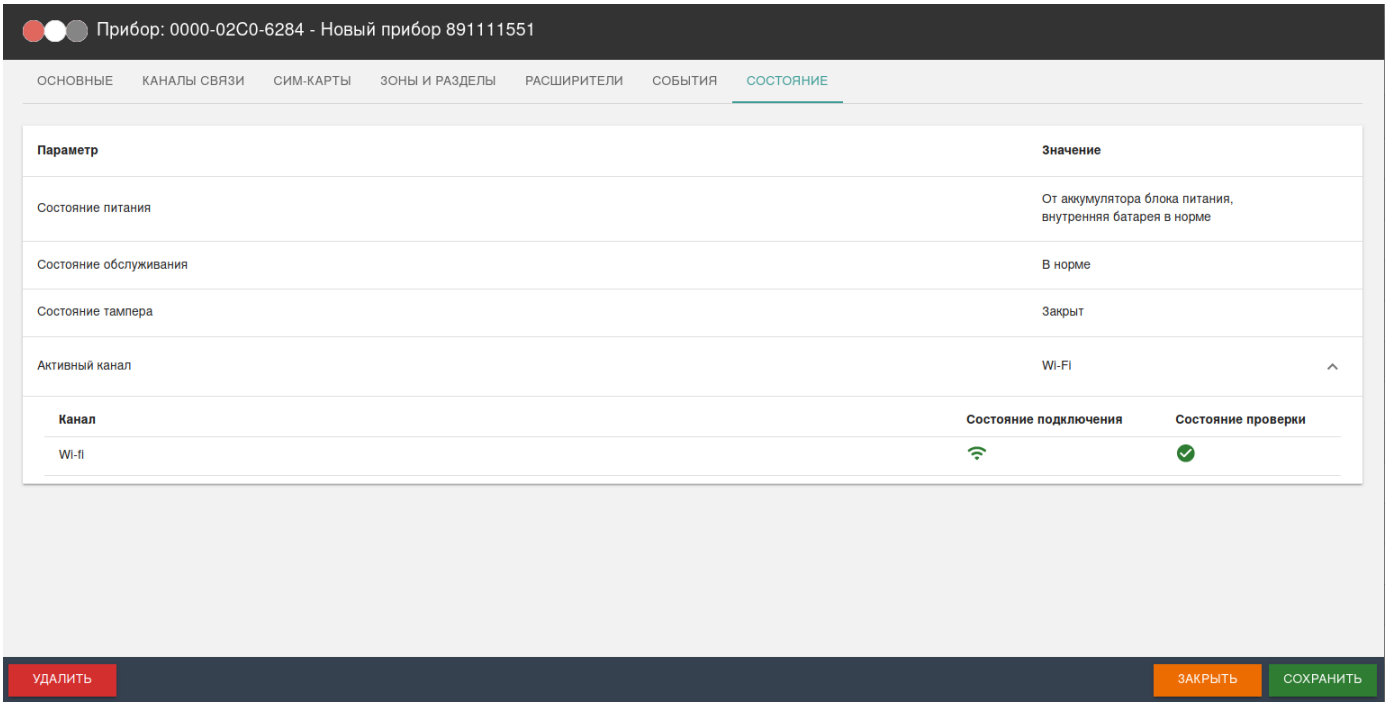


Рис. 63 Добавление прибора. Вкладка «Состояние»

В связи с тем, что не все приборы поддерживают "Дежурный режим 3" в данной вкладке информация может отсутствовать(рис. 63).

- **Состояние питания** - отображает текущее подключение прибора к источнику питания, а так же состояние аккумуляторной батареи.
- **Состояние обслуживания** - возможность передачи на прибор состояние договора(в разработке)
- **Состояние тампера** - При отключенном контроле взлома отображает информацию о том вскрыт корпус или нет.
- **Активный канал** - Отображает информацию о том по какому каналу связи в данный момент работает прибор.
  - **Канал** - Определяется аппаратной частью прибора. Список доступных каналов связи определяется списком: Ethernet, Wi-Fi, GPRS(SIM1),GPRS(SIM2).
  - **Состояние подключения** - имеет два состояния *на связи*, *отключён*.
  - **Состояние проверки** - "проверка пройдена", "ошибка проверки" состояния или состояние "не проверено"

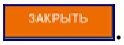
6.3.2 Сохранение, редактирование и удаление записи прибора

Если необходимо внести изменения в данные по прибору, то в этом случае нужно нажать кнопку "Редактировать" , расположенную справа от записи информации о приборе, в таблице приборов. После того, как вся необходимая информация о приборе введена в карточку прибора

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

необходимо нажать кнопку "Сохранить" 

.

Для того, чтобы закрыть карточку прибора, необходимо нажать кнопку "Закрыть" 

.

Для удаления прибора, вначале необходимо исключить его из объекта, и только после этого можно войти в карточку прибора и нажать кнопку "Удалить" 

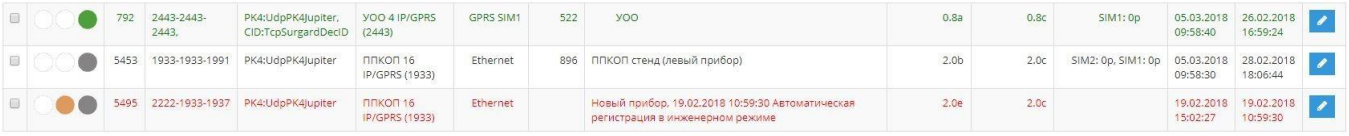
6.3.3 Подмена прибора

Система имитостойкости СПИ «Юпитер» и СПИ "Сатурн" 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) . Далее рекомендуется выполнить следующие действия:

1. Для корректной подмены оба прибора должны находиться в снятом состоянии.



	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

Рис. 64 Цветовая индикация прибора на подмену

2. Настраиваем **новый прибор** и подключаем к серверу, он появляется во вкладке `Клиенты-Приборы` выделенный красным цветом(рис. 64).

3. Войти в карточку прибора в режиме **"Редактировать"** 
. В карточке прибора будет кнопка **"Заменить"**(рис. 65)

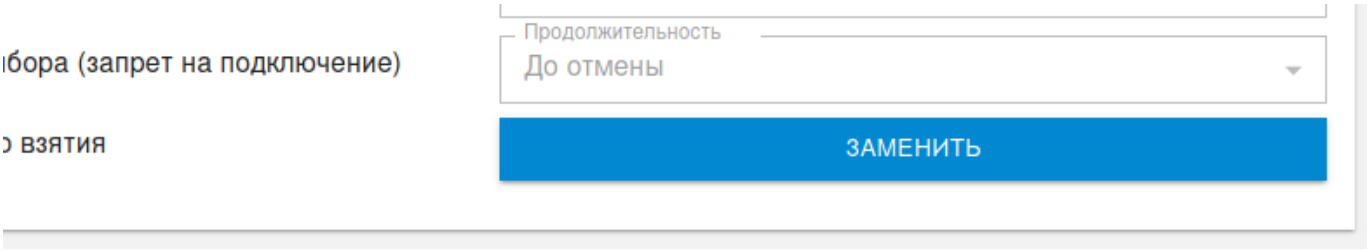


Рис. 65 Внешний вид формы разрешения замены прибора

4. После операции замены,нажать кнопку "Сохранить" 

и "Закрыть" 

.

5. После произведенных действий, статусы приборов изменятся. Далее, можно войти в карточку подменённого прибора и там, либо отредактировать, либо удалить, либо прибор заблокировать.

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

6.3.4 Удаленное обновление ПО прибора

В СПИ предусмотрена возможность обновления ПО приборов удаленно. Для этого в пункте меню "Клиенты" необходимо выбрать раздел "Приборы". После этого в списке приборов необходимо выбрать фильтр **"Требующие обновления"**, в таблице приборов останутся приборы, чья прошивка не совпадает с версией прошивки на сервере репозитория. Иногда, возникает ситуация, когда версия ПО в приборе старше версии расположенной в репозитории, в этом случае, запускать обновление ПО для таких приборов нет необходимости.

Перед запуском механизма обновления ПО приборов, убедитесь, что ПО, установленное в устройстве на данный момент, поддерживает удаленное управление.

Для визуального контроля процесса загрузки ПО и функционирования приборов используется следующая цветовая индикация(рис. 66):



Рис. 66 Цветовое обозначение состояния приборов

В случае, необходимости обновления ПО необходимо выполнить следующие действия:

1. Отметьте приборы, у которых требуется обновить ПО.
2. Нажмите на кнопку "Групповые операции" 

3. В открывшейся форме, нажмите кнопку запуска операции - "Обновить прошивку" 

4. Для проверки состояния загрузки ПО можно открыть карточку прибора в режиме "Редактировать"  и открыть вкладку "События". В протоколе событий должно появиться сообщение, содержащее следующую информацию:

```
"UOO " HM10 0 - Например, для прибора "УОО"- это означает, что процесс загрузки начался, скачено 0%

или в более понятном виде

Доступная версия ПО 1.0K
Загрузка файла обновления ПО 0%
Текущая версия ПО 1.0g admin: Администратор
```


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

Далее будет отображатся ход выполнения задачи
5. Если при загрузке ПО не возникло ошибок, то после завершения загрузки обновления, прибор самостоятельно перезагрузится и будет работать в штатном режиме.

6.3.5 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.

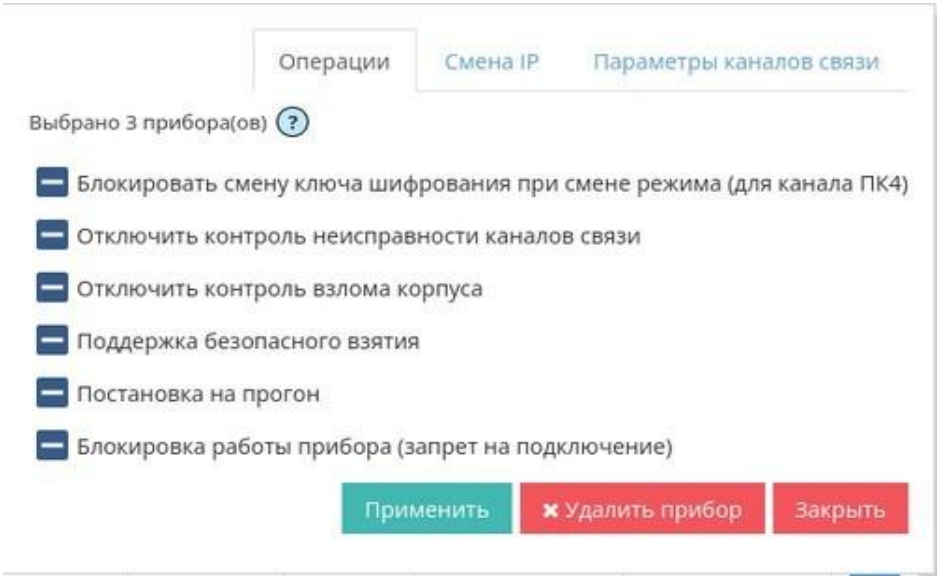


Рис. 67 Групповые операции с приборами. Вкладка «Операции»

6.3.5.1 Групповые операции с приборами охраны. Вкладка «Операции»

В групповых операциях доступны следующие действия:

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

Для того чтобы, измененные настройки начали действовать необходимо нажать кнопку "Применить" 

.

Для удаления, выделенных приборов необходимо нажать кнопку "Удалить прибор"



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

При обновлении ПО приборов, когда используется фильтр "Требующие Обновления" внизу окна групповых операций появляется дополнительная кнопка "Обновить прошивку" 

При использовании фильтра "Инженерный режим" появляется возможность автоматического создания объектов 

для приборов, ещё не назначенных объектам.

6.3.5.2 Групповые операции с приборами охраны. Вкладка «Смена IP»

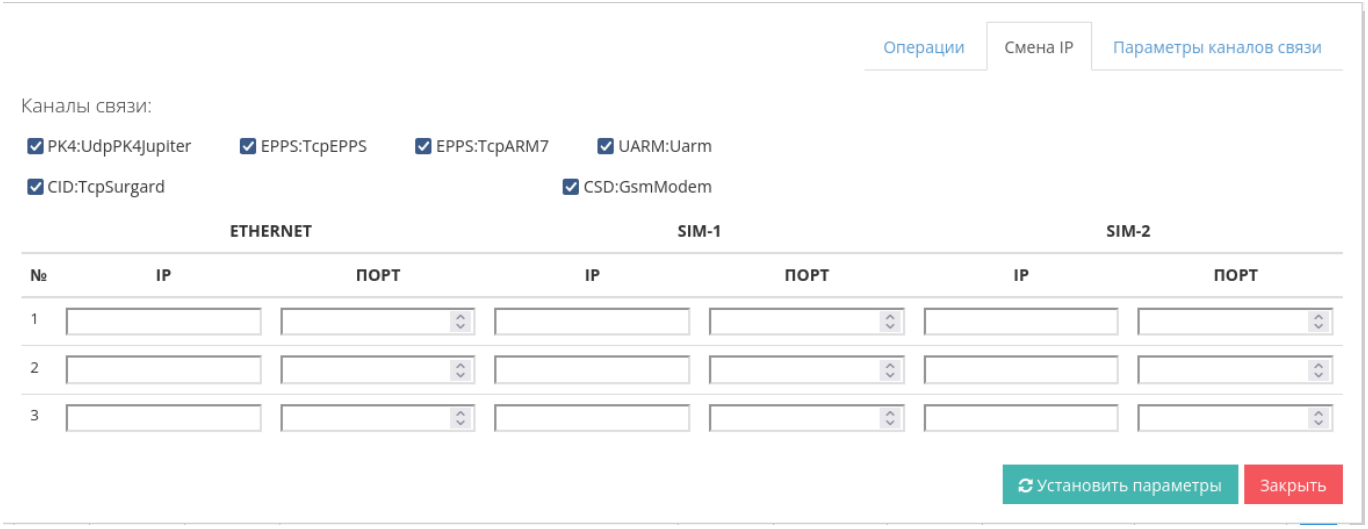


Рис. 68 Групповые операции с приборами. Вкладка «Смена IP»

При внесении изменений в сетевые настройки прибора(рис. 68):

- Выбрать протокол для которого вносятся изменения, как правило это протокол **UdpPK4Jupiter**
- Внести изменения в сетевые настройки, прописав в подразделы ***Ethernet***, ***SIM1***, ***SIM2***
  - **IP** - интернет адрес СПИ, куда буден передавать информацию прибор
  - **ПОРТ** - Порт сервера, определяте индивидуальные настройки ОО в ПО.

Для каждого канала связи можно указать/изменить три записи, для связи с сервером. Если вносится изменение в поле, в котором уже есть настройки на сервер, то в этом случае запись в приборе перезапишется новой, поэтому необходимо соблюдать осторожность при выполнении этой операции. В том случае если в строку изменения не внесены(пустая строка), изменение записи в приборе не произойдёт.

Чтобы необходимые изменения передались на приборы, необходимо нажать "Установить параметры" 

6.3.5.2 Групповые операции с приборами охраны. Вкладка «Параметры каналов связи»

Изменение параметров каналов связи (оповещения о потере связи с приборами)(рис. 69)

Перед началом внесения изменений убедитесь, что выделены именно те каналы связи куда надо внести изменения

Можно изменить:

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

- Время до вывода сообщения о неисправности канала связи
- Время до вывода сообщения о потере связи с устройством
- Период оповещения о потере связи с устройством
- Если в приборе настроены трансляции, то в этом случае появляется возможность "Сменить таблицу перекодировок"

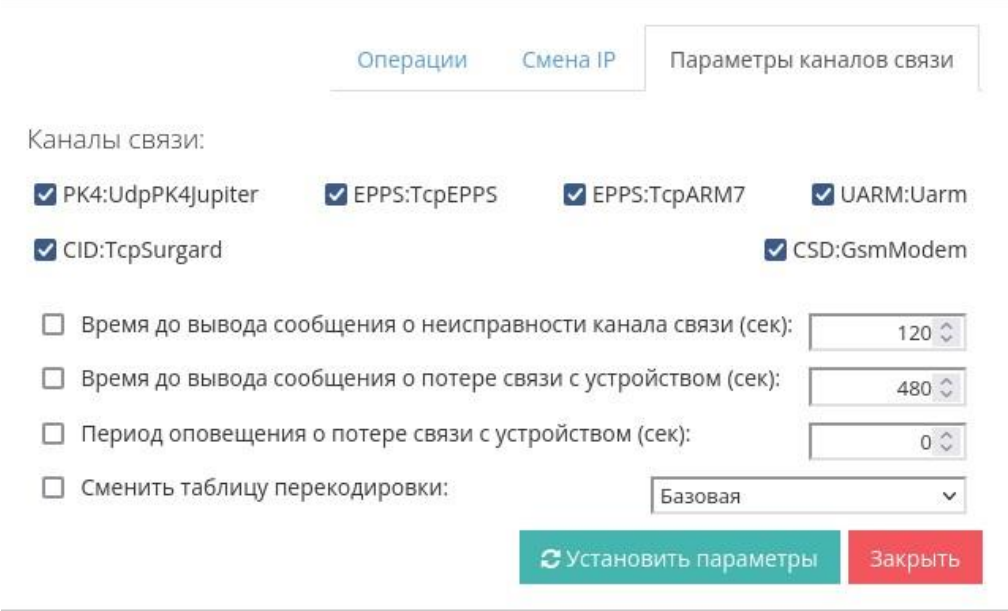


Рис. 69 Групповые операции с приборами. Вкладка «Параметры каналов связи»

Чтобы необходимые изменения передались на приборы, необходимо нажать "Установить параметры" 

6.4 Ответственные лица

В се ответственные лица, а также делегированные по договорам и объектам отображаются в **Таблице Ответственных лиц**(рис.70):

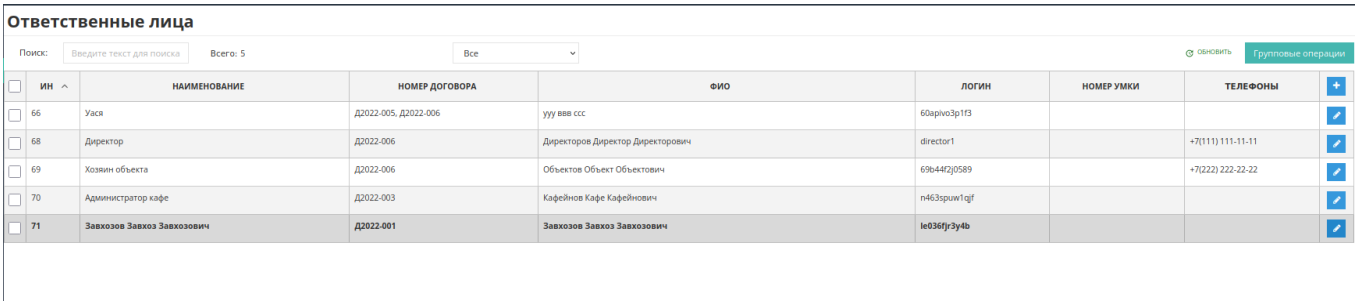


Рис. 70 Таблица ответственных лиц(ХО)

В этом разделе предусмотрены следующие действия над таблицей:

- **Поиск** - Поиск ХО по любому известному признаку или его части.

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

- **Всего** - Отображает общее количество Обветственных, зарегистрированных в БД конкретной ОО.

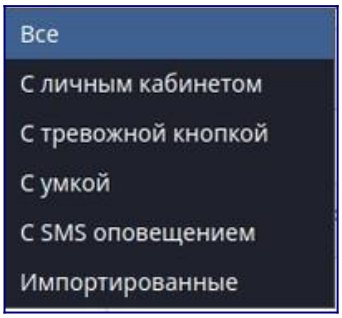


Рис. 71 Фильтр Ответственных лиц

- **Фильтр опций** - Фильтр позволяет вывести в таблицу ответственных, у которых присутствует один из указанных параметров(рис. 71):
  - ***Все*** - фильтр отключён.
  - ***С личным кабинетом*** - пользователи, которым разрешено использовать мобильное приложение "Сатурн".
  - ***С тревожной кнопкой*** - пользователи, у которых установлено мобильное приложение "Тревожная кнопка".
  - ***С Умкой*** - Пользователи, использующие GPS-трекер "УМКА".
  - ***С SMS оповещением*** - ответственные, которым подключено информирование посредством SMPP сервиса.
  - ***Импортированные*** - будут отображаться данные перенесённые из "Юпитер-7".
- **Обновить** - 

- Сделать принудительное обновление текущей информации по ответственным лицам.
- **Групповые операции** 

- Позволяет выполнить однотипные операции для одной и более записей. Данный функционал позволяет назначить или отменить, отмеченным пользователям, доступ к личному кабинету, удалить эти записи или закрыть форму без выполнения действий.

Таблица отображает основные параметры ответственного лица:

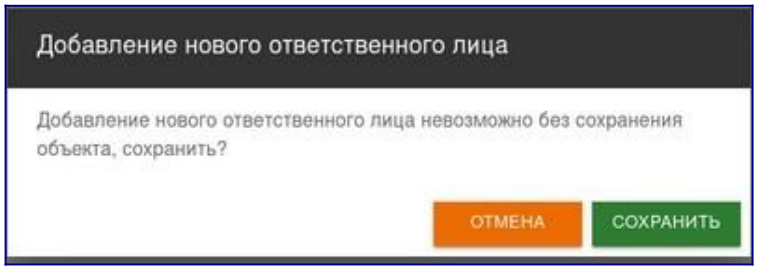
-  - поле выбора записи для групповых операций. Позволяет выбрать сразу все записи или отдельно.
- **ИН** - Идентификационный номер. Определяется внутри БД и присваивается записи ответственного лица автоматически, при сохранении карточки. Не является порядковым номером записи в таблице.
- **НАИМЕНОВАНИЕ** - Может быть пустым, а так же нести информацию о персонализации ответственного или обозначать его должность.
- **НОМЕР ДОГОВОРА** - Договор в котором участвует данное лицо. Ответственное лицо может быть не указано в договоре, но при этом может быть прикреплено к объекту.

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

- **ФИО** - Отображает Фамилию, Имя, Отчетсво лица, указанного в карточке.
- **ЛОГИН** - Отображает имя пользователя, зарегистрированного в сервисах "Личный кабинет" и "Тревожная кнопка".
- **НОМЕР УМКИ** - Идентификационный номер GPS-трекера, закрепленного за ответственным.
- **ТЕЛЕФОНЫ** - Номера телефонов, записанных в карточке регистрации ответственного лица.

6.4.1 Добавление и редактирование ответственного лица

Для добавления нового ответственного лица необходимо нажать на кнопку "Добавить" . В том случае, когда возникает необходимость изменить данные ответственного, необходимо нажать на кнопку "Редактировать" . При этом откроется карточка учета Ответственноло лица.
В данной вкладке можно ввести ответственных/делегированных лиц. При этом обратите внимание на тот момент, что ХО можно прикрепить к одному или нескольким объектам, а в договоре указывается лицо, с которым заключен договор.



- Если в договоре указано Физ.лицо, являющееся Хоз.органом, то его необходимо указать в этом списке.
- Если при создании записи Хоз.органа не указан объект, запись ХО удаляется. Вариант сохранения "пустого" ХО не предусмотрен.

Для регистрации записи ХО необходимо нажать значок "Добавить" . При этом если в карточке объекта были произведены какие-либо действия система выдаст предупреждение

Можно закрыть окно, нажав "ОТМЕНА" и продолжить вносить изменения в другие разделы, либо нажать "СОХРАНИТЬ" и перейти к вводу информации по Хоз.органам.

6.4.1.1 Учетная карточка Ответственного лица

Для добавления информации об ответственном лице необходимо заполнить соответствующую форму(рис. 72). Поля в, предлагаемой форме имеют следующие значения:

- **Наименование** - Здесь можно указать должность или информацию, связанную с персонализацией ХО.
- **Фамилия, Имя, Отчество** - ФИО лица , включенного в договор, либо имеющего доверенность, либо имеющего право на действия, связанные с охраной объекта(постановка, снятие, КТС и т.п.)

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

- **Объекты** - Так как в договоре может быть указано несколько объектов, а ХО может быть указан в разных договорах, при создании карточки ХО, ему можно назначить конкретный объект или несколько объектов. В выпадающем списке отображаются все доступные объекты. Нажав на один из них, можно закрепить объект за ответственным лицом. Таким образом можно указать несколько объектов. Для удаления объектов из списка необходимо нажать на кнопку удаления , расположенную справа от наименования объекта. Список объектов, прикреплённых к договору, задается во вкладке "Объекты".

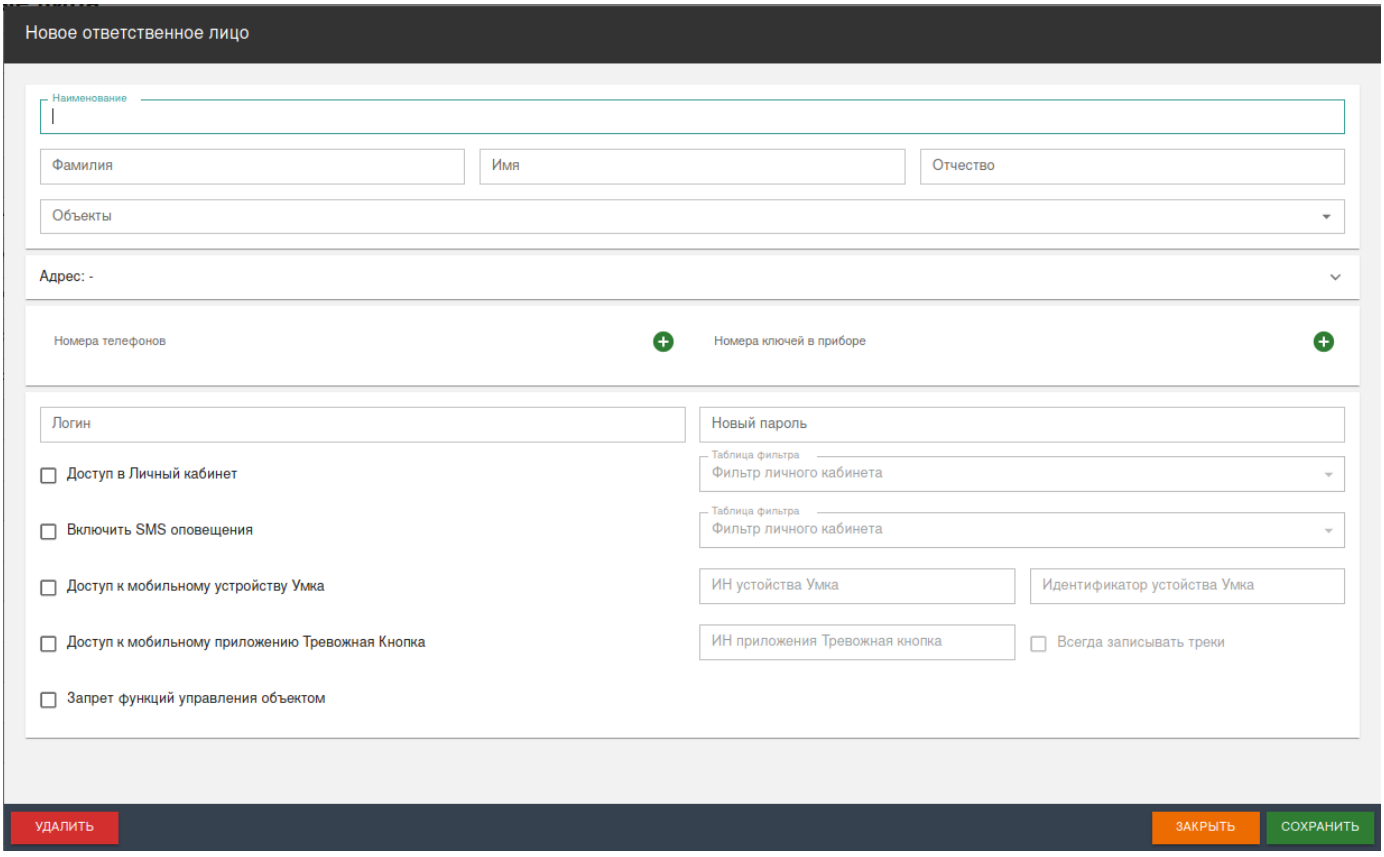
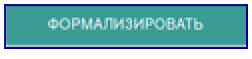


Рис. 72 Карточка регистрации ответственного лица

- **Адрес** - Адрес регистрации или фактического местонахождения/расположения, указанного выше субъекта. Форма для заполнения открывается при активации строки, маркер меняет форму, например . Для более точной формализации адреса, желательно указывать полный почтовый адрес. Если известен и введен населенный пункт и адрес можно уточнить его данные, нажав кнопку 

система попытается связаться с кладром и уточнить данные, связанные с указанным адресом.
!!!ВНИМАНИЕ!!! Обратите особое внимание на то обстоятельство, что основным критерием уникальности **Ответственного лица**, выступает его номер телефона. Таким образом, нельзя создать разные ХО с одним номером телефона.
- **Номера телефонов** - для ввода данной информации необходимо нажать на символ "Добавить" . После чего, откроется форма для заполнения, где указывается:

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

- **Номер телефона** - в формате - +7XXXXXXXXX, либо 8XXXXXXXXXX. Допускается использование разделителей. Необходимо учитывать, что номера телефонов "Ответственных лиц", "Договора", "Объекта" могут быть не связаны между собой.
- **Комментарий** - Информация служебного или личного характера, которая связана с данным телефонным номером. Например, время в которое можно звонить на этот номер или его территориальное расположение на объекте.
- **Тип** - Определяет специфику телефонного номера. В выпадающем списке можно выбрать тип номера телефона:
  - - - тип не указан.
  - ***Основной*** - главный номер телефона для связи с ответственным.
  - ***Домашний стационарный*** - Личный номер городской телефонной линии.
  - ***Рабочий стационарный*** - Служебный/Рабочий номер городской телефонной линии.
  - ***Личный мобильный*** - Личный номер, предоставленный оператором мобильной связи.
  - ***Служебный мобильный*** - Служебный/Рабочий номер, предоставленный оператором мобильной связи.

Если возникла необходимость в удалении записи, нажмите символ "Удалить" и согласитесь с действием.

На одного ответственного может быть зарегистрировано несколько номеров телефонов.

- **Номера ключей в приборе** - Как правило, у каждого ответственного за объект, в приборе есть ключи, при вводе которых объект ставится под охрану или снимается с охраны. В том случае, если указаны данные на каком приборе какой номер ключа привязан к данному ответственному лицу, дежурный или оператор на ПЦО в ленте событий может увидеть персонализированные данные. За одним ответственным может быть закреплено несколько ключей, как на одном приборе, так и на нескольких. Для добавления ключа необходимо нажать "Добавить". В открывшейся форме необходимо заполнить, следующие поля(рис. 73):
  - **Прибор** - Из выпадающего списка выбрать необходимый прибор.
  - **Ключ доступа** - Указать номер ключа в приборе, закрепленный за ответственным лицом.
  - **PIN** - численный пароль, задаётся автоматически при сохранении ХО. Данный код необходим при автоматической проверке ТК. Если при записи PIN не сформирован, то это означает, что в приборе отсутствует данный ключ.

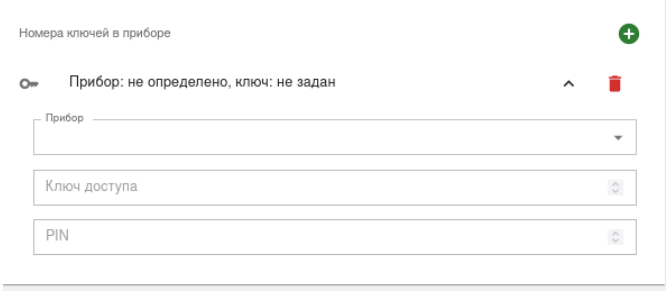


Рис. 73 Форма для ввода номера ключа ХО в приборе

- Если возникла необходимость в удалении записи, нажмите символ "Удалить" и согласитесь с действием.

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

Дальнейшие параметры определяют доступ к системе - Данные для авторизации в мобильных приложениях - "Личный кабинет" и "Тревожная кнопка v 2.0".

- **Логин** - Генерируется автоматически при создании записи ответственного лица, но может быть задан вручную.
- **Новый пароль** - Необходимо задать самостоятельно. Позволяет изменить пароль при утере или компроментации.
- **Доступ в Личный Кабинет** - Разрешает/Запрещает доступ пользователя к сервису "Личный кабинет".
    - После активации сервиса открывается "Таблица фильтра" для Личного Кабинета, которая позволяет выбрать фильтр сообщений, что позволяет сократить трафик.
- **Включить SMS оповещения** - Разрешить отправку SMS-сообщений этому пользователю по событиям на объектах, включенных в договор. Данный функционал имеет смысл использовать при настроенном SMPP сервере.
    - После активации сервиса открывается "Таблица фильтра" для SMS уведомлений, которая позволяет выбрать фильтр сообщений.
- **Доступ к мобильному устройству "Умка"** - Разрешает/Запрещает доступ к сервису взаимодействия с носимым GPS-трекером "Умка". При активации данного сервиса необходимо заполнить поле ***"Идентификатор мобильного устройства "Умка"***. Идентификатор устройства обычно расположен на ярлыке, с обратной стороны устройства. После этого данное устройство идентифицируется сервером КРОС как прибор, поэтому в дальнейшем все действия аналогичны операциям с обычным прибором. Инструкция по настройке GPS-трекера расположена в разделе Часы "УМКА"
- **Доступ к мобильному приложению "Тревожная Кнопка"** - Разрешает/Запрещает доступ к сервису "Тревожная кнопка". При включении этого сервиса в разделе Приборы автоматически создаётся прибор, использующий драйвер мобильного приложения. Таким образом, сервер КРОС работает с мобильным приложением, как с обычным прибором. Описание приложения расположено в разделе Мобильные приложения

  Для корректного определения местоположения мобильного объекта, когда разрешен **Доступ к мобильному приложению "Тревожная Кнопка"** и/или **Доступ к мобильному устройству "Умка"**, рекомендуется включить параметр **Всегда записывать трек перемещения**, что позволит оперативно определить местонахождение ответственного лиц. При этом после сохранения данных в списке приборов автоматически создается прибор, связанный с приложением "Мобильная ТК" или часами "УМКА".
- **Запрет функций управления объектом** - данная опция не позволяет пользователю управлять объектом. Пользователь получает информацию в режиме мониторинга.

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

- **Инкассатор** - специальный режим, который необходимо активировать, в случае договора по охране инкассаторов. Данный атрибут указывает, что ответственное лицо является инкассатором.

При создании объекта ХО можно создать во Вкладке **ХО**. Необходимо учитывать то обстоятельство, что вводимый ХО может уже присутствовать в **списке ответственных**. В этом случае, для включения ХО в список ответственных на объекте, необходимо в списке ответственных найти необходимый ХО и в его карточке выбрть необходимый объкет.

7. Меню «Охрана»

В окне «Реквизиты» (меню «Охрана» → «Реквизиты») (рис 74) **Администратор сервера** создает структуры подразделений охранных организаций внутри основного сервера.

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

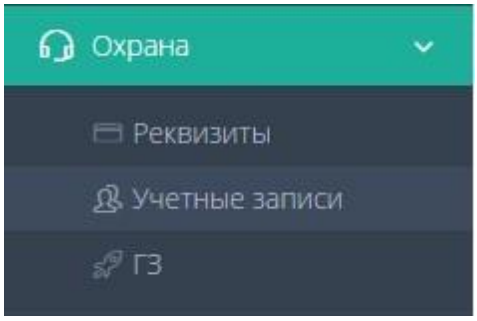


Рис. 74 Меню «Охрана»

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, и тд.

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.

7.1 Реквизиты

В окне «Реквизиты» (меню «Охрана» → «Реквизиты»)(рис. 75) **Администратор сервера** создает структуры подразделений охранных организаций внутри основного сервера. Так же, он может редактировать системные параметры ОО.

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

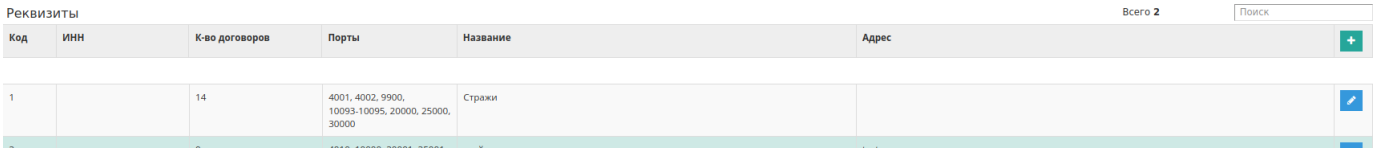


Рис. 75 Таблица охранных организаций

Для добавления новой охранной организации необходимо нажать кнопку "Добавить" В случае, когда необходимо посмотреть данные по организации или внести изменения, следует нажать "Редактировать" в строке записи ОО.

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.

Администратор имеет доступ к настройкам только своей ОО и не может добавлять новые реквизиты или удалять существующие, только редактировать относящиеся к его организации. **Администратор** не может изменить системные настройки своей ОО.

7.1.1 Реквизиты охранной организации. Вкладка «Основные Данные»

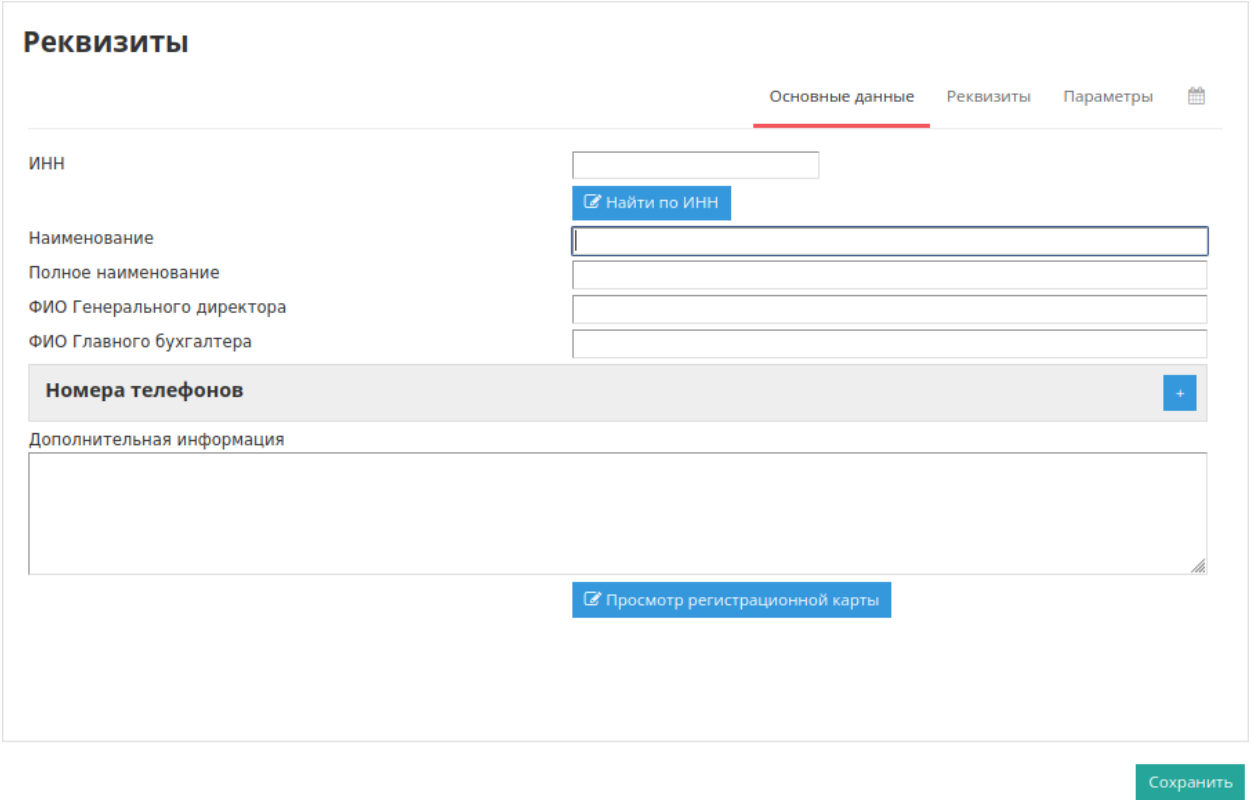


Рис. 76 Реквизиты охранной организации. Вкладка «Основные Данные»

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

Вкладка «Основные Данные» карточки регистрации охранной организации(рис. 76) включает в себя следующую информацию:

- **ИНН** - Индивидуальный Налоговый Номер ОП. Для уточнения данных можно использовать кнопку "Найти по ИНН". После проверки ИНН в БД налоговой инспекции, нижеследующие данные будут заполнены автоматически. 

- **Наименование** - Краткое наименование ОО.
- **Полное наименование** - Наименование ОО, так как оно зарегистрировано в налоговой инспекции.
- **ФИО Генерального директора** - Данные по руководителю ОО.
- **ФИО Главного бухгалтера** - Данные по лицу, осуществляющему финансовую деятельность предприятия.
- **Номера телефонов** - Номера телефонов ОО. Для ввода информации необходимо нажать на кнопку "Добавить"  и согласиться на операцию добавления номера, нажав "Да". После чего, заполнить необходимые поля:

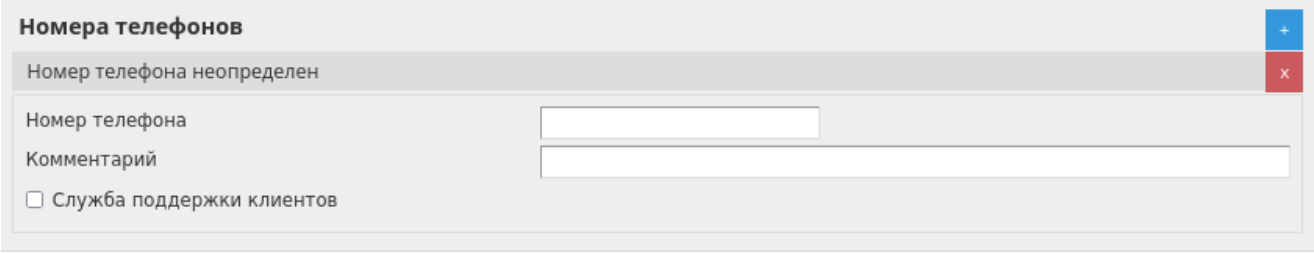


Рис. 77 Форма для ввода номеров телефона организации

- ♦ ***Номер телефона*** - Номер телефона в формате, содержащем код населённого пункта, например +7(XXX)XXX-XX-XX или 8(XXXXX) XX-XX-X.
- ♦ ***Комментарий*** - Информация по номеру телефона или его расположению, например, время работы или расположение у операторов.
- ♦ ***Службы поддержки клиентов*** - отметка о том, что данный номер не предназначен для приёма оперативной информации.

  - Для удаления информации по номеру телефона необходимо нажать значок "Удалить" .

- **Дополнительная информация** - Информация об ОО требующая внимания. Для просмотра всей информации , связанной с ОО необходимо нажать на кнопку "Просмотр регистрационной карты" 

В случае, когда карточку ОП редактирует **Администратор сервера**, то у него появляется возможность отправить информацию на e-mail 

, однако это разрешено только в том случае, если в системе настроен "SMTP сервер".

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

7.1.2 Реквизиты охранной организации. Вкладка «Реквизиты»

Вкладка предназначена для ввода статистической и банковской информации, связанной с ОО(рис. 78).

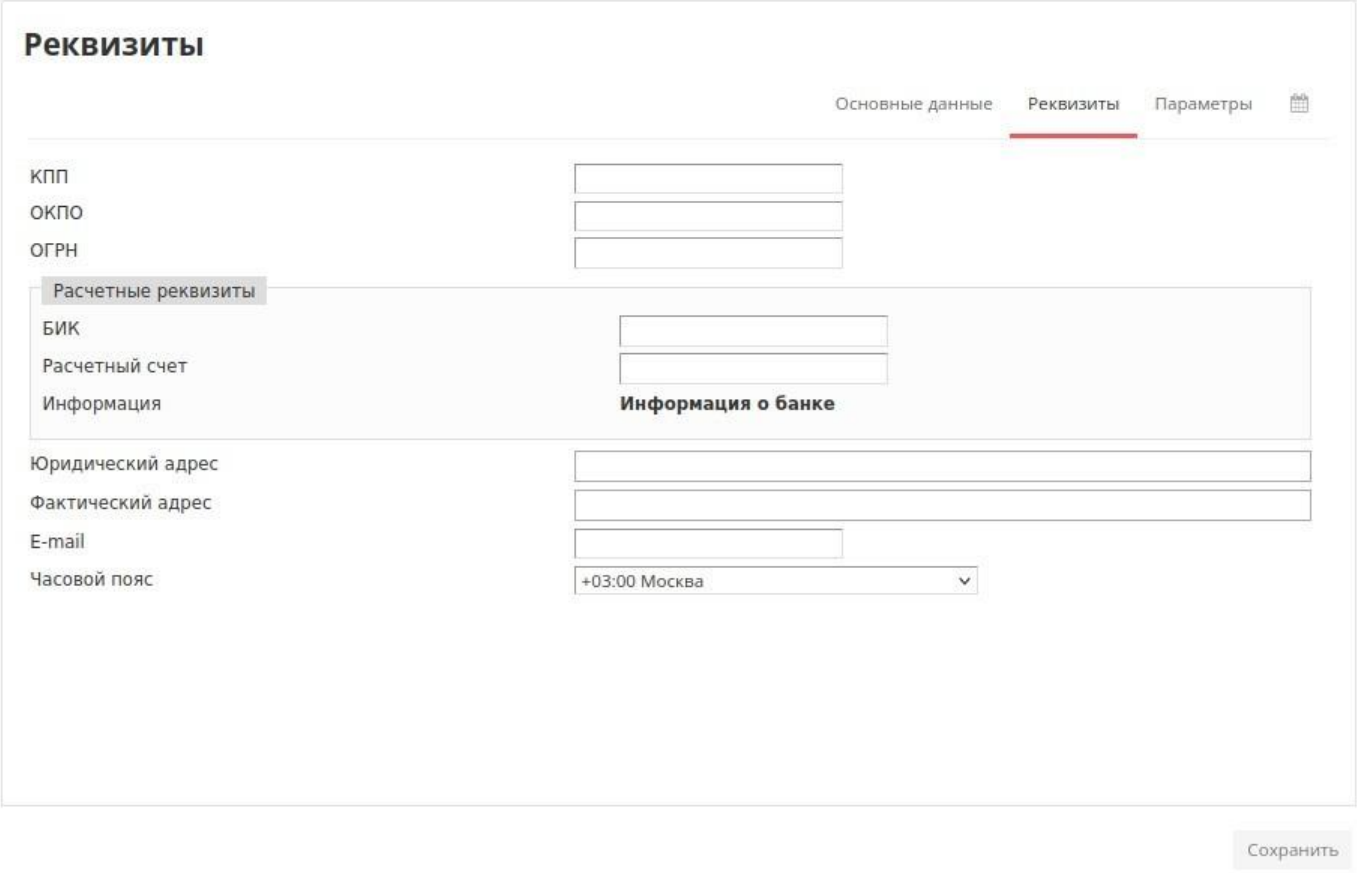


Рис. 78 Реквизиты охранной организации. Вкладка «Реквизиты»

- **КПП** - Код причины постановки на учет — это код, который дополняет ИНН и содержит информацию об основании постановки на учет в налоговом органе.
- **ОКПО** - общероссийский классификатор предприятий и организаций. Состоит он из 8 или 10 цифр. Каждой фирме Росстат присваивает уникальный ОКПО, его обязана иметь любая организация.
- **ОГРН**(для ИП – **ОГРНИП**) – это основной государственный регистрационный номер юридического лица, который присваивается при его создании и после записи о нем в ЕГРЮЛ (или ЕГРИП для ИП). Указывается ОГРН в свидетельстве, которое официально выдается налоговой службой и свидетельствует о постановке на налоговый учет.
- **Расчетные реквизиты**:
  - ***БИК*** - Банковский идентификационный код – девятизначный уникальный код кредитной организации. Он предназначен для идентификации участников расчетов и является обязательным элементом реквизитов любого банка. БИК используется в платежных документах на территории России.

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

- ***Расчетный счет*** — Это специальный счет в банке, который открывается для индивидуальных предпринимателей и юридических лиц. Он используется для безналичных расчетов с контрагентами, выплаты заработной платы, уплаты налогов и сборов.
- ***Информация*** - После ввода банковских реквизитов здесь появится информация об отделении банка.

- **Юридический адрес** - адрес регистрации ОО.
- **Фактический адрес** - адрес реального месторасположения ОО.
- **Часовой пояс** - Часовой пояс в котором расположена ОО.

7.1.3 Реквизиты охранной организации. Вкладка «Параметры»

При создании ОО, в рамках сервера КРОС, ей выделяется уникальный набор портов, который определяет настройки обмена информацией(рис. 79). Вносить изменения в конфигурацию портов ОО может только пользователь **superadmin**.

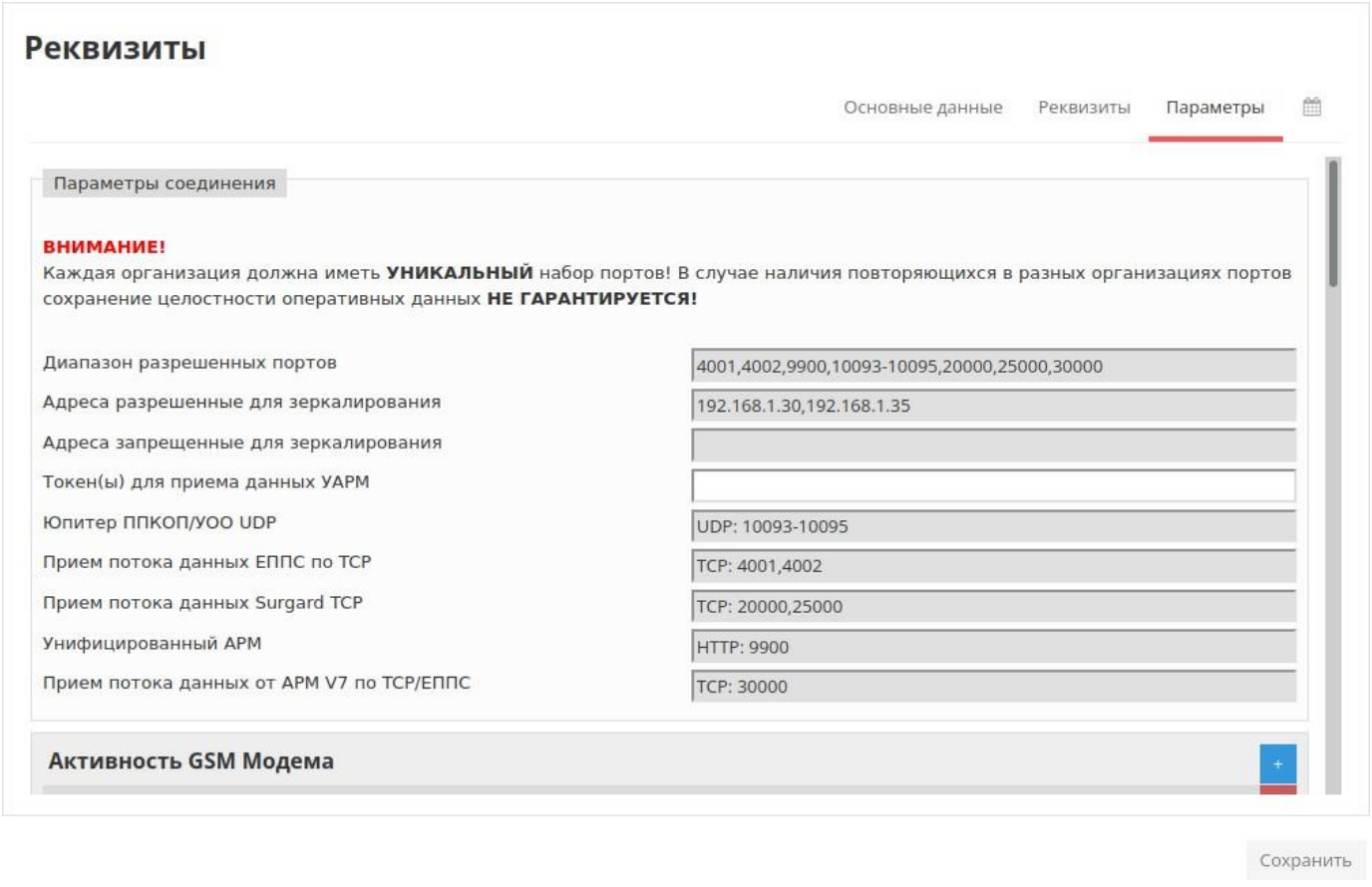


Рис. 79 Реквизиты охранной организации. Вкладка «Параметры»

На данной вкладке можно посмотреть параметры, определенные для работы данной ОО, изменить параметры настройки портов может только Администратор сервера - superadmin. Так же здесь можно изменить параметры реагирования данной ОО.

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

7.1.3.1 Параметры соединения

- ***Диапазон разрешенных портов*** - Общий список портов, назначенный конкретной ОО.
- ***Адреса разрешенные для зеркалирования*** - Назначаются Администратором сервера при наличии трансляции с другого сервера.
- ***Адреса запрещенные для зеркалирования*** - После включения трансляции на передающем сервере, адреса серверов попадают в данный список, чтобы избежать, неконтролируемую передачу данных, а так же, чтобы избежать ошибок при настройке трансляций на разные ОП. Перевести адрес сервера из запрещенных в разрешенные может только Администратор сервера.
- ***Токен(ы) для приема данных УАРМ*** - Идентификаторы, определяющие индивидуальный номер подключения, ключ шифрования.
- ***Юпитер ППКОП/УОО UDP*** - порт принимающий сообщения от приборов.
- ***Прием потока данных ЕППС по TCP*** - Порты по которым сервер будет принимать информацию по протоколу ЕППС(Зеркалирование).
- ***Прием потока данных Surgard TCP*** - Порт приема сообщений по протоколу Surgard и Surgard v4.
- ***Унифицированный АРМ*** - Порт для обмена сообщениями по протоколу УАРМ.
- ***Прием потока данных от АРМ V7 по TCP/ЕППС*** - Порт для обмена информацией с сервером "Юпитер-7"

7.1.3.2 Активность GSM Модема

Позволяет настроить варианты реагирования на сигналы от GSM модема "Юпитер-4". Для того, чтобы записать номер телефона и действие, с ним связанное, необходимо нажать кнопку "Добавить" . Для удаления, соответственно, кнопку "Удалить"

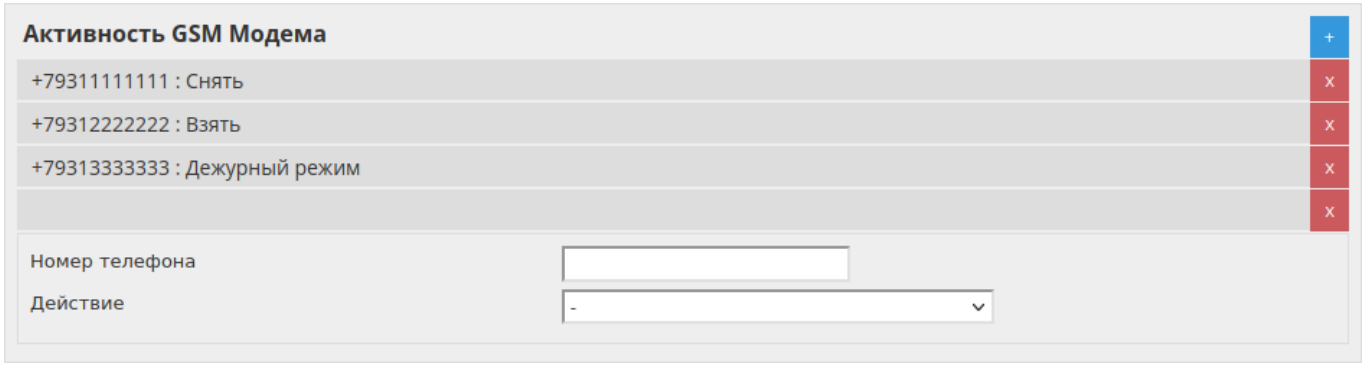


Рис. 80 Фома для ввода номеров телефона GSM-модема

Настроить данные параметры необходимо ещё до ввода в эксплуатацию модема:

- ***Номер телефона*** - номер телефона, закрепленный за СИМ-картой на определенном канале и отвечающий за одну из основных функций охранной деятельности(рис. 81).
- ***Действие*** - определяет реакцию, при поступлении звонка на конкретный номер телефона:

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

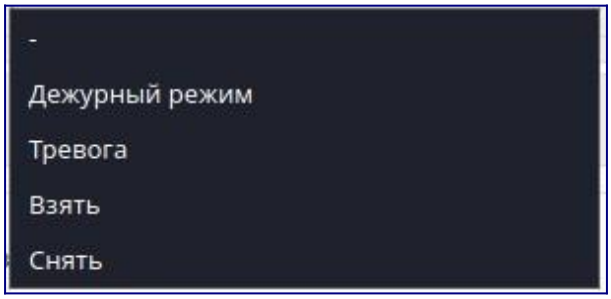


Рис. 81 Режимы работы каналов модема

- - Действие не определено. Номер отключен.
- *Снять* - при настроенных соответствиях Ответственного лица, при поступлении звонка с его номера, прибор, установленный на объекте будет снят с охраны, согласно ключу, указанному в карточке ответственного лица.
- *Взять* - По звонку, если он соответствует ответственному лицу, объект будет взят под охрану в соответствии с ключом, ему соответствующим.
- *Дежурный режим* - проверка состояния связи.
- *Тревога* - Передать тревожное состояние прибора на пульт охраны.

Наличие подобных настроек позволяет настроить использование прибора в сетях с неустойчивым каналом Интернет, однако, этот вариант может оказаться существенно дороже.

7.1.3.3 Каналы IP Модема

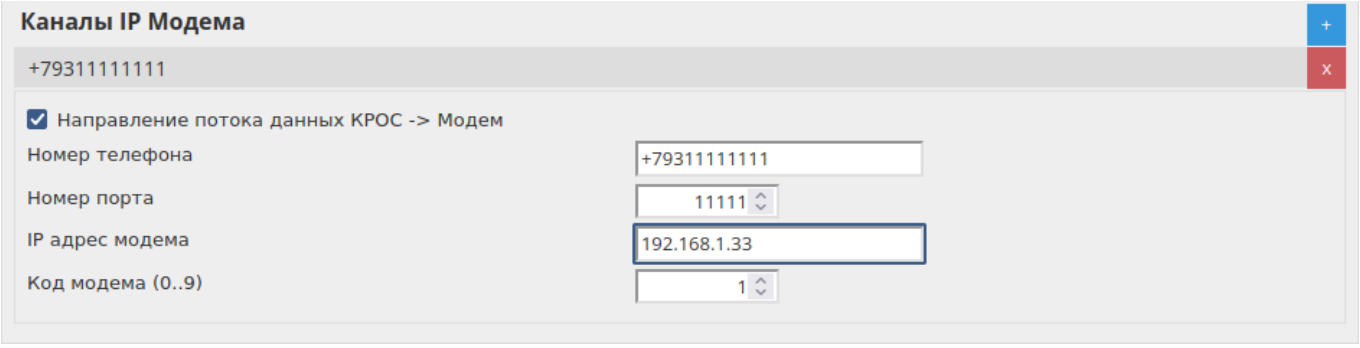


Рис. 82 Форма регистрации номеров телефона IP-модема

При использовании модема модели "Юпитер-7520" необходимо произвести дополнительные настройки каналов. Для этого необходимо "Добавить" телефонного номера, предварительно согласившись с внесением изменения, нажав "Да" на запрос системы(рис. 82).

- **Направление потока данных КРОС -> Модем** - предназначено для использования модемов специального назначения, не используется в обычной охранной деятельности.
- **Номер телефона** - указывается номер телефона, соответствующий действию, описанному в разделе Активность GSM Модема
- **Номер порта** - указывается номер порта, соответствующий номеру телефона(настраивается при конфигурировании модема).

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

- **Сервисный порт** - порт передачи удаленных команд модему, указывается при настройке модема.
- **Код модема (0...9)** - обычно это номер COM-порта, который будет эмулировать драйвер модема, поэтому рекомендуется выставить у каждого номера телефона свой персональный код.

Для удаления, ненужной записи, нажмите кнопку "Удалить".

7.1.3.4 Инженерный режим

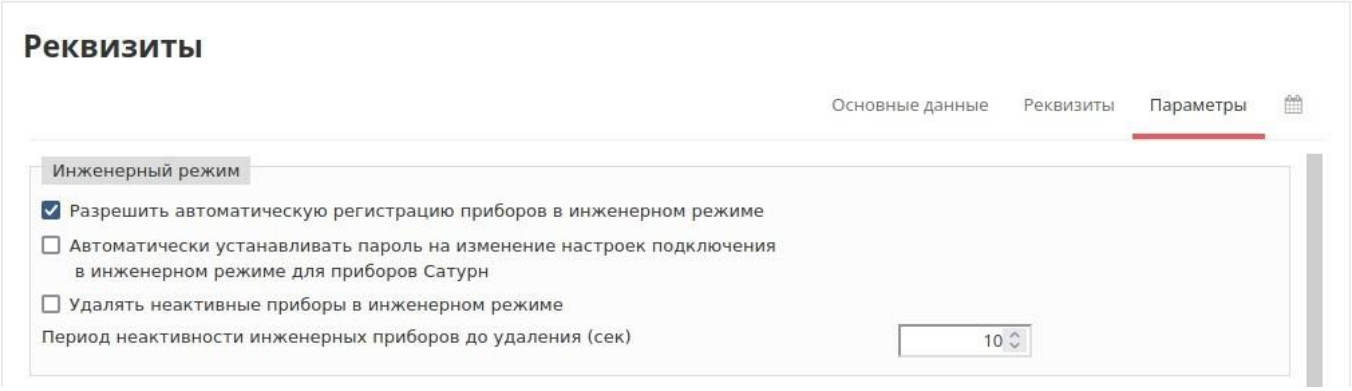


Рис. 83 Задание параметров инженерного режима

Предусматривается обработка информации от приборов, находящихся в Инженерном режиме(рис. 83).

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, от приборов в инженерном режиме, не передаются в АРМ ДПУ/ДО/СК и Web-АРМ, работающие в штатном режиме. Также, в трансляциях данных с таких приборов, в настройках трансляции, необходимо явно установить параметр *Инженерный режим*. Для настройки **Инженерного режима** используют следующие параметры:

- **Разрешить автоматическую регистрацию приборов в инженерном режиме**. Если параметр ***включён*** - все вновь подключаемые к КРОС приборы будут автоматически регистрироваться в так называемой “*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 ***отключён*** - 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.

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

- **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.

7.1.3.5 Режим работы

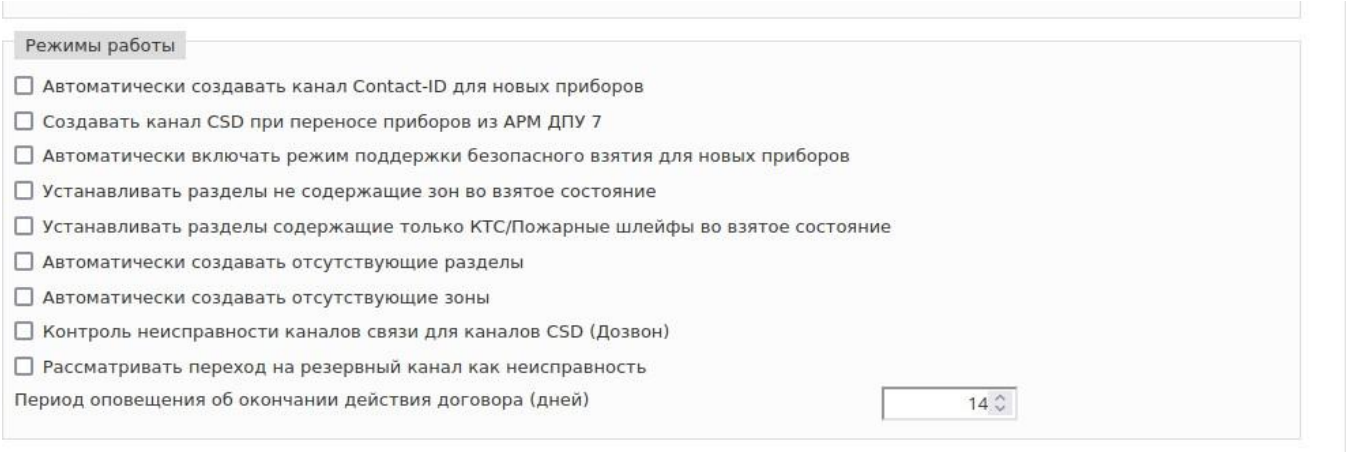


Рис. 84 Параметры основного режима работы ОО

- **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.
- **Создавать канал CSD при переносе приборов из АРМ ДПУ 7**. При импорте данных из "Юпитер-7", автоматически создается канал управления по модему, что в ряде случаев приводит к ошибкам контроля канала связи. Данный параметр рекомендуется устанавливать в том случае, когда управление приборами осуществляется посредством модема.
- **Автоматически включать режим поддержки безопасного взятия для новых 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.

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

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/Пожарные шлейфы во взятое состояние**. Если раздел содержит только ***КТС*** или "Пожарные шлейфы", то логически он всегда находится под охраной. В некоторых случаях, например, для внесения изменений в конфигурацию прибора, конфигуратором, встроенным в КРОС, прибор должен быть полностью снят с охраны. В этом случае необходимо отключить данный параметр, выполнить удаленное конфигурирование прибора и после проверки работы прибора включить параметр. При отключении этого параметра прибор позволяет перевести такой раздел в снятое состояние. При включении, описываемый параметр принудительно устанавливает такой раздел во взятое состояние.
- **Автоматически создавать отсутствующие разделы**. При получении информации о разделах от прибора, в том случае, если структура разделов для данного прибора в БД отсутствует, такая информация будет сохранена автоматически.
- **Автоматически создавать отсутствующие зоны**. В когда получено сообщение 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 канала связи для приборов, работающих по каналу CSD (модем).
- **Рассматривать переход на резервный канал как неисправность**. В случае перехода прибора на резервные каналы связи генерирует неисправность.
- **Период оповещения об окончании действия договора (дней)**. Если договор не поставлен на автопродление, то в момент, когда количество суток до даты истечения договора становится меньше этого значения, в Web-АРМ посылается единоразовое уведомление вида: "ВНИМАНИЕ! До окончания срока действия договора ... осталось меньше ... дней".

7.1.3.6 Обработка тревог

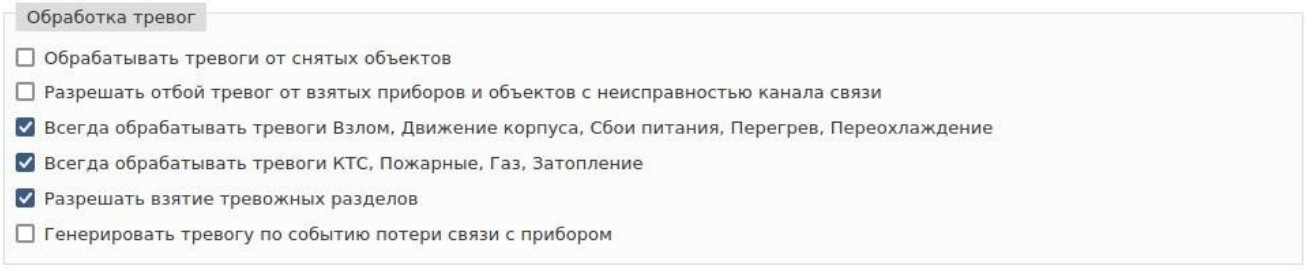


Рис. 85 Параметры обработки тревог

В некоторых случаях возникает необходимость корректировки реагирования КРОС на те или иный сообщения. Для этого существует ряд параметров(рис. 85):

- **Обрабатывать тревоги от снятых объектов**. Если этот параметр установлен? то в случае получения тревожного сообщения от снятого раздела? будет создан дескриптор тревоги и

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

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:
  - ***взят под охрану***
  - ***находится в тревожном состоянии***
  - ***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.
- **Разрешать взятие тревожных разделов**. По умолчанию отправка команд взятия разделам, находящимся в тревожном состоянии запрещена. Этот параметр позволяет разрешить отправку команд взятия тревожным разделам. Целесообразно использовать в том случае, когда раздел вышел из строя по каким-либо причинам и исправить его работу оперативно нет возможности.
- **Генерировать тревогу по событию потери связи с прибором**. Параметр отвечает за генерацию тревожного сообщения при потере связи прибора с пультом охраны.

7.1.3.7 Режим работы АРМ

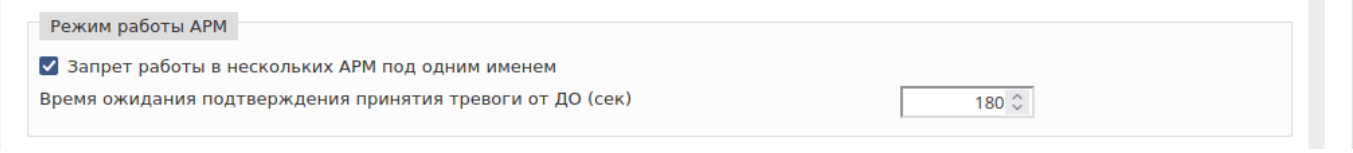


Рис. 86 Общие параметры работы пользователей в АРМ

- **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 оператора дежурному в ручном режиме происходит ожидание подтверждения принятия тревоги в работу. Если в течение указанного времени ни один дежурный не принял тревогу в обработку, то она возвращается оператору.

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

7.1.3.8 Контроль резервного питания

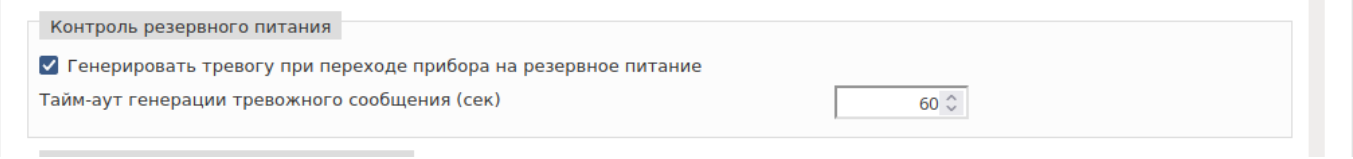


Рис. 87 Управление контролем перехода приборов на резервное питание

- **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.
- **Тайм-аут генерации тревожного сообщения (сек)**. Если после истечения заданного тайм-аута от прибора не пришло сообщение "Восстановление питания", то в этом случае КРОС генерирует тревожное сообщение.

7.1.3.9 Параметры учета состояния договора

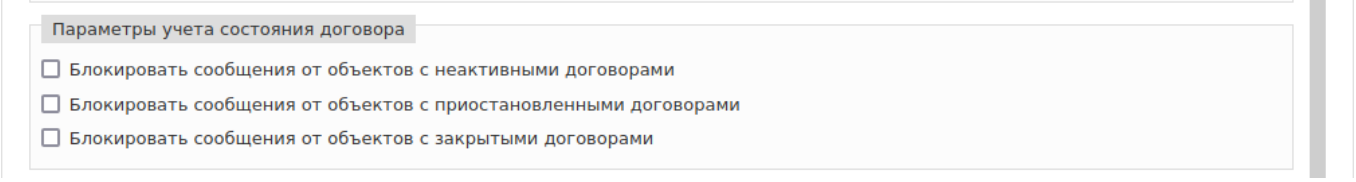


Рис. 88 Параметры реагирования КРОС в зависимости от состояния договоров

КРОС может контролировать состояние договоров обслуживания, периодически проверяет даты начала и окончания действия договоров, а так же, если их текущее состояние не определено, устанавливает состояние ***Активен*** , в случае актуальности указанного периода действия договора, либо ***Закрыт*** - в случае если период договора истек.
Для управления 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.
- **Блокировать сообщения от объектов с приостановленными договорами**. Объекты будут отключены в случае если для договора установлено состояние ***Приостановлен*** . Это состояние может быть установлено/снято вручную или с использованием календаря.
- **Блокировать сообщения от объектов с закрытыми договорами**. Объекты будут отключены, если срок договора истек, либо состояние договора установлено в ***Закрыт***.

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

7.1.3.10 Настройки доступа к SMPP серверу



Рис. 89 Параметры настройки СМС извещений

Отправка SMS-сообщений осуществляется через интернет. Для этого настраивается прямое подключение к SMS-серверу провайдера, предоставляющего услуги, который, в свою очередь отправляет SMS-сообщение адресату. ОО должна заключить договор с местным оператором связи на возможность подключения данной услуги. В каждом регионе условия подключения могут отличаться.

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.

7.1.3.10.1 Настройки доступа к SMPP серверу

Настройка осуществляется Администратором охранной организации. Для этого в требуется:
1) В меню **"Охрана"** - выбрать **"Реквизиты"** - войти во вкладку **"Параметры"**

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

2) Выбрать параметр **"Разрешить отправку СМС сообщений через SMPP сервер"**
Ввести параметры SMPP сервера:

- ***Сетевой адрес SMPP сервера*** - IP-адрес сервера, через который отправляются SMS-сообщения.
- ***Номер порта*** - номер порта, назначенный оператором связи.
- ***Логин учетной записи*** - имя пользователя для подключения к сервису, выдаётся провайдером.
- ***Пароль учетной записи*** - пароль доступа к учетной записи, выданный провайдером.

Остальные поля носят служебный характер и не требуют изменения.

7.1.3.10.2 Создание Таблицы фильтра для СМС

Для уменьшения затрат на sms-сообщения рекомендуется 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"**
4) Ввести название новой таблицы
5) Отметить только те сообщения, которые **будут** включены в СМС пакет.

7.1.3.10.3 Включение СМС информирования для Ответственного лица

В настройках Ответственного лица предусмотрена возможность SMS информирования. Для того чтобы активировать эту возможность, в карточке учета Ответственного лица необходимо отметить параметр "Включить SMS оповещения" и выбрать таблицу, созданную специально для SMS оповещения.

7.1.4 Реквизиты охранной организации. Вкладка "Тарификация"

Данная вкладка предназначена для специальных проектов и не предназначена для стандартного использования. Если требуется разъяснение по данному функционалу, свяжитесь со службой технической поддержки "КРОС" и задайте свои вопросы.

7.1.5 Реквизиты охранной организации. Вкладка "Календарь"

В настройках ОО предусмотрена возможность корректировки в календаре "Рабочих", "Праздничных", "Предпраздничных" и "Рабочих выходных" и "Выходных" дней. Данный календарь распространяется на все Расписания охраны, всех объектов. Для того чтобы внести изменения в календарь необходимо открыть его на редактирование, нажав иконку "Календарь"

Переключение между месяцами осуществляется с помощью стрелок "Влево"  и "Вправо" . Числа в календаре расположены в столбцах по дням недели:

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

Пн - Понедельник
Вт - Вторник
Ср - Среда
Чт - Четверг
Пт - Пятница
Сб - Суббота
Вс - Воскресенье

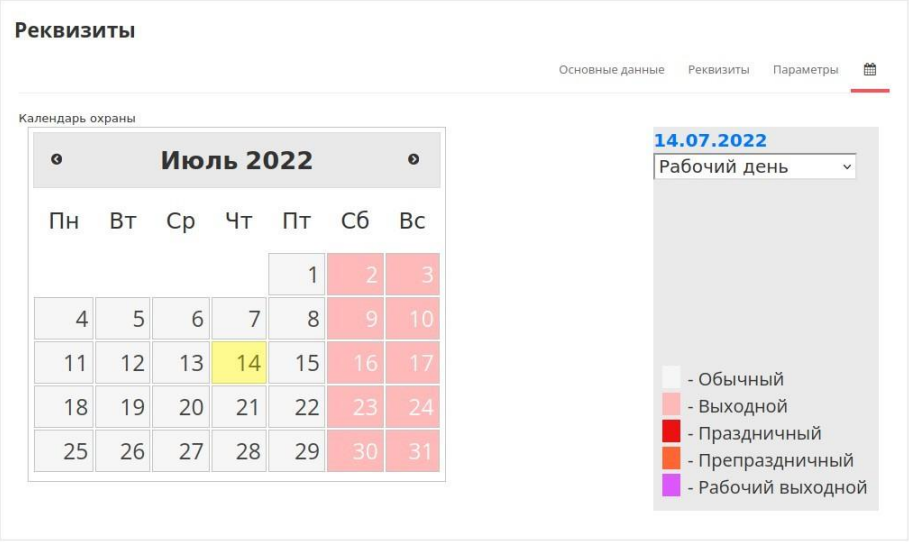
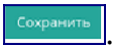


Рис. 90 Календарь. Внешний вид.

Текущая дата будет отображена на жёлтом фоне.

Отредактировать значения дня можно выделив конкретное число. В окне назначения отобразится редактируемая дата, после чего в выпадающем списке нужно выбрать её назначение. Если редактируется выходной день, то в списке появится - **"Рабочий выходной"**. При совпадении праздничного и выходного дней, исключается возможность назначить его "Праздничным". После окончания редактирования календаря необходимо нажать кнопку "Сохранить" 

.

7.1.6 Сохранение, редактирование и удаление данных

После окончания ввода данных требуется нажать кнопку "Сохранить" 

- В случае редактирования данных **Администратором предприятия** достаточно в меню "Охрана" выбрать раздел "Реквизиты".

Карточка учета ОП откроется для редактирования. После чего необходимо нажать "Сохранить" 

.

- В случае, когда необходимо внести изменения в сетевые параметры ОП, необходимо зарегистрироваться в системе под пользователем с правами **"Администратор сервера"** и в таблице ОП выбрать необходимое и открыть его в карточку в режиме "Редактировать" 
.

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

После этого можно вносить необходимые изменения. После чего требуется нажать кнопку "Сохранить" 

- Если никаких изменений вносить не надо, тогда необходимо нажать кнопку "Закрыть" 

- При необходимости исключения ОО, из списка зарегистрированных на данном сервере, необходимо войти в карточку учёта ОО и нажать кнопку "Удалить" 

7.2 Учетные записи

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

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

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

Администратор имеет доступ к учетным записям сотрудников своего охранного предприятия.

7.2.1 Карта пользователя

Учетные записи служат для разграничения прав доступа пользователей.

Чтобы добавить учетную запись нужно уажать на кнопку "Добавить" .

7.2.1.1 Карта пользователя. Вкладка «Идентификация»

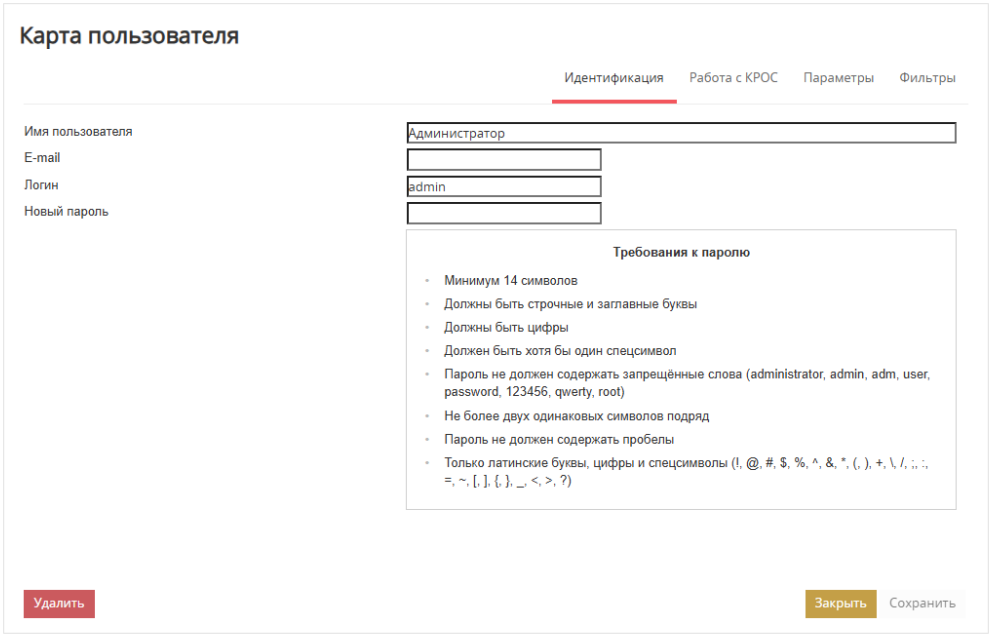


Рис.91 Карта пользователя. Вкладка "Идентификация"

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

На вкладке «Идентификация»(рис. 91) необходимо ввести основные данные сотрудника ОО для его авторизации:

- **Имя пользователя**. Наименование пользователя, или его инициалы, или любое другое его обозначение.
- **Логин**. Уникальное имя пользователя в рамках конкретной ОО.
- **Новый пароль**. Пароль не отображается. При компрометации, его можно изменить на новый. Настоятельно рекомендуется использовать сложные пароли, особенно в том случае когда используется перенаправление порта 9900 из вне.
- **E-mail**(при необходимости). Один из способов связи с пользователем.

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

7.2.1.2 Карта пользователя. Вкладка «Работа в КРОС»

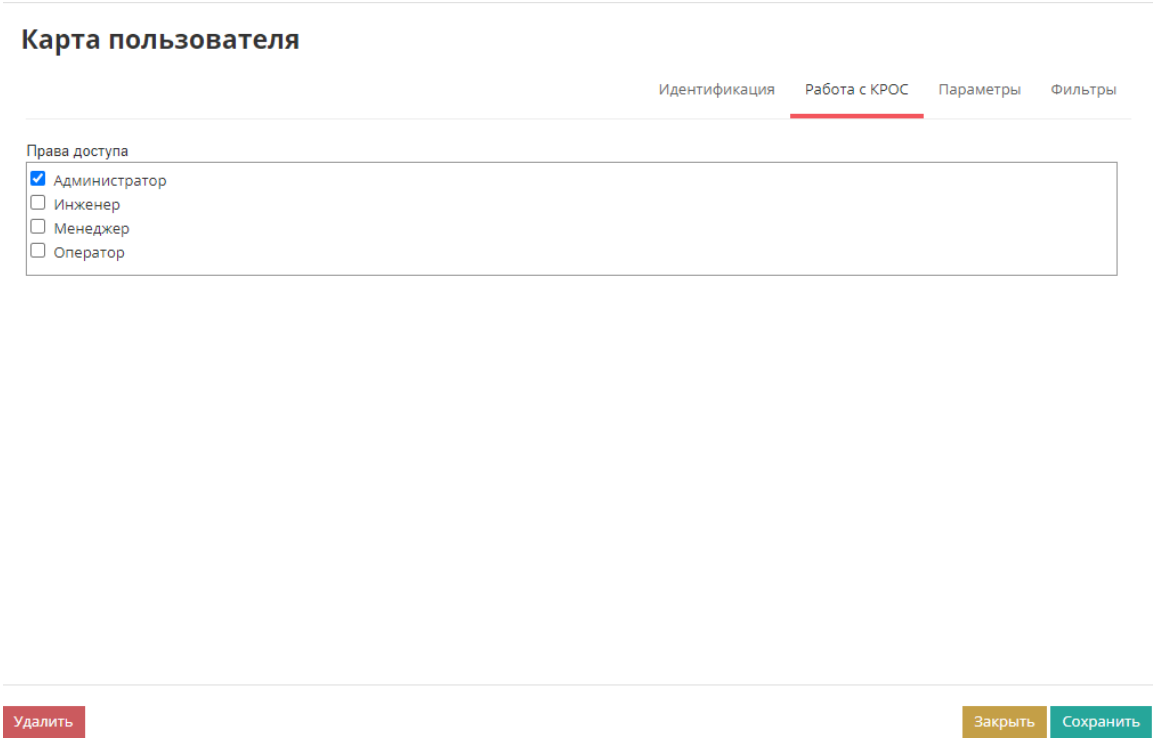


Рис.92 Карта пользователя. Вкладка "Работа в КРОС"

Здесь определяются «Права доступа» пользователя, согласно назначенной ему роли. После активизации вкладки, пользователю задаются права доступа к Web-интерфейсу Сервера-КРОС.

Подробнее про права и роли доступа описано в разделе Роли пользователей и авторизация.

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

7.2.1.3 Карта пользователя. Вкладка «Параметры»

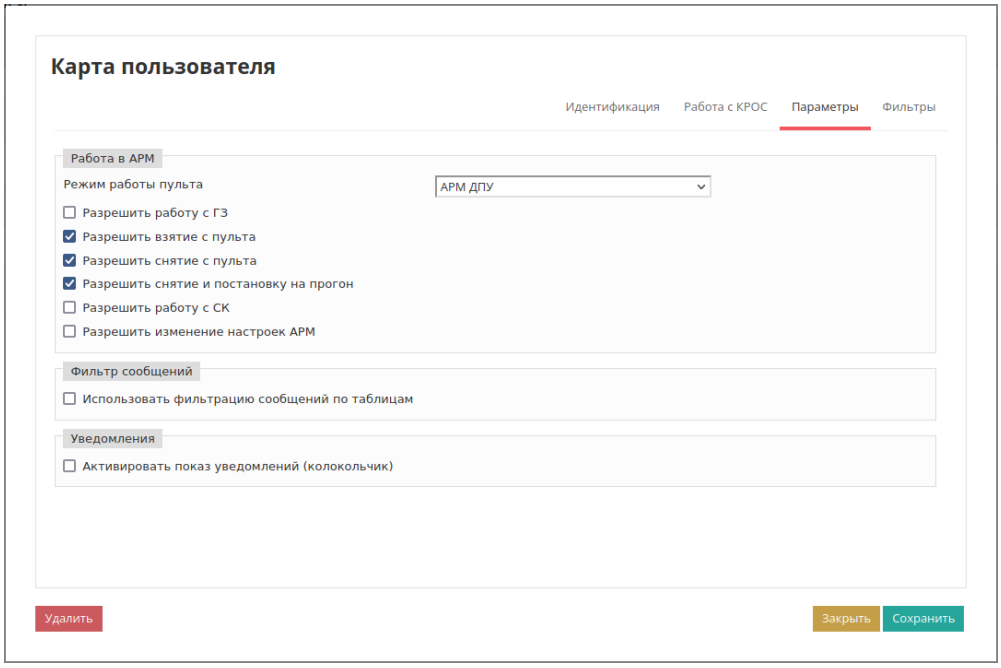


Рис. 93 Карта пользователя. Вкладка "Параметры"

В данной вкладке регулируется взаимодействие пользователя с АРМ.

- **Работа в АРМ:**
- ***Режим работы пульта***. По-умолчанию ***Доступ запрещен***. В выпадающем списке режимов(рис. 94) можно выбрать:

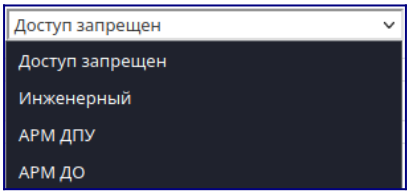


Рис. 94 Выбор разрешений режима работы пользователя

- ***Инженерный*** - режим, исключающий работу с тревожными состояниями и ГЗ.
- ***АРМ ДПУ*** - администратор ОП может назначить пользователю все права, тогда он может полностью заменить дежурного.
- ***АРМ ДО*** Рабочее место дежурного, подразумевается, что только он может принимать решение о вызове ГЗ на объект по тревоге.

Основные параметры режимов работы пульта включают в себя:

- **Разрешить работу с ГЗ** - Разрешить/запретить пользователю работу с ГЗ.
- **Разрешить взятие с пульта** - Разрешить пользователю отправлять команду "Взять объект под охрану".
- **Разрешить снятие с пульта** - Разрешить пользователю снимать объект с охраны.

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

- **Разрешить снятие и постановку на прогон** - Разрешить пользователю использовать режим "технического обслуживания" прибора.
- **Разрешить работу с СК** - Разрешить пользователю работу с ситуационной картой, определение местоположения тревоги и объекта на карте региона и населенного пункта.
- **Разрешить изменение настроек АРМ** - Пользователю разрешается самостоятельно настроить внешний вид АРМ и звуковое оповещение.

- **Уведомления**

♦ **Активировать показ уведомлений (колокольчик)** - позволяет включить/отключить, для конкретного пользователя, возможность индикации внутрисистемных событий:

 - Событий нет

 - Есть информационные сообщения.

 - Есть сообщения, на которые стоит обратить внимание.

 - Есть сообщения, требующие особого внимания.

7.2.1.4 Карта пользователя. Вкладка «Фильтры»

Фильтр объектов для пользователя создается аналогично зоне ответственности в трансляции(рис. 95).

В том случае, когда необходимо ограничить передачу информации по объектам или, когда есть единый центр охраны и от него настраивается передача информации, не связанным между собой конечным потребителям этой информации, в этом случае можно ограничить передачу данных, задав **зону ответственности**.

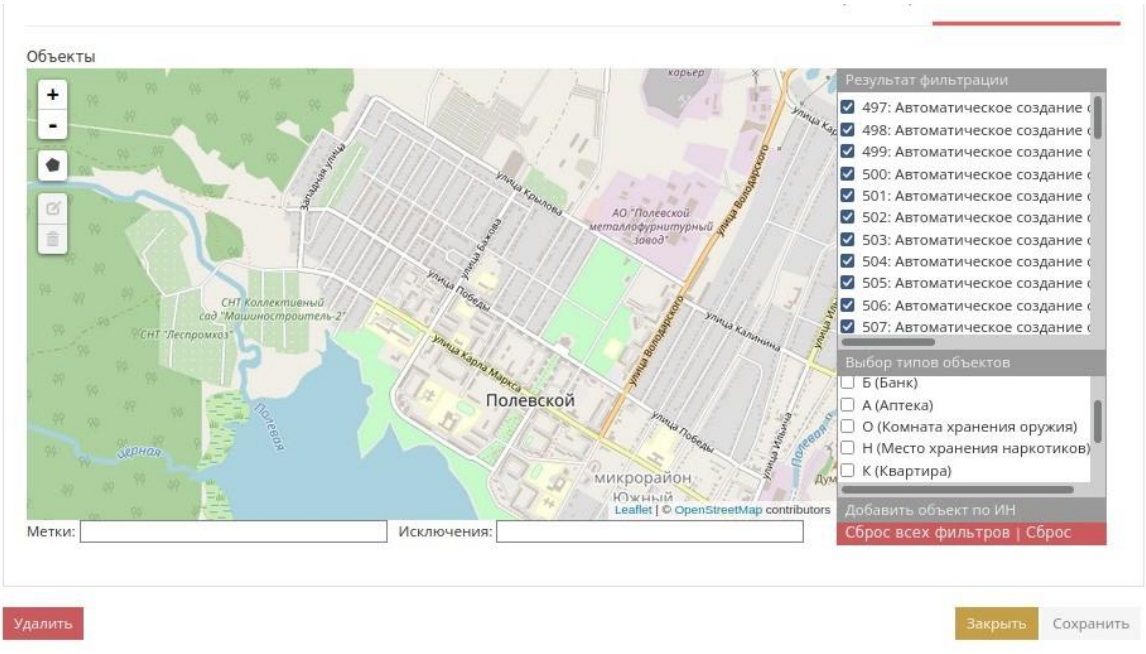


Рис. 95 Карта пользователя. Вкладка "Фильтры"

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

Задать зону ответственности можно несколькими способами:

- **Выбор типов объектов** - использование фильтра позволит выбрать объекты по типу, который был назначен объекту при заполнении карточки объекта. При этом в окне **Результат фильтрации** будут отмечены те объекты, которые отвечают, выбранному типу или типам.
- **Метки** - Несколько объектов, помимо типа, можно объединить в группы используя метки. Если указать эту метку, то объекты с этой меткой попадут в **Результат фильтрации**.
- **Исключения** - объекты с указанной здесь меткой будут исключены из списка **Результат фильтрации**.
- **Выбрать зону ответственности, используя редактор зоны**. Для этого в левой части окна, там где расположена карта, необходимо нажать пиктограмму с пятиугольником и вызвать редактор, создания зоны. Далее, следуя подсказкам рядом с маркером вы создадите зону, после чего в окне **Результат фильтрации** будут отмечены те объекты, которые попали в эту зону. Используя знаки + и - можно увеличить или уменьшить масштаб карты. Можно создать несколько зон ответственности(рис. 96).
  - **Редактировать зону ответственности**. Если есть необходимость редактировать зону ответственности, то в этом случае необходимо нажать на значок **Редактировать**. На карте активируются границы зоны и появятся дополнительные точки, передвигая которые, можно увеличить или уменьшить зону. После окончания редактирования, необходимо нажать надпись **"Сохранить"** или **"Отменить"**, рядом со значком **Редактировать**.
- **Удалить зону ответственности** - если возникла необходимость в удалении зоны ответственности. Необходимо выбрать значок **Удалить** и указать зону, которую надо удалить. После удаления зоны **Результат фильтрации** должен измениться.
- **Сброс всех фильтров** - сбросит все результаты фильтрации.
- **Сброс** - вернет состояние зоны ответственности на значение по-умолчанию.

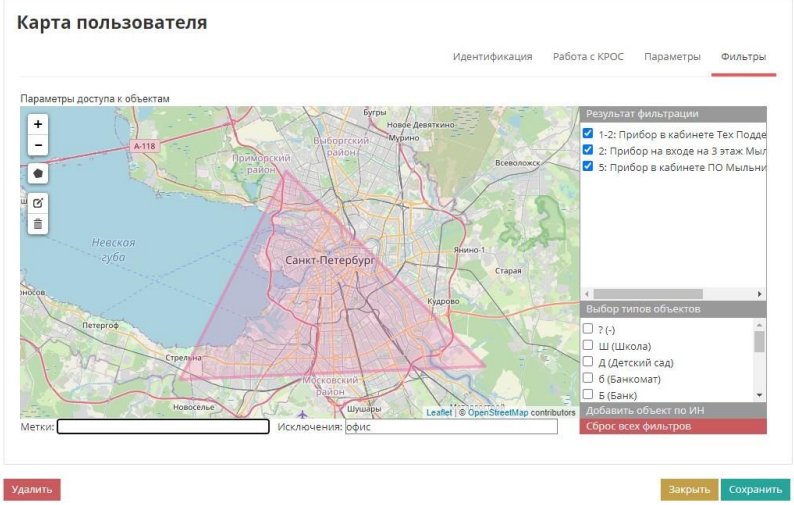


Рис.96 Результат редактирования функционала «Фильтр»

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

При создании зоны ответственности, методы фильтрации можно комбинировать.

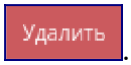
После задания фильтров в окне **Результаты фильтрации** можно дополнительно отметить или снять отметку выделения с объекта. В результате выполненных действий список объектов отображаемых, в АРМ, трансляциях или у пользователя будет ограничен.

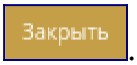
7.2.3 Сохранение, редактирование и удаление учетной записи

Чтобы учетные данные были внесены в БД, необходимо нажать кнопку "Сохранить" 

, расположенную в правом нижнем углу карточки пользователя. Для внесения изменений в учётную запись нужно нажать на кнопку "Редактировать" , расположенную справа от её описания. После чего можно внести изменения и нажать кнопку "Сохранить" 

.

Чтобы удалить учетную запись нужно нажать на кнопку "Редактировать"  учетную запись. И в карточке учета пользователя нажать кнопку "Удалить" 

. Если никаких изменений вносить не надо, карточку пользователя можно просто "Закрыть" 

.

7.3 Группы задержания

В разделе «ГЗ»(рис. 97) (меню «Охрана»→«ГЗ») создаются, редактируются, удаляются ГЗ и задаются параметры их подключение к приложению «Юпитер-ГЗ».

К разделу «ГЗ» по-умолчанию имеют доступ пользователи с правами **Администратор предприятия**, то есть пользователи, которым назначена роль "Администратор".



Рис. 97 Таблица групп задержания

Всего - Отображает общее количество групп задержания

Поиск - Позволяет осуществлять поиск ГЗ по любому известному признаку. Значение столбцов в таблице:

- **Связь с ГЗ**:
  - ▲ - состояние связи с ГЗ не определено. Приложение "Юпитер-ГЗ" ещё не выходило на связь.
  - ▲ - ГЗ не на связи. Приложение "Юпитер-ГЗ" не запущено или экипаж находится вне зоны действия сети, либо не работает мобильный интернет.
  - ▲ - Приложение "Юпитер-ГЗ" работает, экипаж на связи.
- **Номер** - Номер ГЗ. Указываетя при регистрации группы.
- **Наименование** - название ГЗ, принятое в ОП.

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

- **Пароль** - пароль доступа приложения "Юпитер-ГЗ".

7.3.1 Карточка учёта ГЗ

Для регистрации в КРОС новой ГЗ, необходимо нажать на кнопку "Добавить" .

7.3.1.1 Карточка учёта ГЗ. Вкладка «Основное»

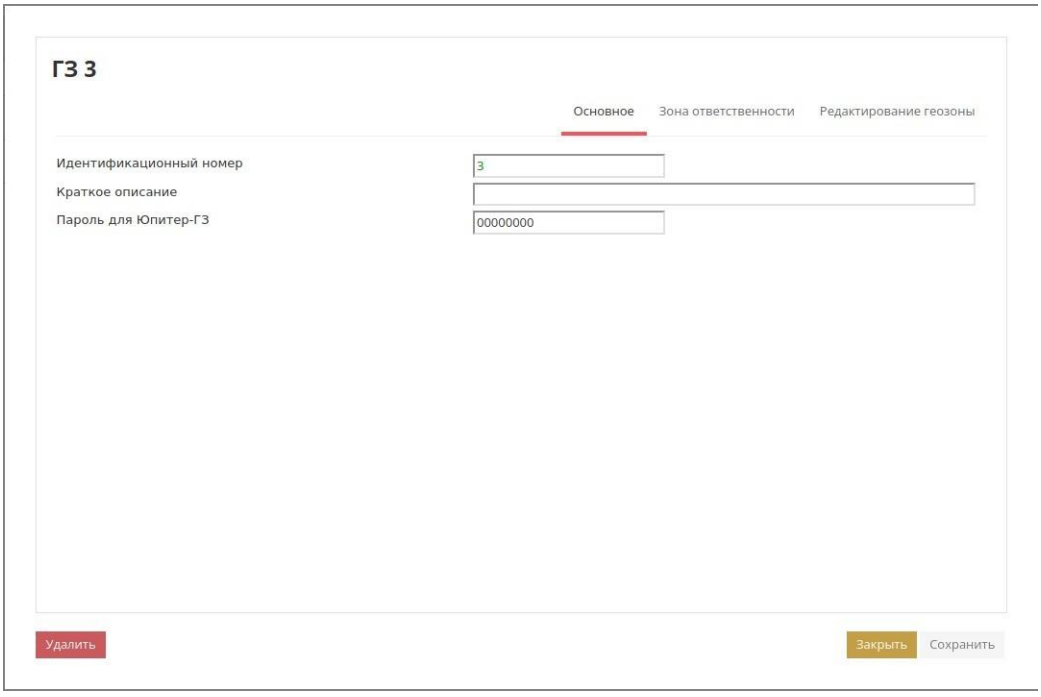


Рис. 98 Карточка учёта группы задержания. Вкладка «Основное»

После открытия карточки регистрации ГЗ(рис. 98), необходимо заполнить следующие поля:

- **Идентификационный номер** - Может быть порядковый номер, или номер экипажа, или номер машины.
- **Краткое описание** - Описание экипажа/наряда, например, ФИО.
- **Пароль для Юпитер-ГЗ** - пароль доступа мобильного приложения "Юпитер-ГЗ".

7.3.1.2 Карточка учёта ГЗ. Вкладка «Зона ответственности»

Зона ответственности настраивается аналогично ***п. 7.2.1.4 Карта пользователя. Вкладка «Фильтры».***

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

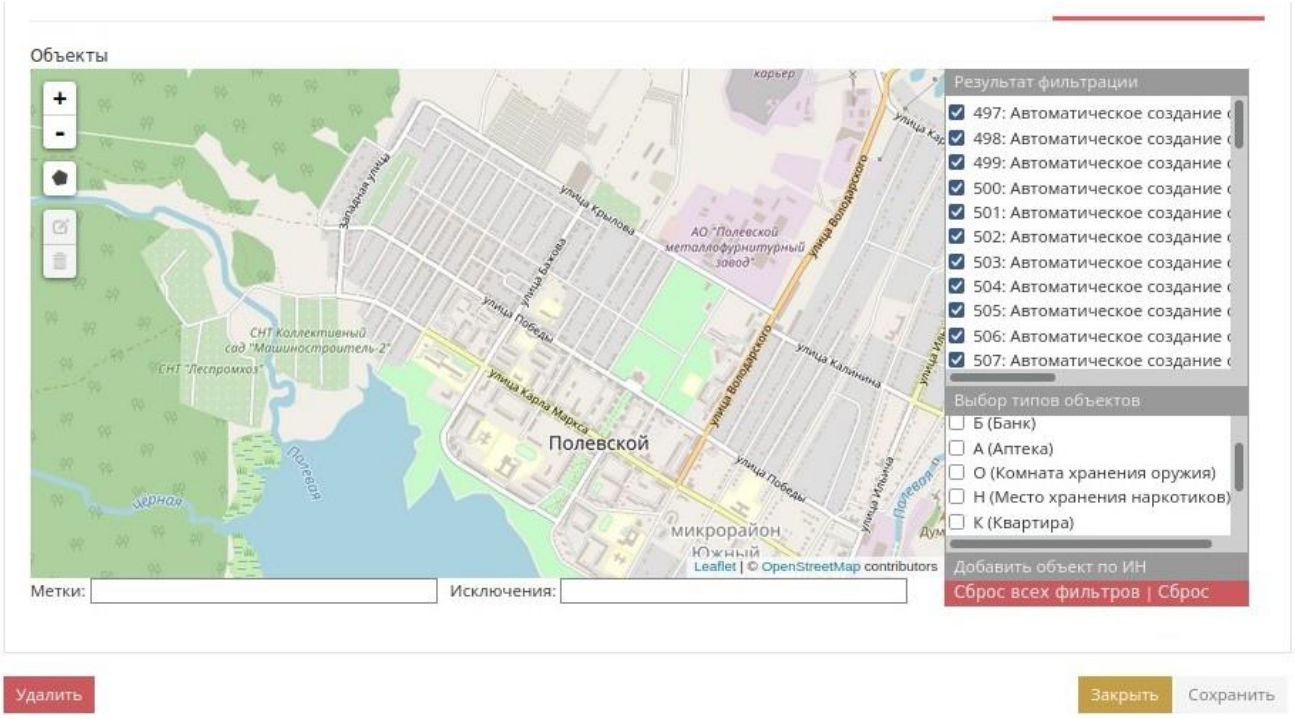


Рис. 99 Определение зоны ответственности

Задать зону ответственности можно несколькими способами(рис. 99):

- **Выбор типов объектов** - использование фильтра позволит выбрать объекты по типу, который был назначен объекту при заполнении карточки объекта. При этом в окне **Результат фильтрации** будут отмечены те объекты, которые отвечают, выбранному типу или типам.
- **Метки** - Несколько объектов, помимо типа, можно объединить в группы используя метки. Если указать эту метку, то объекты с этой меткой попадут в **Результат фильтрации**.
- **Исключения** - объекты с указанной здесь меткой будут исключены из списка **Результат фильтрации**.
- **Выбрать зону ответственности, используя редактор зоны**. Для этого в левой части окна, там где расположена карта, необходимо нажать пиктограмму с пятиугольником и вызвать редактор, создания зоны. Далее, следуя подсказкам рядом с маркером вы создадите зону, после чего в окне **Результат фильтрации** будут отмечены те объекты, которые попали в эту зону. Используя знаки + и - можно увеличить или уменьшить масштаб карты. Можно создать несколько зон ответственности.
  - **Редактировать зону ответственности**. Если есть необходимость редактировать зону ответственности, то в этом случае необходимо нажать на значок **Редактировать**. На карте активируются границы зоны и появятся дополнительные точки, передвигая которые, можно увеличить или уменьшить зону(рис. 100). После окончания редактирования, необходимо нажать надпись **"Сохранить"** или **"Отменить"**, рядом со значком **Редактировать**.

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

- **Удалить зону ответственности** - если возникла необходимость в удалении зоны ответственности. Необходимо выбрать значок **Удалить** и указать зону, которую надо удалить. После удаления зоны **Результат фильтрации** должен измениться.
- **Сброс всех фильтров** - сбросит все результаты фильтрации.
- **Сброс** - вернет состояние зоны ответственности на значение по-умолчанию.

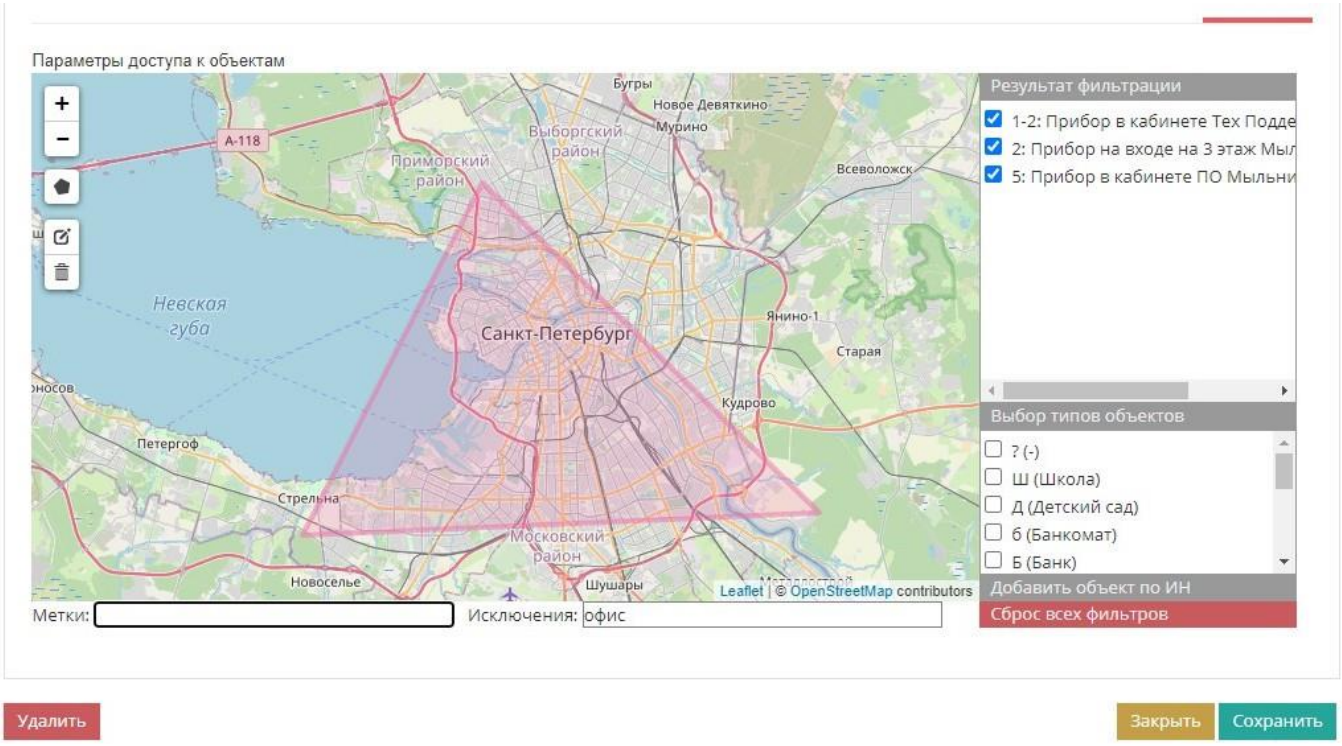


Рис. 100 Результат редактирования зоны ответственности

После задания фильтров в окне **Результаты фильтрации** можно дополнительно отметить или снять отметку выделения с объекта. В результате выполненных действий список объектов отображаемых, в АРМ, трансляциях или у пользователя будет ограничен.

7.3.1.1 Карточка учёта ГЗ. Вкладка «Редактирование геозоны»

Данная вкладка позволяет настроить геозону, за которой закреплена группа быстрого реагирования, и объекты, охраны в этой зоне расположенные. Геозона создается аналогично зоне ответственности, а именно с использованием редактора зон(рис. 101):

- Для этого в окне, там где расположена карта, необходимо нажать пиктограмму с пятиугольником и вызвать редактор, создания зоны. Далее, следуя подсказкам рядом с маркером создаётся зона. Используя знаки + и - можно увеличить или уменьшить масштаб карты. Можно создать несколько геозон.
- Если необходимо отредактировать геозону, то в этом случае необходимо нажать на значок **Редактировать**. На карте активируются границы зоны и появятся дополнительные точки,

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

передвигая которые, можно увеличить или уменьшить зону. После окончания редактирования, необходимо нажать надпись **"Сохранить"** или **"Отменить"**, рядом со значком **Редактировать**.

- Для удаления геозоны, необходимо выбрать значок **Удалить** и указать зону, которую надо удалить.

При необходимости, можно использовать контроль, нахождения ГЗ в геозоне. Для этого необходимо разрешить:

- **Контроль входа в геозону**
- **Контроль выхода из геозоны**

При этом в АРМ будут приходить сообщения когда ГЗ покинула зону контроля или вернулась ав неё.

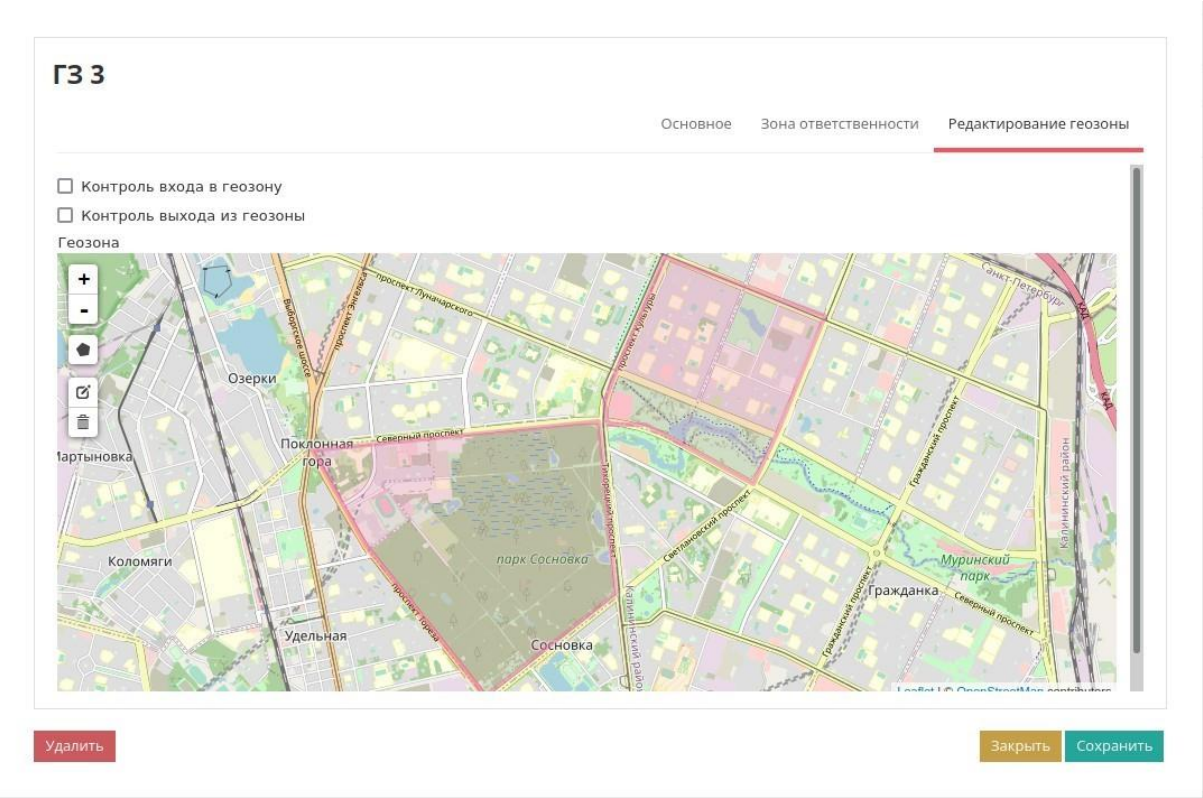


Рис. 101 Результат редактирования геозоны

7.3.2 Сохранение, Редактирование и Удаление записи о ГЗ

После настройки всех пунктов, нажать «Сохранить» Сохранить в нижней части окна «ГЗ». Чтобы закрыть окно «ГЗ» без сохранения, нужно щелкнуть по кнопке «Закрыть» Закрыть.
Для изменения данных, нажать "Редактировать" в строке с записью ГЗ, после чего нажать «Сохранить» Сохранить.

Для удаления записи о ГЗ, нажать "Редактировать" и затем "Удалить" Удалить.

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

8. Меню «Администрирование»

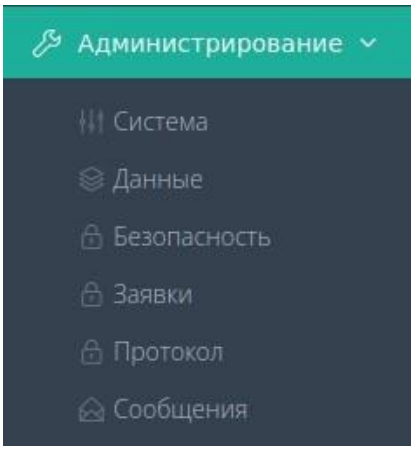


Рис. 102 Меню «Администрирование»

Меню "Администрирование"(рис. 102) содержит настройки системы общие для всех ОП, зарегистрированных на конкретном сервере КРОС. Для пользователя с правами "Администратор сервера" доступны все разделы меню.

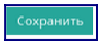
Пользователю обладающему правами "Администратора предприятия" доступны "Справочники", "Протокол" и "Сообщения". Остальным пользователям данные разделы могут быть недоступны.

8.1 Администрирование. 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.

В окне «Система» (меню «Административные»→«Система») производится обновление и перезапуск сервера КРОС - доступно "Администратору сервера", а также настройка SMTP и HTTP -серверов - доступно "Администратору предприятия".

К окну «Система» имеет доступ только пользователи с ролью - **Администратор сервера**.

После внесения изменений необходимо "Сохранить" 

данные и перезагрузить сервер КРОС.

!!!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.

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

8.1.1 Система. Вкладка «Сервер»

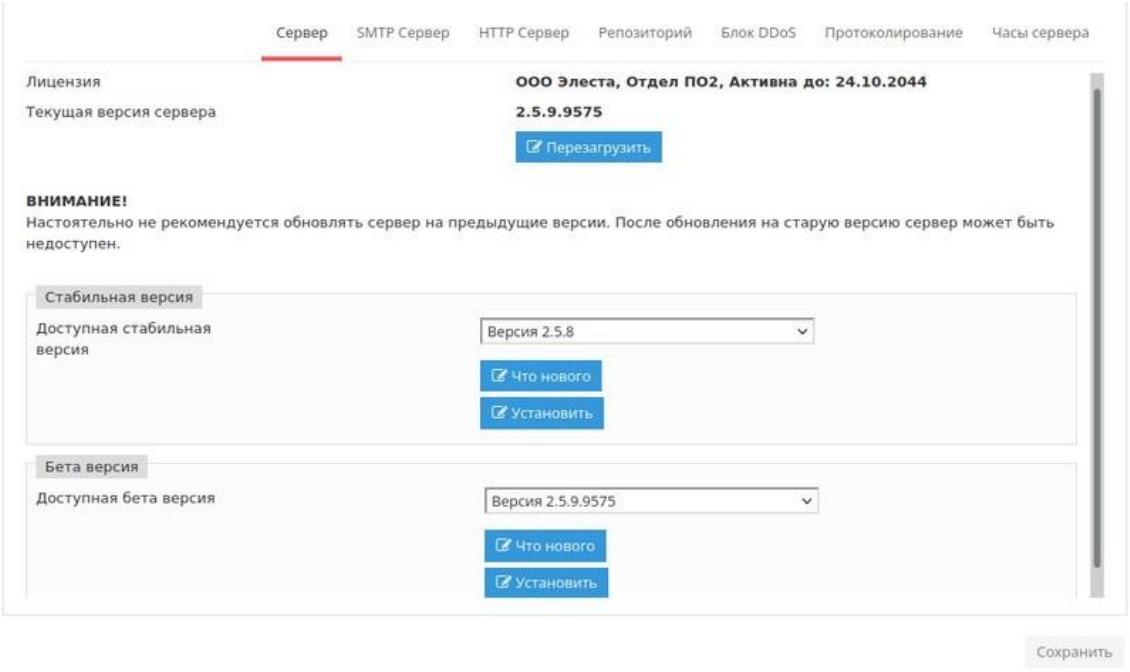


Рис. 103 Система. Вкладка «Сервер»

!!!Внимание!!! Перед обновлением сервера, рекомендуется сделать резервную копию как базы данных, так и самого установленного сервера "КРОС", скопировав целиком папку, находящуюся по адресу ***/usr/local/smpo-server*** в любое удобное место. Таким образом, при неуспешном обновлении всегда будет возможность откатить версию сервера на последнюю рабочую.

Раздел содержит основную информацию о лицензии и версии сервера КРОС.

- **Лицензия** - Информация о текущей активной лицензии: на какую организацию зарегистрированна лицензия, её тип и срок её действия, либо её отсутствие.
- **Текущая версия сервера** - Текущая работающая версия сервера КРОС. Если номер версии отображается **красным цветом**, значит версию КРОС можно обновить.
- Кнопка **Перезагрузка** - Операция перезагрузки сервера, позволяет перезагрузить сервис ПО КРОС, отдельно от перезагрузки ОС. Компьютер, на котором установлен сервер, не перезапускается.

При запуске процедуры обновления ПО, в окне КРОС должна появиться информация, отображающая процесс скачивания данных. Так же информация дублируется в информационной строке внизу рабочего экрана КРОС.

- 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.

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

- **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.

- Бета версия

Информация о доступном обновлении бета версии. Этот раздел отображается только в случае если активная лицензия КРОС имеет доступ к данному функционалу. Фактически это доступ к версии КРОС после исправления ошибок и внесения дополнений.

- **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.

8.1.2 Система. Вкладка «Вкладка «SMTP сервер»

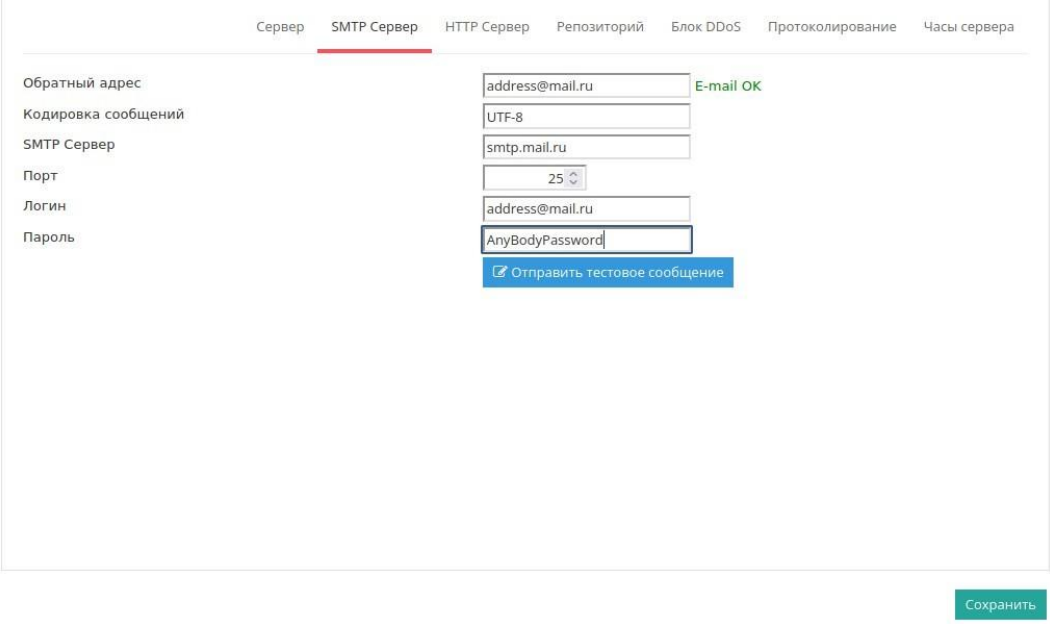


Рис.103 Система. Вкладка «Вкладка «SMTP сервер»

Во вкладке «SMTP сервер»(рис. 103) производится настройка параметров для отправки сообщений через SMTP сервер . Необходимо учитывать, что данные указываются для сервера КРОС и "Администратор предприятия" не имеет прав на его замену.

Для настройки SMTP сервера необходимо указать:

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

- **Обратный адрес** - e-mail адрес, с которого будут отправляться сообщения. Сообщение ***E-mail OK*** - сообщает, что формат, указанного адреса верен, **сервер КРОС не проверяет адрес на его существование**.
- **Кодировка сообщений** - нужно указать название кодировки. По-умолчанию, указывается универсальная кодировка UTF-8. При желании можно указать другие кодировки, например, windows-1251 или KOI-8.
- **SMTP-сервер** - указывается адрес SMTP-сервера, от которого будут приходить сообщения. Как правило, это SMTP сервер того же поставщика услуг, электронную почту которого вы указали в поле "Обратный адрес".
- **Порт** - указывается порт SMTP-сервера. Как правило - 25 или 465.
- **Логин** и **Пароль** - указываются логин и пароль для авторизации на SMTP-сервере.

После заполнения формы можно нажать кнопку **"Отправить тестовое сообщение"**, для проверки корректности введенных данных. Для сохранения настроек, нужно нажать кнопку «Сохранить» 

.

После настройки SMTP-сервера, в настройках Охранной организации, Реквизиты - Вкладка «Основные данные», пользователь с правами "Администратор сервера" может отправить регистрационную информацию на указанный адрес, нажав кнопку 

. С помощью данной функции, на указанный E-mail, будет отправлено электронное письмо, со следующей информацией:

- 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 Сервер-КРОС).

8.1.3 Система. Вкладка «Вкладка «HTTP сервер»

Во вкладке «HTTP сервер»(рис. 104) происходит настройка параметров HTTP-сервера. HTTP и HTTPS сервер является неотъемлемой частью сервера КРОС и используется для построения WEB-интерфейсов системы администрирования.

Таким образом, приведенные ниже настройки 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, для этого требуются дополнительные сетевые настройки, 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.

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

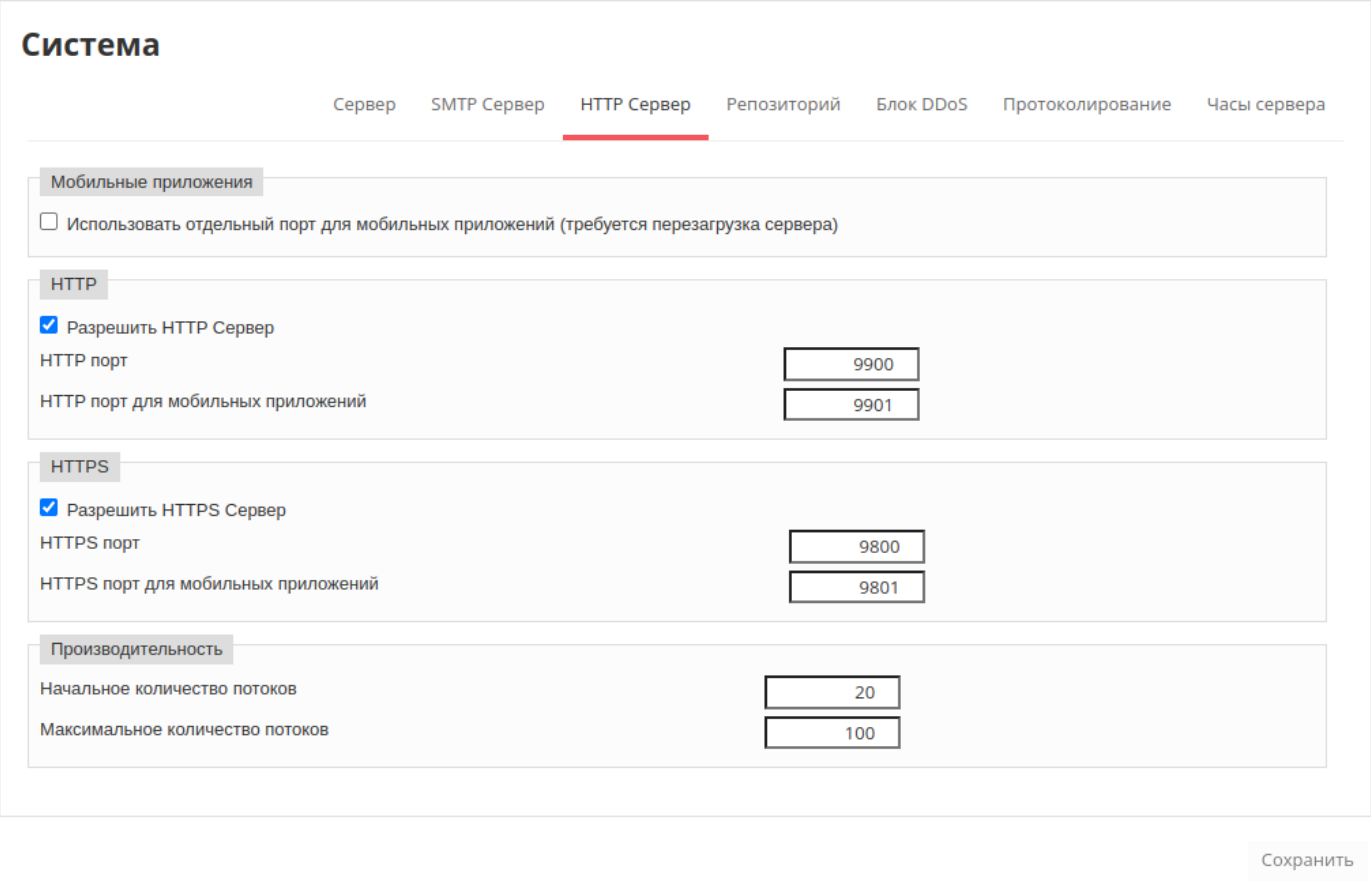


Рис.103 Система. Вкладка «Вкладка «HTTP сервер»

- ***Мобильные приложения***

- **Использовать отдельный порт для мобильных приложений (требуется перезагрузка сервера)** - Позволяет выполнить настройки КРОС для использования отдельного порта, обслуживающего мобильные приложения. По-умолчанию для обслуживания мобильных приложений используется порт 9900. Так как контроль работы драйверов мобильных приложений происходит на уровне лицензирования, обслуживание мобильных приложений будет происходить даже при отключенных серверах HTTP и HTTPS.

- ***HTTP***

- **Разрешить HTTP сервер** - Разрешить работу HTTP сервера, как неотъемлемой части КРОС. HTTP сервер будет запущен при старте КРОС.
  - **HTTP Порт** - указывается номер порта TCP по которому WEB интерфейс КРОС и API HTTP драйверов будет доступны по протоколу HTTP. При смене ***Порта*** необходимо перезагрузить сервер КРОС.
  - **HTTP порт для мобильных приложений** - позволяет назначить отдельный порт обслуживающий мобильные приложения. Эта настройка будет использоваться даже в том случае, когда использование HTTP сервера не разрешено.

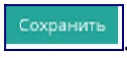
SEC.RU | Короткий путь к информации Скачано с sec.ru

- ***HTTPS***

- **Разрешить HTTPS сервер** - Разрешить работу сервера по протоколу HTTPS с поддержкой SSL-сертификата как неотъемлемой части КРОС. HTTPS сервер будет запущен при старте КРОС. Необходимо учитывать, что в ряде браузеров необходимо разрешить SSL-сертификат сервера КРОС.
  - **HTTPS Порт** - указывается номер порта TCP по которому WEB интерфейс КРОС и API HTTP драйверов будет доступны по протоколу HTTPS. При смене ***Порта*** необходимо перезагрузить сервер КРОС.
  - **HTTPS порт для мобильных приложений** - позволяет назначить отдельный порт обслуживающий мобильные приложения. эта настройка будет использоваться даже втом случае, когда использование HTTPS сервера не разрешено.

- ***Производительность***

- **Производительность** - отвечает за обработку запросов по протоколам HTTP и HTTPS.
- **Начальное количество потоков** - минимальное количество потоков, которые сервер КРОС может обработать с момента старта.
- **Максимальное количество потоков** - максимальное количество потоков, которые сервер КРОС может обработать в единицу времени. Если потоков больше, то в этом случае КРОС формирует очередь входящих сообщений.

Для сохранения изменений нужно нажать кнопку «Сохранить» 

.

8.1.4 Система. Вкладка «Вкладка «Репозиторий»

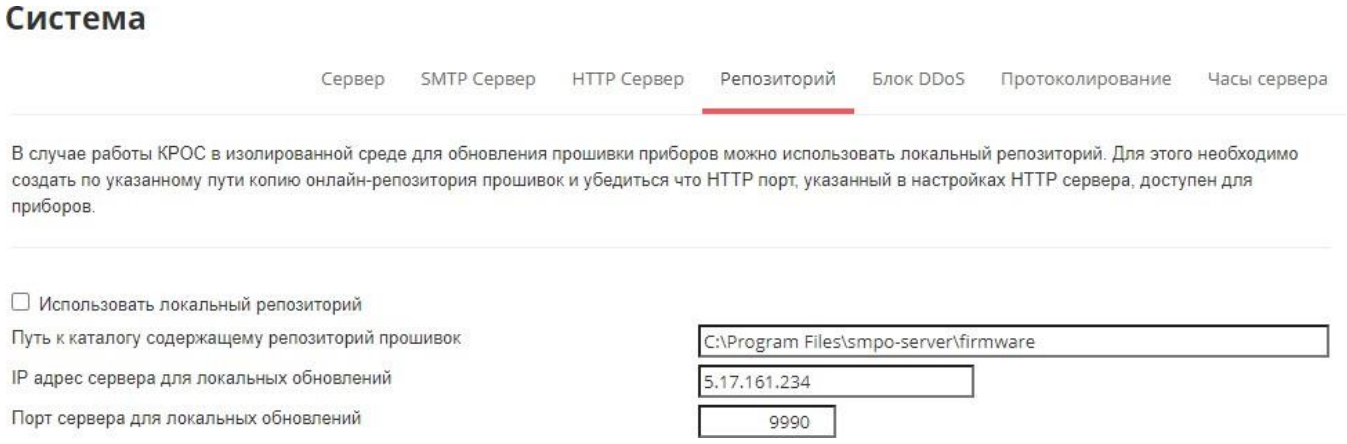


Рис. 104 Система. Вкладка «Вкладка «Репозиторий»

Для возможности обновления ПО приборов удаленно, предусмотрена возможность настройки репозитория прошивок(рис. 104). В случае, когда сервер КРОС имеет выход в интернет, необходимо, чтобы галочка **"Использовать локальный репозиторий"** была снята. Если она установлена, необходимо ее снять, и перезагрузить сервер КРОС.

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

В случае работы КРОС в изолированной среде для обновления ПО 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. Для уточнения данных по запросу можно отправить e-mail.

Для настройки локального репозитория предусмотрены следующие параметры:

- **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. Полный путь к папке репозитлрия по-умолчанию: В **Windows** - ***"C:\Program Files\smpo-server\firmware***; В **Linux** - ***"/usr/local/smpo-server/firmware"***.
- **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, если приборы подключаются через VPN, прокси-сервер или в локальной сети. В общем случае, здесь нужно указать адрес, используемый в настройках IP соединения приборов.
- **Порт сервера для локальных обновлений** - Порт, по которому сервер КРОС раззешает доступ приборов к репозиторию прошивок.

Структура репозитория должна совпадать с репозиторием компании ООО «Элеста». Для уточнения информации необходимо связаться со службой технической поддержки.

8.1.5 Система. Вкладка «Вкладка «Блок DDos»

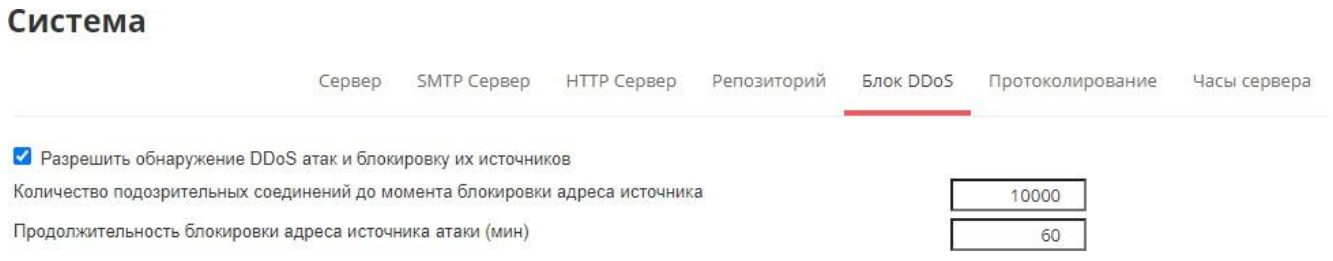


Рис. 105 Система. Вкладка «Вкладка «Блок DDos»

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

КРОС содержит базовый функционал для обнаружения DDoS атак и временной блокировки их источников(рис. 105). Система обработки входящих соединений контролирует и фиксирует для каждого адреса отправителя количество пакетов, не обработанных ни одним из драйверов-приемников.

Если это количество, необработанных пакетов, превысит установленный лимит - данные от зафиксированного адреса перестают приниматься в течении установленного периода времени. За это отвечают следующие параметры:

- **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.

8.1.6 Система. Вкладка «Вкладка «Протоколирование»

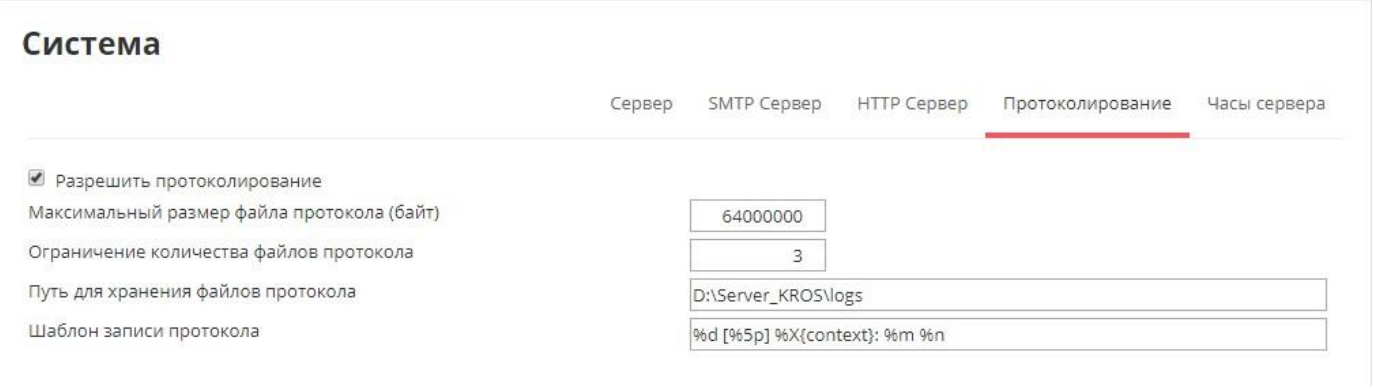


Рис. 106 Система. Вкладка «Вкладка «Протоколирование»

На сервере предусмотрено создание лог файлов как самого сервера, так и всех его драйверов.

В данной вкладке есть возможность задать параметры работы с логами(рис. 106):

- **Максимальный размер файла протокола(байт)** - указывается размер каждого файла логирования, который записывается в байтах. По-умолчанию 64Мбайт.
- **Количество хранимых файлов протокола** - сколько файлов логирования, достигших максимального размера, хранить системе.
- **Путь для хранения логов** - По-умолчанию лог-файлы записываются в подкаталог "logs", корневого каталога, установленного сервера КРОС. Данный параметр можно изменить на принятый в ОС или любой другой, удобный администратору системы.
- **Шаблон записи протокола** - формат записи информационных сообщений в файлы логирования.
- После изменения настроек рекомендуется перезапустить сервер КРОС.

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

В **ОС Windows** файлы логирования по-умолчанию записываются в ***"C:\Program Files\smpo-server\logs"***.

В **ОС Linux** по-умолчанию лог-файлы записываются в ***"/usr/local/smpo-server/logs"***. В серверах, поставляемых по Государственным контрактам путь хранения лог-файлов может быть - ***"/mnt/hdd/logs"***.

8.1.7 Система. Вкладка «Вкладка «Часы сервера»



Рис. 107 Система. Вкладка «Вкладка «Часы сервера»

Сервер КРОС имеет возможность работать с разными серверами синхронизации времени Они могут быть как **глобальными**, так и **частными**.

- **Разрешить синхронизацию времени** - Разрешения синхронизации времени на уровне сервера КРОС. В этом случае КРОС постарается проигнорировать системные настройки ОС и синхронизировать время внутри системы согласно настроек ОО.
- **Синхронизировать часы сервера перед стартом** - Запустить процесс синхронизации системных часов до запуска основного модуля ПО.
  - **Период синхронизации (сек)** - установить временной интервал, по истечении которого будет осуществлена синхронизация времени.
  - **Список серверов времени** - Сервера времени добавляются через запятую. Можно вводить как имя сервера, так и IP адрес.

Преимущества синхронизации времени с серверами, чем с локальным временем в том, что появляется возможность работать с разными часовыми поясами.

Сервер КРОС при работе не использует системное время, оно отображается только в логе сервера и при записи событий.

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

8.2 Администрирование. Данные

Во вкладке «Данные» (меню «Административные»→«Данные») производится настройка базы данных, а так же система резервного копирования и система очистки БД.

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

8.2.1 Данные. Вкладка «SQL Сервер»

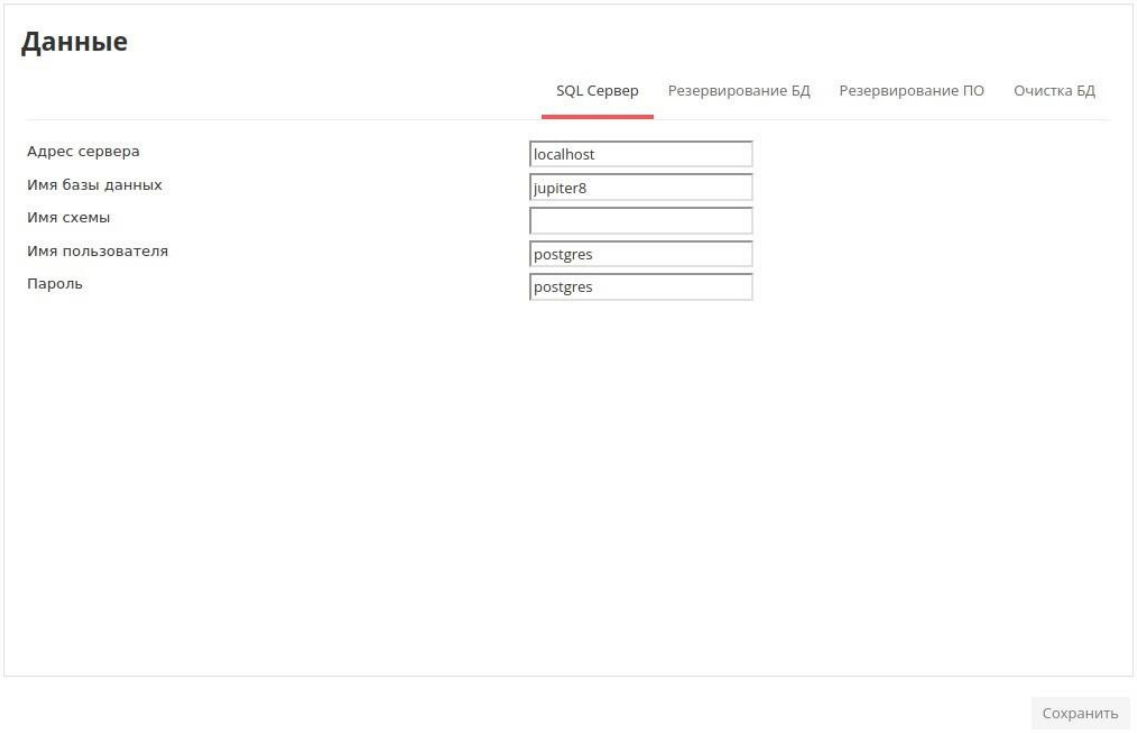


Рис. 108 Данные. Вкладка «SQL Сервер»

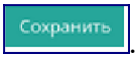
Во вкладке «SQL Сервер»(рис. 108) производятся настройки доступа к серверу баз данных. После изменения параметров сервер КРОС требует обязательной перезагрузки. Предполагается работа с сервером PostgreSQL.

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 требуется изменить название базы данных, на отличное от стандартного.

- **Адрес сервера** - IP адрес или доменное имя компьютера, на котором устоновлен сервер SQL. По умолчанию используется порт ***5432***. Если необходимо использовать другой порт - то он указывается через двоеточие, например ***localhost:5433***.
- **Имя базы данных** - Основная база данных КРОС. По умолчанию ***jupiter***.
- **Имя схемы** - Схема в контексте базы данных PostgreSQL. По умолчанию используется ***public***, поэтому имя схемы можно не указывать.

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

- **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» 

. Чтобы изменения вступили в силу необходимо перезагрузить сервер КРОС.

8.2.2 Данные. Вкладка «Резервирование БД»

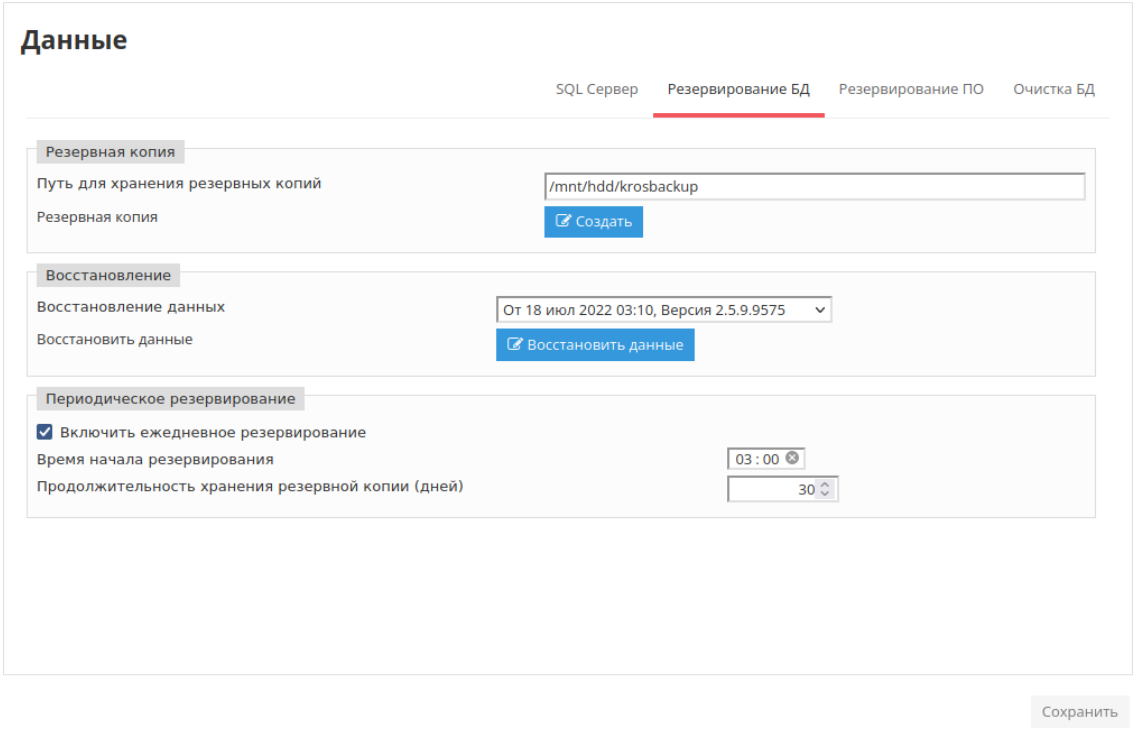


Рис. 109 Данные. Вкладка «Резервирование БД»

В данной вкладке задаются параметры создания резервной копии БД(рис. 109).

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.

Следует учитывать различия резервных копий базы данных и версий сервера.

Так же, обращаем Ваше внимание на тот факт, что ОС **Astra Linux «Смоленск»**, в работе с данными использует механизм мандатных меток, что вносит специфику при восстановлении данных(восстановление возможно только в ОС **Astra Linux «Смоленск»**).

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

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

КРОС в целом, в том числе и за версию сервера. Не сохраняет данные (договора, объекты, приборы и т.д).

- Резервная копия

Отображает парамерты, определяющие системные настройки резервирования и восстановления БД. Перед созданием резервной копии или восстановлением БД, необходимо настроить ряд параметров:

· **Путь для хранения резервных копий** - По-умолчанию, для Windows - "C:\Program Files\ smpo-server\backup", в Linux - "/usr/local/smpo-server/backup" или "/mnt/hdd/krosbackup". Настоятельно рекомендуем использовать для резервных копий отдельный дисковый накопитель.Существует возможность указать несколько разных путей для создания резервных копий, для этого перечислите необходимые пути через запятую.

· **Резервная копия** - Кнопка "Создать", позволяет создать резервную копию БД вне расписания. Перед обновлением версии КРОС обязательно необходимо сделать резервную копию БД.

- Восстановление

Выбор архива БД и запуск процесса восстановления:

- **Восстановление данных** - в выпадающем списке необходимо выбрать бэкап БД, который необходимо восстановить. Обратите внимание, что это не обязательно будет архив с последней датой. После восстановления работы КРОС обратите внимание, чтобы версия КРОС и версия бэкапа совпадали.
- **Восстановить данные** - выполнить операцию восстановления. После этого система запустит процесс восстановления и предложит перегрузить КРОС, необходимо согласиться. Скорость восстановления информации зависит от объема информации в бэкапе.

Для того, чтобы программа корректно обсчитывала статусы приборов и объектов, после восстановления БД, необходимо временно выключит "Зеркалирование" на всех компьютерах, если таковое используется. Затем на основном сервере, для каждой охранной организации, необходимо зарегистрироваться под каждым администратором ОО, выполнить следующую команду в браузере:

```
IP.адрес.сервера.КРОС:порт/query/forcenest
```

После окончания процедуры в браузере появится сообщение - "ОК".
Теперь можно включить "Зеркалирование" на всех компьютерах.

- Периодическое резервирование

Позволяет создавать резервные копии базы данных в автоматическом режиме

- **Включить ежедневное резервирование** - Позволяет создать задачу суточного резервного копирования БД.

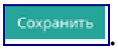
SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Время начала резервирования** - Рекомендуется выбрать такое время, когда нагрузка на систему минимальна? Как правило это вторая половина ночи, по-умолчанию, установлено время текущей временной зоны - 3:00.
- **Продолжительность хранения резервной копии** - устанавливается временной интервал в течении которого система должна хранить резервные копии.

По умолчанию время хранения составляет 30 дней. Файлы старше, указанного срока, удаляются автоматически. Если при установке новой версии или восстановлении работы КРОС, в каталоге резервного копирования находятся файлы, созданные раннее указанного срока, от даты запуска ПО, то такие файлы будут удалены при создании очередной резервной копии БД.

!!!Внимание!!!

По регламенту работы с системами БД, необходимо предусмотреть хранение их долгосрочных архивов. Например, на внешних носителях, с периодичностью обновления один раз в месяц или один раз в неделю. Так же, возможно настроить хранение долгосрочных резервных копий на сетевых ресурсах(в пределах локальной сети).

После выставления всех настроек нажать кнопку "Сохранить" 

. После этого резервные копии начнут создаваться согласно установленным настройкам.

8.2.2 Данные. Вкладка «Резервирование ПО»

8.2.2.1 Резервирование средствами КРОС

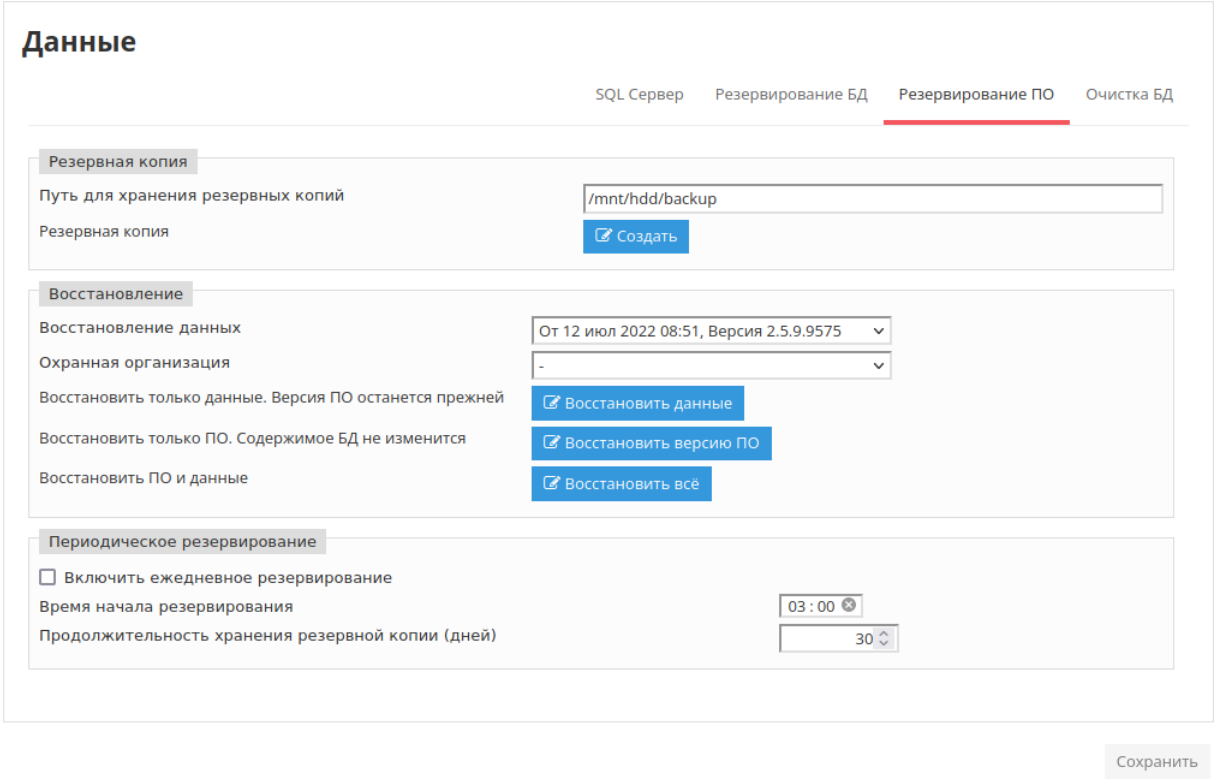


Рис. 110 Данные. Вкладка «Резервирование ПО»

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

Создать резервную копию ПО можно двумя способами: средствами самого сервера КРОС и в ручную(рис. 110).

Данный способ создания резервной копии позволяет сделать архив текущей версии ПО и всей структуры сервера , а так же делает выгрузку БД в файл формата ".xml". Для создания резервной копии ПО, в сервере КРОС предусмотрены параметры:

- Резервная копия

- **Путь для хранения резервных копий** - Место хранения резервной копии ПО. По-умолчанию, резервная копия ПО записывается: в Windows - "C:\Program Files\smpo-server\backup"; в Linux - "/usr/local/smpo-server/backup" или "/mnt/hdd/backup". Так же можно изменить путь по-умолчанию, указав новое место хранения резервной копии, в формате ОС.
- **Резервная копия** - Нажав кнопку "Создать", можно сделать архив ПО вне расписания.

- Восстановление

Если путь хранения резервных копий указан корректно, то в этом случае система восстановдения данных сама найдет, созданные ранее резервные копии. Для восстановления данных необходимо задать следующие параметры:

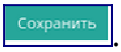
- **Восстановление данных** - в выпадающем списке нужно выбрать ту резервную копию, которую необходимо восстановить.
- **Охранная организация** - Так как выгрузка БД происходит по всем ОО, предлагается сделать выбор, данные какой ОО необходимо восстановить.
- **Восстановить только данные. Версия ПО останется прежней** - После нажатия на кнопку "Восстановить данные", система восстановит данные, по выбранной ОО. Предыдущие данные будут уничтожены.
- **Восстановить только ПО. Содержимое БД не изменится**- При нажатии на кнопку "Восстановить версию ПО", система восстановит ПО из резервной копии. Данная процедура крайне не желательна на действующей БД, так как возможны процессы связанные с внутренней организацией работы ПО. Процедуру восстаг=новления ПО можно делать, либо на пустой БД, либо в том случае, когда что-то перестало работать.
- **Восстановить ПО и данные** - После выбора "Восстановить все", произойдет полное восстановление данных, по выбранной ОО.

- Периодическое резервирование

- **Включить ежедневное резервирование** - включение данной опции, позволяет настроить автоматическое создание резервной копии ПО.
- **Время начала резервирования** - Рекомендуется выбрать такое время, когда нагрузка на систему минимальна? Как правило это вторая половина ночи, по-умолчанию, установлено время текущей временной зоны - 3:00.

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

- **Продолжительность хранения резервной копии** - По умолчанию время хранения составляет 1 месяц

После выставления всех настроек нажать кнопку "Сохранить" 

. После этого резервные копии начнут создаваться согласно установленным настройкам.

8.2.2.2 Резервирование ПО средствами ОС

- Создание резервной копии версии сервера

Перед обновлениями версии сервера КРОС рекомендуется делать резервную копию папки с ПО сервера, чтобы в случае неуспешного обновления можно было подменить файлы, и запустить старую, работавшую до обновления версию.

Пример, создания резервной копии ПО для ***ОС Astra Linux***: Сделать это проще всего запустив файловый менеджер от имени суперпользователя и выполнил архивирование папки по адресу /usr/local/smpo-server.

1. Необходимо открыть терминал *fly-terminal* и выполнить команду остановки сервера КРОС: ***sudo /etc/init.d/smpo-server stop*** или ***sudo service smpo-server stop***.
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**

- Восстановление резервной версии версии сервера

Восстановление версии сервера из резервной копии требуется, на примере Astra Linux:

1. Необходимо открыть терминал *fly-terminal* и выполнить команду остановки сервера КРОС: ***sudo /etc/init.d/smpo-server stop*** или ***sudo service smpo-server stop*** .
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 Данные. Вкладка «Очистка БД»

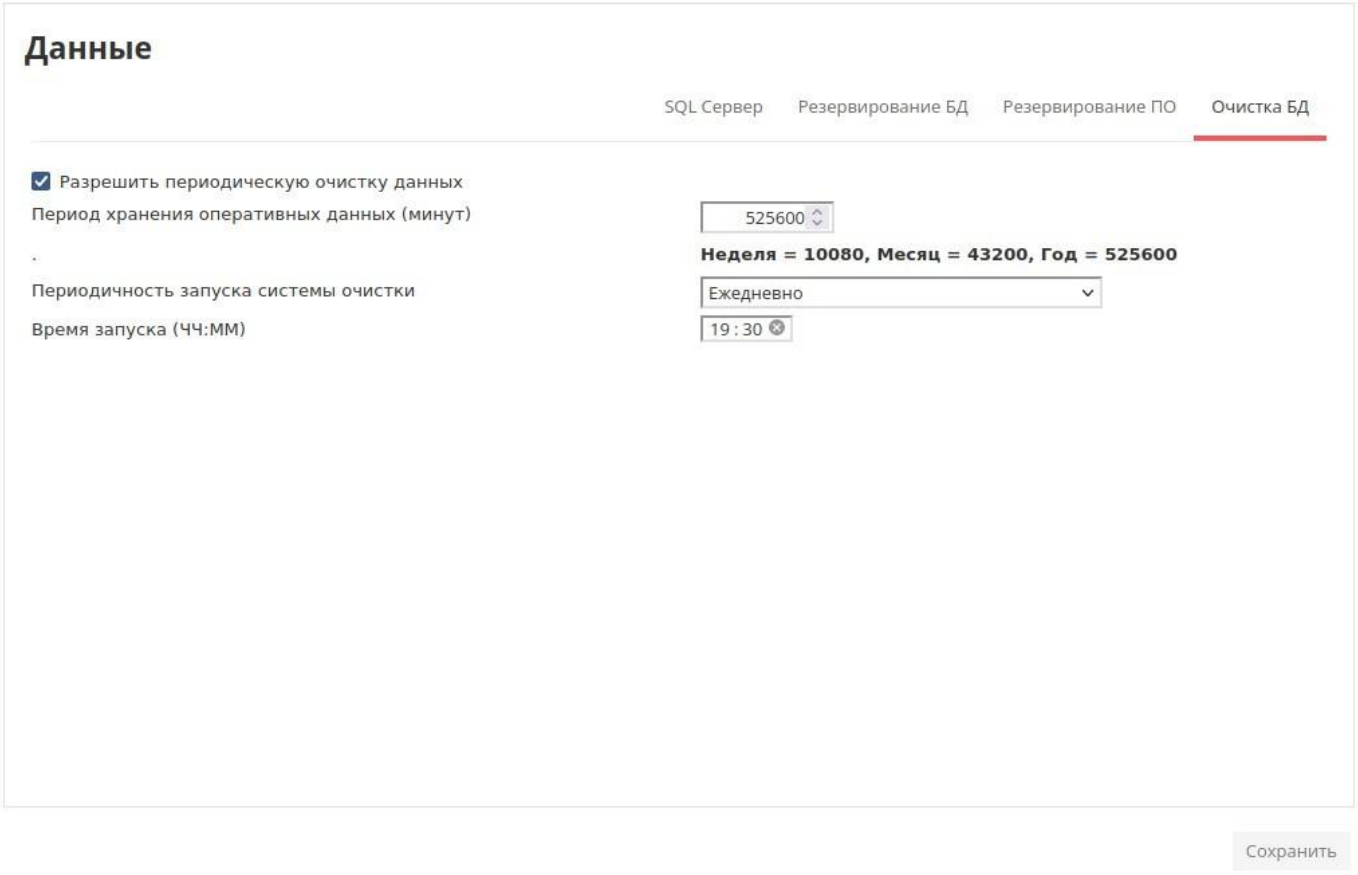


Рис. 111 Данные. Вкладка «Очистка БД»

В штатных средствах комплекса предусмотрена система автоматической очистки БД(рис. 111).

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. Для использования данной процедуры необходимо указать параметры:

- **Разрешить периодическую очистку данных** - Включение/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.

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

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.

Для сохранения изменений, нужно нажать на кнопку «Сохранить» 

.

8.3 Администрирование. 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.

8.3.1 Безопасность. Вкладка «Роли»

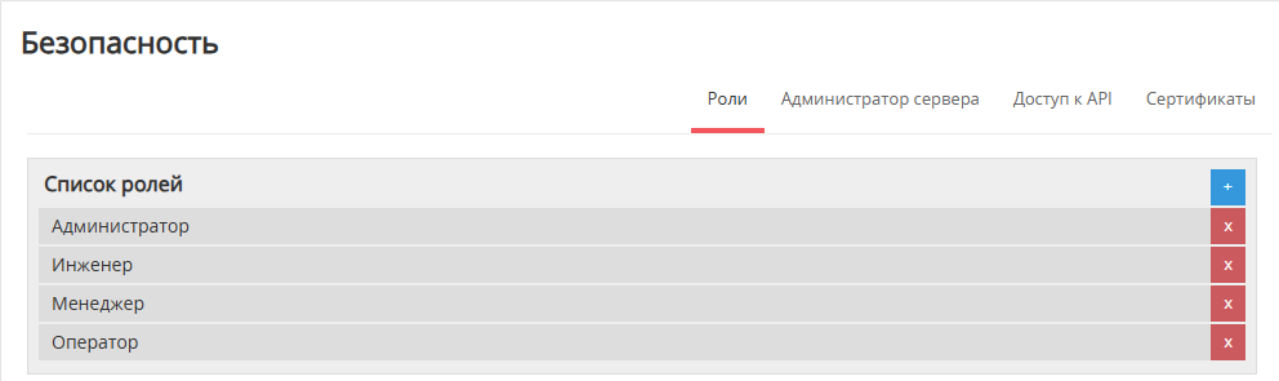


Рис. 112 Безопасность. Вкладка «Роли»

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

Для определения прав доступа в КРОС существует система Ролей(рис. 112). Каждая роль может содержать определенный набор прав доступа. Каждый пользователь охранной организацииможе иметь одну или несколько ролей. Новые роли могут быть введены в системе КРОС только **Администратором сервера**.

К разделу **«Безопасность»** имеет доступ только **Администратор сервера**.

В системе по умолчанию настроены 4 роли:

- **Администратор** - для пользователей имеющих полные права на работу с сервером в рамках своей организации. Право на изменение и создание учетных записей организации.
- **Инженер** - устанавливается пользователям имеющим доступ на просмотр и изменение технического функционала сервера.
- **Менеджер** - назначается имеющим доступ к просмотру статистики. Изменению и просмотру договоров, объектов и справочников.
- **Оператор** - предусмотрена для создания пользователей, не имеющих доступ к серверу организации, работающих только с ПО АРМ Сервер-Крос.

8.3.1.1 Права доступа

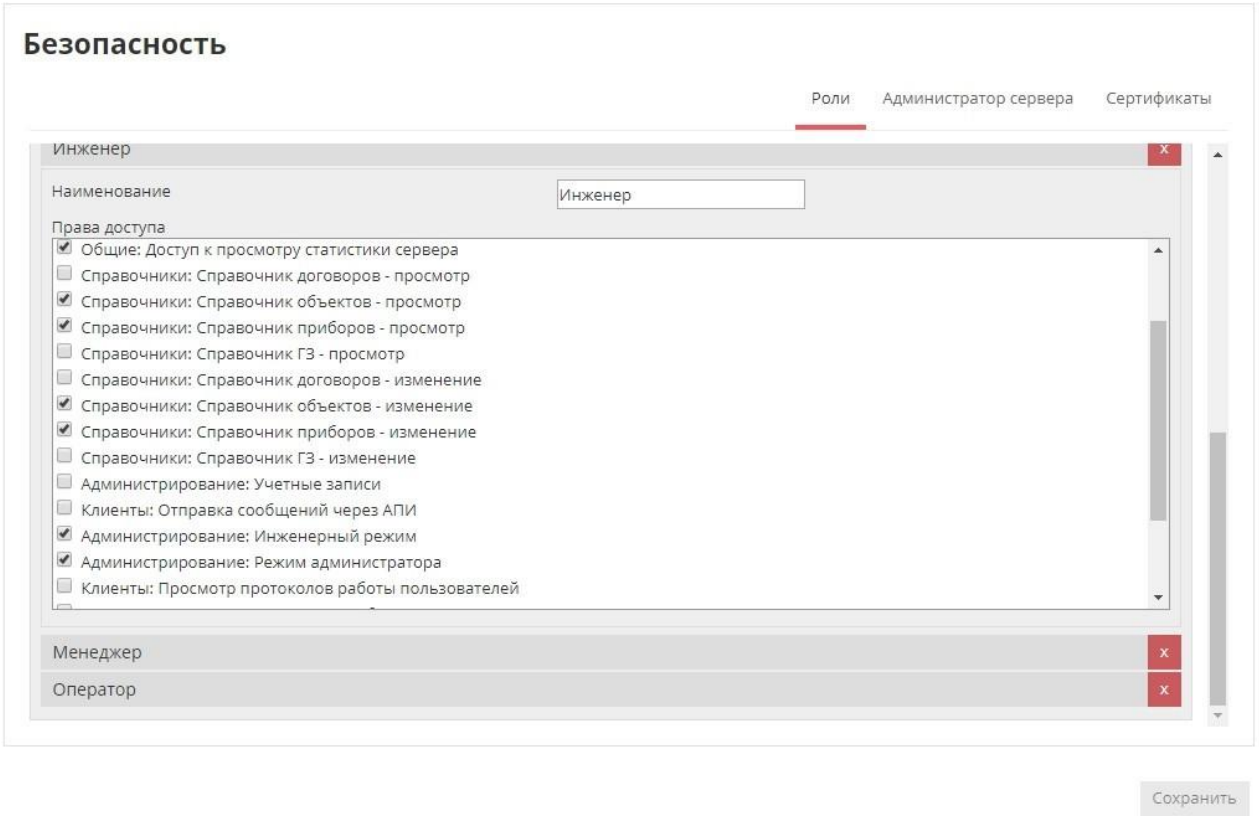


Рис. 113 Права доступа

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

Каждую роль можно настроить индивидуально, ниже представлены права доступа для каждой роли(рис. 113):

Общие: Доступ к просмотру статистики сервера - Доступ к общей статистике работы сервера. ***Меню: Главная***.

- **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***.
- **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** - 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***.

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

- **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 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: Отправка сообщений через АПИ** - Определяет право создавать сообщения и события средствами HTTP/JSON API. Предназначено для отладочных целей.
- **Клиенты: Просмотр протоколов работы пользователей** - Право просмотра протокола работы системы КРОС. ***Меню: Администрирование -> Протокол***.
- **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. Частные случаи* - ***Клиенты: Разрешение взятия*** *и* ***Клиенты: Разрешение снятия***.
- **Клиенты: Конструктор отчетов** - Доступ к генератору отчетов, позволяет создавать свои формы отчётов.
- **Клиенты: Разрешение постановки на прогон** - Позволяет регулировать разрешение постановки/снятия объекта на прогон, блокировки объектов и зон.

8.3.1.2 Создание, редактирование и удаление роли

Во вкладке «Роли» создаются, настраиваются и удаляются роли.

Для создания или редактирования роли необходимо:

1. Зайти на сервер под учетной записью **Администратора сервера** (*superadmin*).
2. Выбрать в меню пункт меню **Администрирование** раздел **Безопасность** вкладка **Роли**.
3. Для создания новой роли необходимо нажать на кнопку "Добавить" , ввести имя роли и выставить разрешения для новой роли. Для редактирования, уже существующей роли, необходимо выбрать роль и раскрыть её, подведя маркер и кликнув клавишей "мышки". После чего отредактировать необходимые параметры.
4. Для сохранения новой роли необходимо нажать кнопку "Сохранить" 

.
5. Для удаления роли необходимо нажать на кнопку "Удалить" 

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

8.3.2 Безопасность. Вкладка «Администратор сервера»

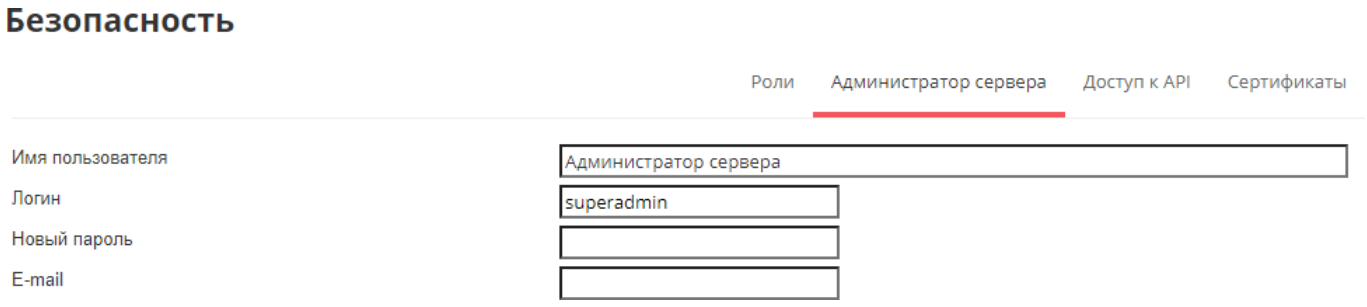


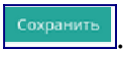
Рис. 114 Безопасность. Вкладка «Администратор сервера»

Во вкладке «Администратор сервера»(рис. 114) происходит настройка данных Администратора сервера.

- **Имя пользователя** - задается имя Администратора сервера. Можно задать своё имя.
- **Логин** - задается логин для входа администратора сервера. Логин пользователя можно изменить.
- **Новый пароль** - задается новый пароль, заменяющий старый, для входа администратора сервера. Если в работе сервера используется доступ из вне, настоятельно рекомендуется изменить пароль на сложный, чтобы исключить несанкционированный доступ.

Примечание: В случае потери измененного пароля, для восстановления доступа к учетной записи Администратора сервера необходимо обратиться в службу технической поддержки представительства ООО «Элеста».

- **E-mail** - для актуального почтового адреса Администратора сервера.

Для сохранения изменений, нужно нажать на кнопку "Сохранить" 

.

8.3.3 Безопасность. Вкладка «Доступ API»

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

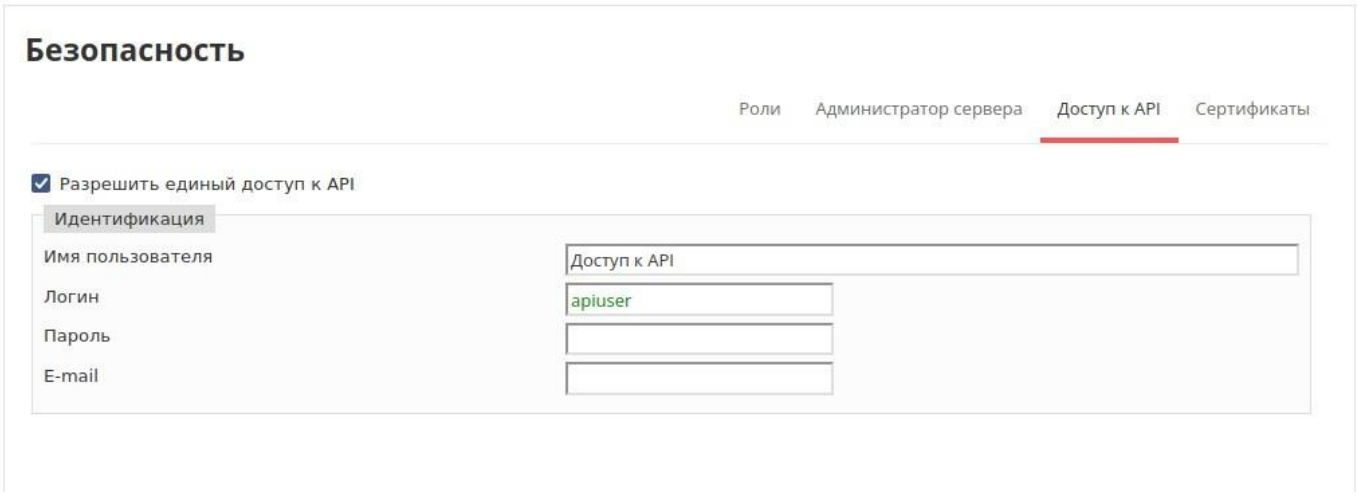
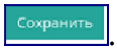


Рис. 115 Безопасность. Вкладка «Доступ API»

API – Application Programming Interface, что значит программный интерфейс приложения. В контексте API слово «приложение» относится к любому ПО с определенной функцией. Интерфейс можно рассматривать как сервисный контракт между двумя приложениями. Этот контракт определяет, как они взаимодействуют друг с другом, используя запросы и ответы. Документация API содержит информацию о том, как разработчики должны структурировать эти запросы и ответы.

API – это механизмы, которые позволяют двум программным компонентам взаимодействовать друг с другом, используя набор определений и протоколов. Архитектура API обычно объясняется с точки зрения клиента и сервера. Приложение, отправляющее запрос, называется клиентом, а приложение, отправляющее ответ, называется сервером. Для использования механизма API необходимо (рис. 115):

- **Разрешить единый доступ к API** - Позволяет осуществлять запросы к серверу посредством API.
  - **Идентификация**:
  - **Имя пользователя** - наименование пользователя.
  - **Логин** - имя пользователя для аутентификации на сервере. Пользователь которому разрешается использовать API запросы.
  - **Пароль** - пароль пользователя.
  - **E-mail** - адрес электронной почты.

После внесения данных, нажать кнопку "Сохранить" 

.

8.3.4 Безопасность. Вкладка «Сертификаты»

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

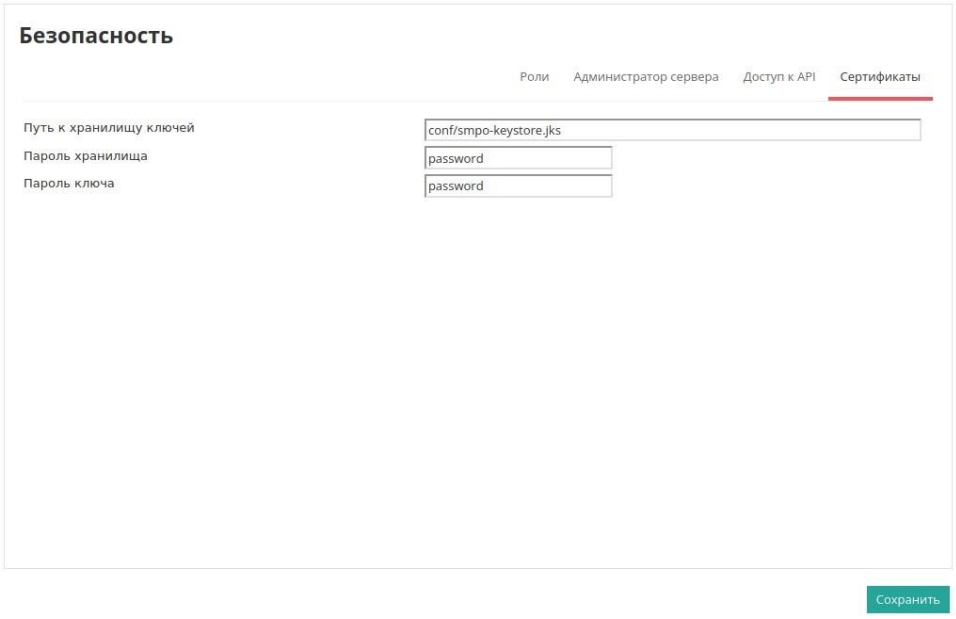
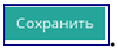


Рис. 116 Безопасность. Вкладка «Сертификаты»

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) Для описания сертификата используются следующие параметры(рис. 116):

- **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» 

.

8.3.5 Усиленная парольная защита

8.3.5.1 Назначение

Режим «Усиленная парольная защита» реализует единые требования к паролям учётных записей системы КРОС в соответствии с разделом Е.10 ЕТ СПИ «Требования к парольной защите АРМ КСА ПЦО».

Режим охватывает состав и длину пароля, историю паролей, срок действия, защиту от подбора и сопутствующие уведомления. Все требования включаются и отключаются единой галочкой, а их состояние применяется к системе КРОС.

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

8.3.5.2 Включение и отключение режима

Настройки режима расположены в разделе «Администрирование» → «Безопасность» и доступны исключительно пользователю с ролью «Администратор сервера» (superadmin). Параметр состояния режима сохраняется в базе данных.

- При снятой галочке «Усиленная парольная защита» требования к паролям (состав, длина, история, срок действия, блокировка при подборе и сопутствующие уведомления) не применяются.
- При установленной галочке требования вступают в силу в полном объёме.

Галочка недоступна для включения до тех пор, пока хотя бы у одного пользователя в системе пароль не соответствует требованиям (см. п. 8.3.5.4).

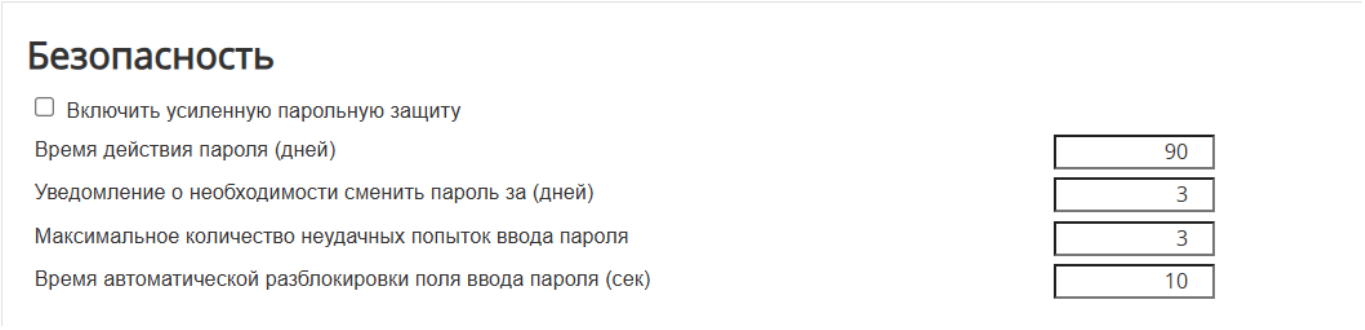


Рис. 117 Безопасность. «Параметры парольной защиты»

8.3.5.3 Настраиваемые параметры

Администратору сервера доступны для настройки следующие параметры (см. Рис. 117):

- Время жизни (срок действия) пароля, дни
- Порог предупреждения об истечении пароля, дни
- Максимальное количество неудачных попыток входа
- Время автоматической разблокировки АРМ, секунды

Время жизни пароля задаётся единым значением в днях для всех пользователей системы; 90 дней - максимально допустимое значение.

Порог предупреждения определяет, за сколько дней до истечения пароля начинают выводиться предупреждающие уведомления.

Максимальное количество попыток и время разблокировки управляют защитой от подбора.

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

8.3.5.4 Требования к паролю и валидация

При включённом режиме пароль должен:

- иметь длину не менее 14 символов — для всех ролей (Администратор сервера, Администратор охранной организации, Менеджер, Инженер, Оператор);
- содержать символы из каждой категории:

✓ строчные латинские буквы (a-z);

✓ прописные латинские буквы (A-Z);

✓ цифры (0-9);

✓ специальные символы: `! @ # $ % ^ & * ( ) + \ / ; : = ~ [ ] { } _ < > ?`

Пароль не должен:

- содержать запрещённые слова в любом регистре: administrator, admin, adm, user, password, 123456, qwerty, root;
- содержать более двух одинаковых символов подряд (например, `aaa`, `111`, `!!!`);
- содержать пробел (« »);
- совпадать с одним из трёх предыдущих паролей пользователя (история паролей).

Проверка пароля выполняется на стороне сервера при попытке изменить пароль учетной записи. Система проверяет:

- соответствие введённого старого пароля текущему;
- длину пароля (не менее 14 символов);
- наличие символов всех категорий (строчные, прописные, цифры, спецсимволы);
- отсутствие запрещённых слов;
- отсутствие более двух одинаковых символов подряд;
- отсутствие пробелов;
- отличие от истории паролей (трёх предыдущих).

При несоответствии требованиям система отображает сообщение о том, какое именно требование не выполнено, и предлагает повторный ввод. При соответствии требованиям новый пароль сохраняется, и пользователю возвращается доступ к системе.

8.3.5.5 Индикация надежности пароля и условия активации режима

В интерфейсе управления учётными записями рядом с каждой записью отображается метка состояния пароля. Метка показывается всегда, независимо от того, включён режим усиленной защиты или нет:

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

- «Надёжный» — пароль удовлетворяет всем требованиям п. 8.3.5.4;
- «Ненадёжный» — пароль не соответствует одному или нескольким требованиям.

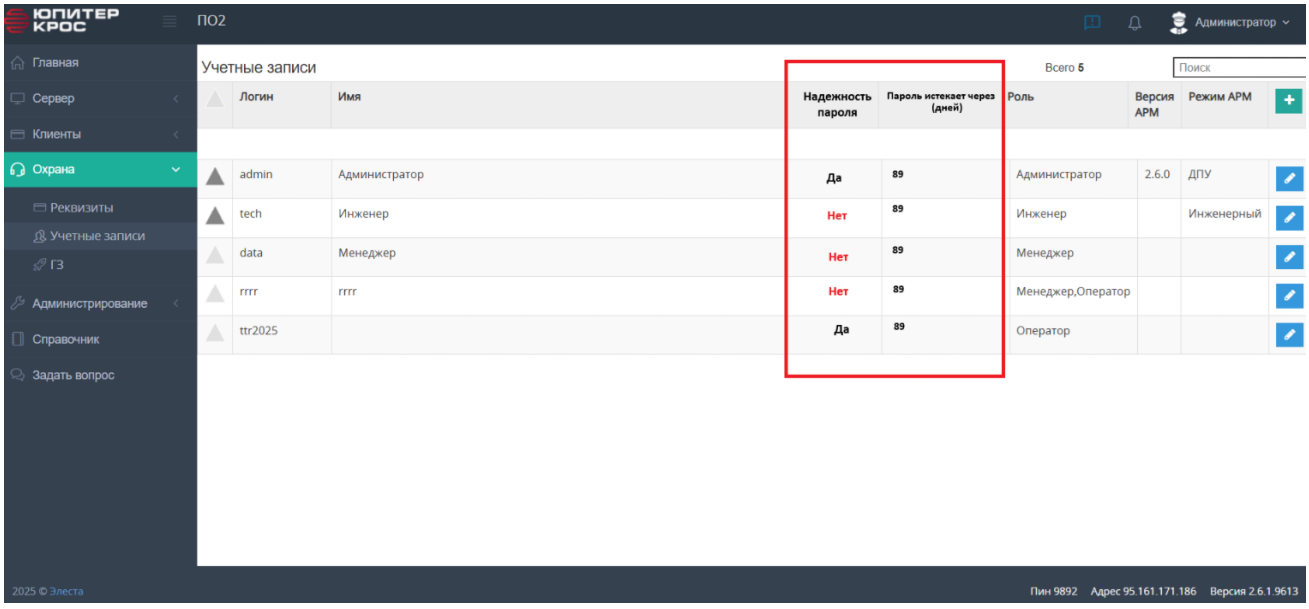


Рис. 118 Охрана. Учетные записи. «Список учётных записей с метками надежности»

Блокировка галочки. Галочка «Усиленная парольная защита» заблокирована в состоянии «выкл», пока хотя бы у одного пользователя пароль не отвечает требованиям. Включение режима становится возможным только после того, как все учётные записи получат надёжные пароли.

При нажатии кнопки «Сохранить» с установленной галочкой, если в системе остаются учётные записи с ненадёжными паролями, система блокирует сохранение и выводит окно со сведениями о том, какие записи препятствуют включению режима. Окно содержит:

- список охранных организаций, у пользователей которых пароли не соответствуют требованиям;
- для каждой организации — перечень логинов с ненадёжными паролями.

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

После закрытия окна администратор возвращается к форме с галочкой в состоянии «выкл».

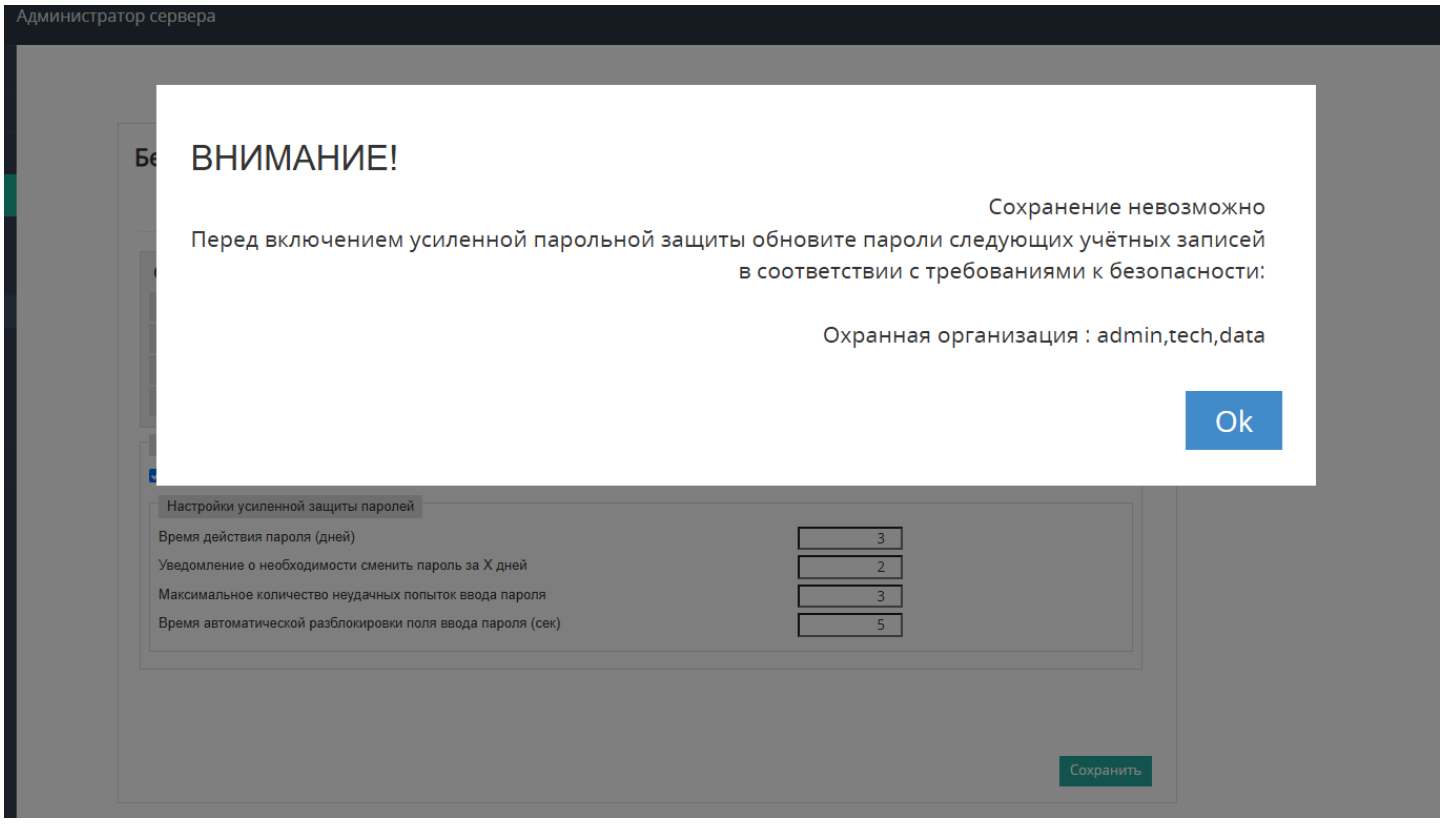


Рис. 119 «Окно со списком организаций и логинов, препятствующих включению режима»

8.3.5.6 Управление сроком действия пароля

Просмотр срока действия.

- Администратор сервера видит актуальный срок действия своего пароля (Рис.120) и паролей Администраторов охранных организаций (Рис.118);
- Администратор охранной организации видит срок действия своего пароля и паролей остальных пользователей своей организации (Рис.118).

Смена пароля администратором.

- Администратор сервера может задать новый пароль себе (Рис.120) и Администратору охранной организации через карточку пользователя (Рис.121);
- Администратор охранной организации может задать новый пароль себе и остальным пользователям своей организации. Смена выполняется в карточке пользователя (Рис.121).

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

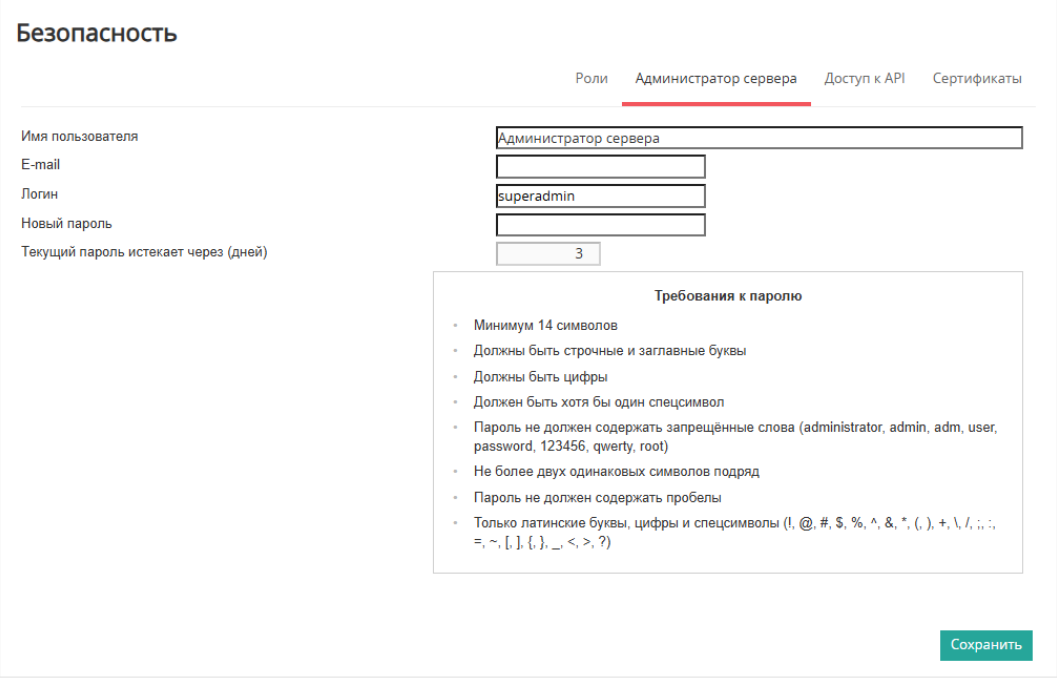


Рис. 120 Безопасность. Администратор сервера. «Отображение срока действия пароля superadmin»

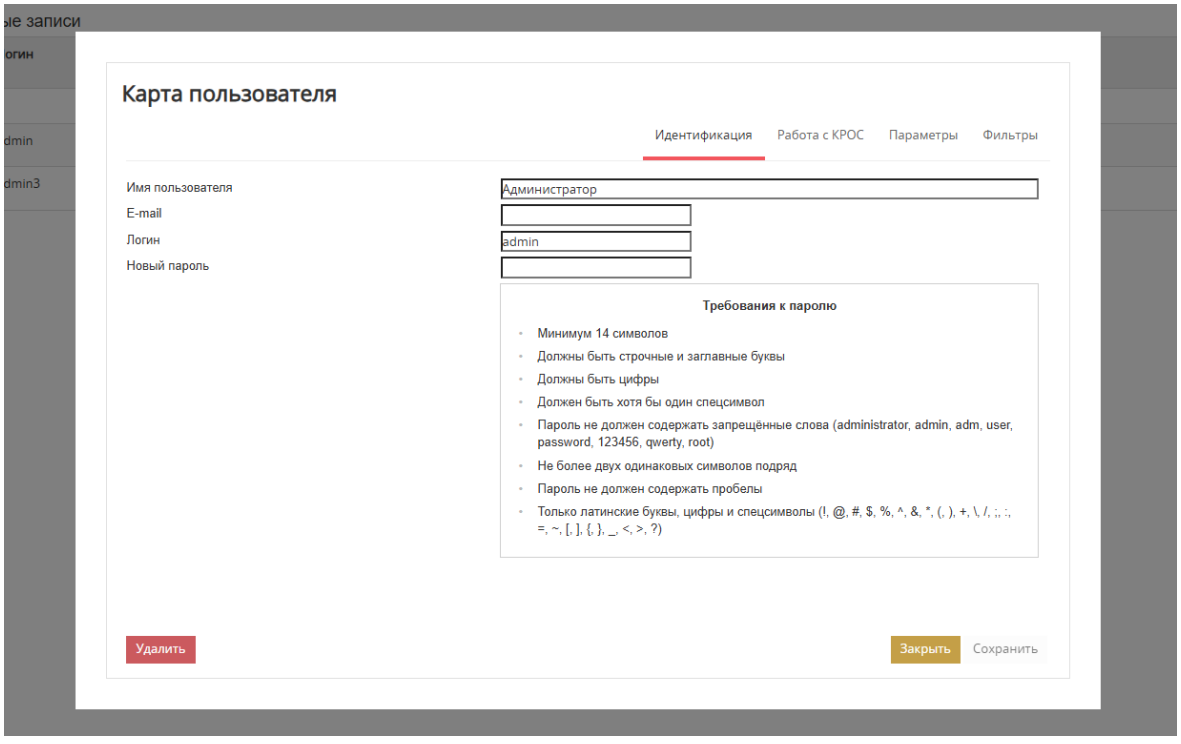


Рис. 121 Охрана. Учетные записи. «Смена пароля через карточку пользователя»

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

8.3.5.7 Защита от подбора пароля

Счётчик неудачных попыток ведётся на сервере и привязан к конкретному АРМ по IP-адресу.

- При каждой неудачной попытке входа счётчик увеличивается на единицу, а пользователю выводится сообщение: **«Неверный логин или пароль. Осталось попыток: N»**.
- Счётчик сбрасывается в 0 **только** после успешного входа.

Блокировка АРМ. При превышении максимального количества попыток (п. 8.3.5.3) система одновременно:

1. Блокирует форму входа на текущем АРМ — поля ввода и кнопка входа становятся недоступны;
2. Отображает надпись: **«Превышено максимальное количество попыток входа. АРМ заблокирован. Разблокировка через: mm:ss»**;
3. Записывает в протокол работы сервера событие **«попытка подбора пароля»** с указанием IP-адреса, введённого логина (если был введён), даты и времени;
4. Рассылает уведомление на все другие АРМ КСА ПЦО, подключённые к тому же серверу ПЦН.

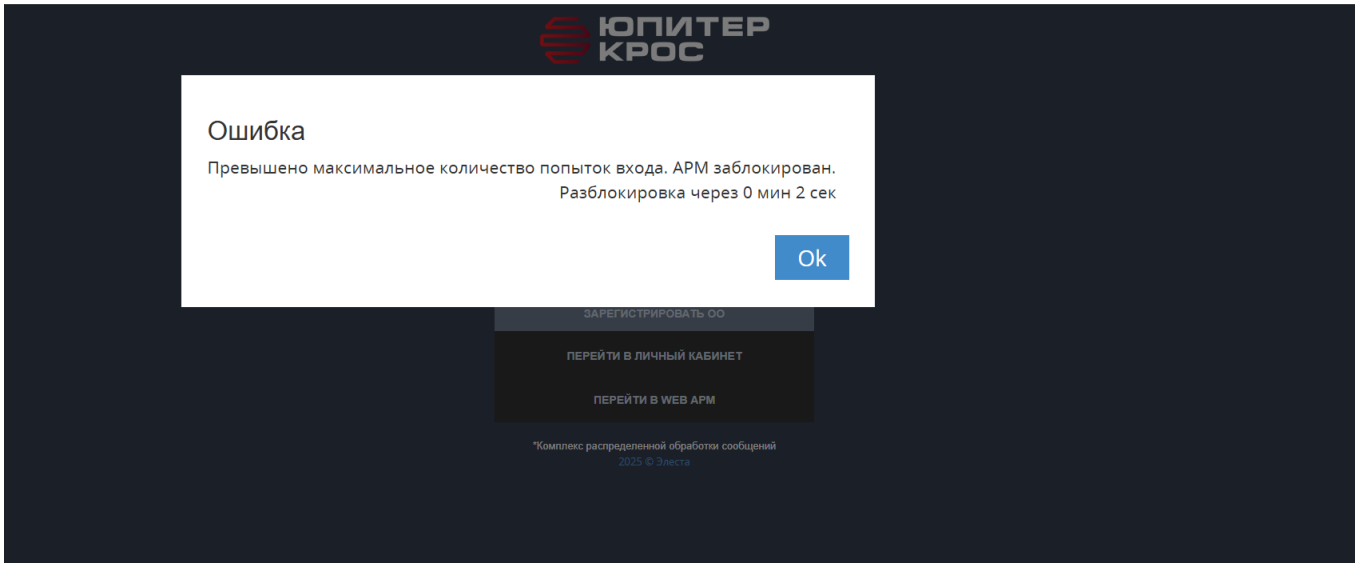


Рис. 122 «Экран блокировки формы входа»

Автоматическая разблокировка. По истечении настроенного времени форма входа разблокируется автоматически. Счётчик при этом **не** сбрасывается и остаётся на максимальном значении. Каждая последующая неудачная попытка немедленно запускает новую блокировку,

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

повторно записывает событие в протокол и рассылает уведомление. Счётчик сбрасывается только после успешного входа.

Уведомление на других АРМ. На всех активных АРМ, подключённых к тому же серверу ПЦН, выводится информационное окно. В административной панели КРОС окно содержит IP-адрес компьютера, последний введённый пароль, дату и время последней попытки. Окно **не** блокирует работу. При повторной блокировке уведомление обновляется, и (или) в него добавляется новый инцидент. Уведомление доставляется только тем АРМ, которые активны в момент события.

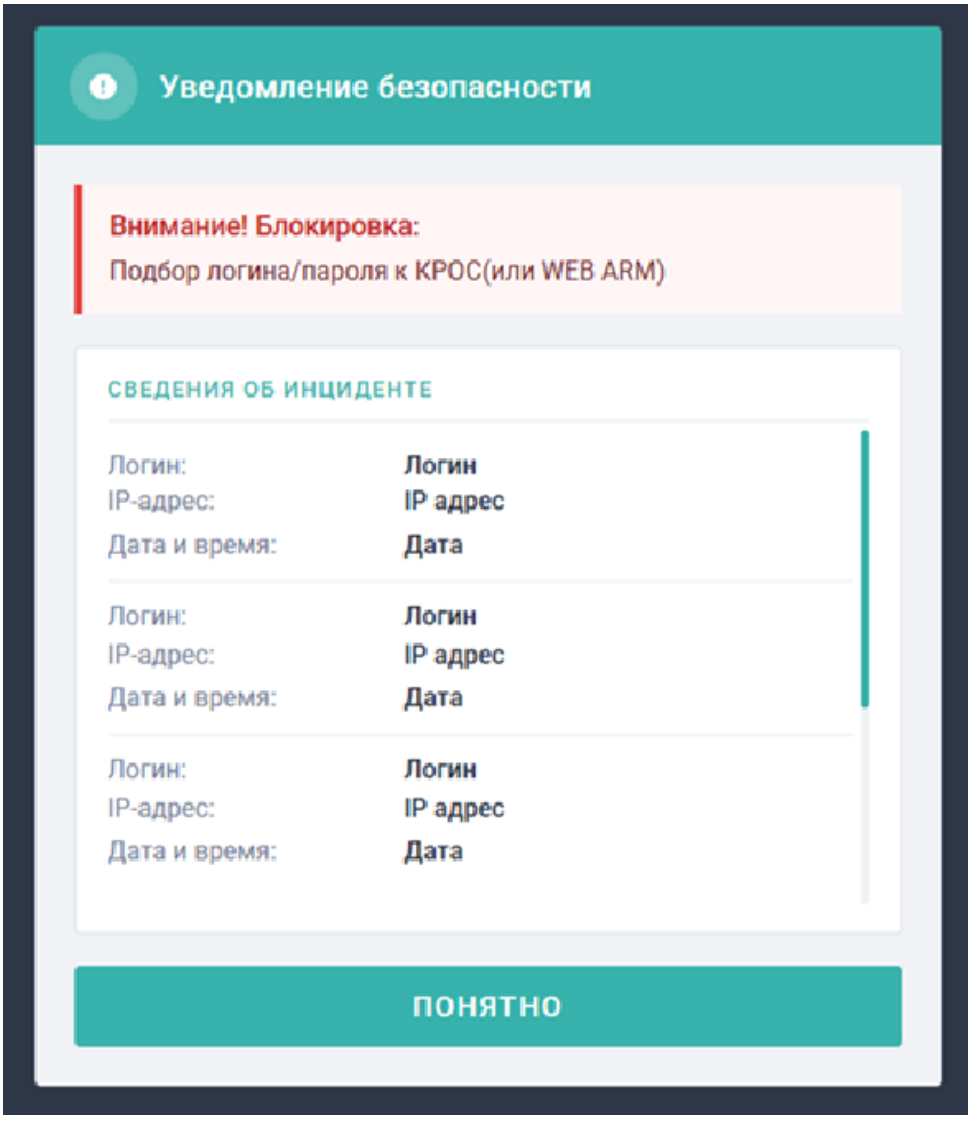


Рис. 123 «Информационное окно по попытке подбора на другом АРМ»

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

8.3.5.8 Истечение срока действия пароля

Если на момент входа срок действия пароля истёк:

- Аутентификация выполняется штатно (проверка логина и пароля);
- Сразу после успешного входа выводится **модальное окно принудительной смены пароля**;
- Доступ к функционалу системы заблокирован до успешной смены пароля;
- После успешной смены пароля пользователь проходит авторизацию заново.

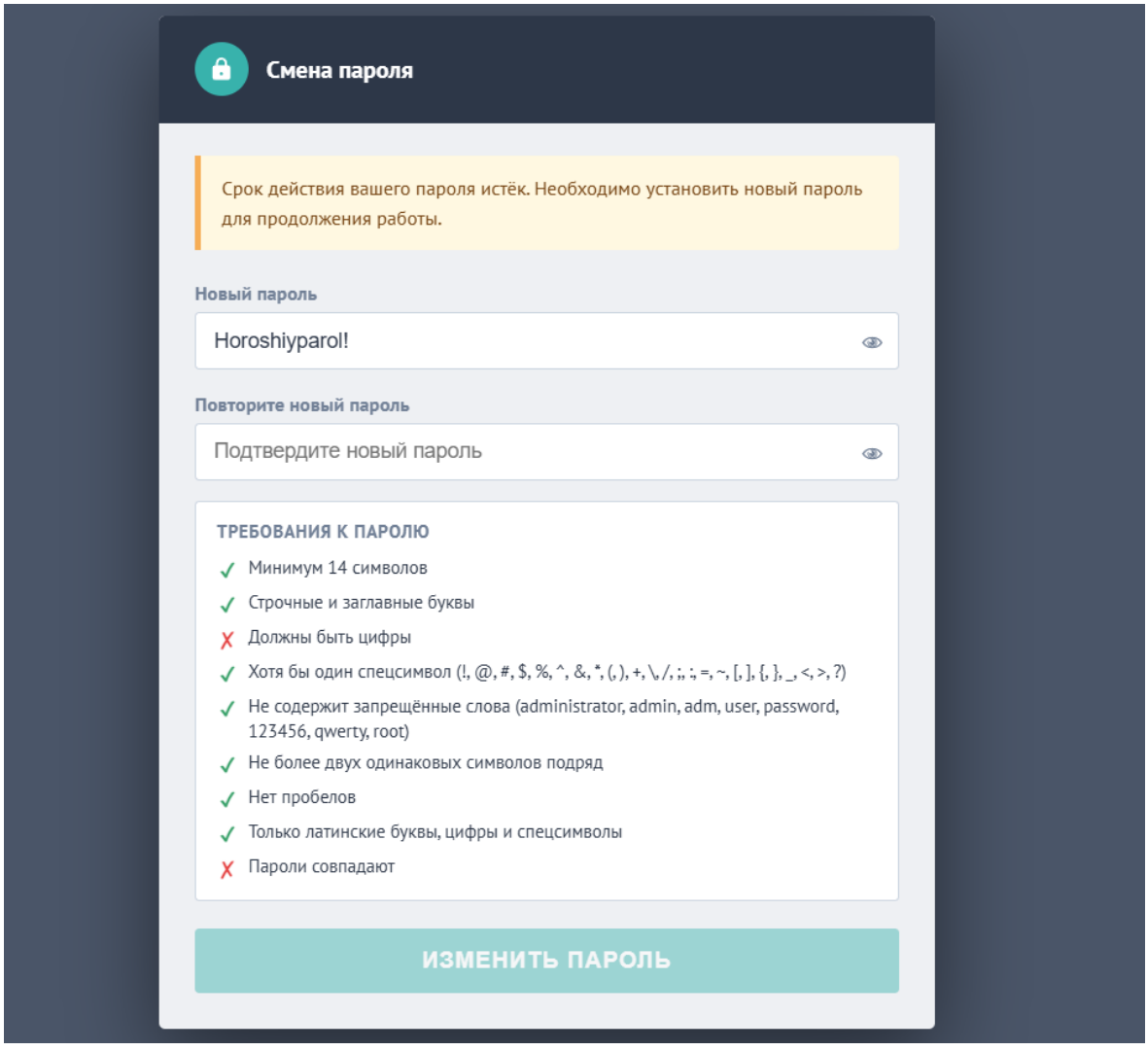


Рис. 124 «Окно принудительной смены пароля»

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

Предупреждение об истечении срока действия пароля.

За настраиваемое число дней до истечения (п. 8.3.5.3) система выводит предупреждения при входе.

О собственном пароле администратора:

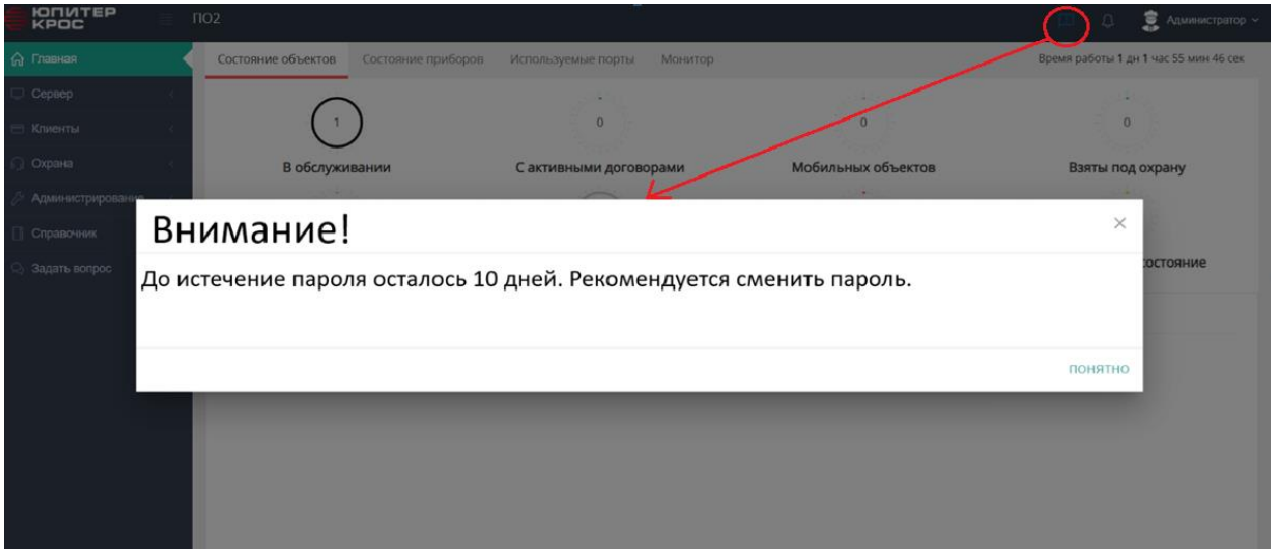


Рис. 125 «Уведомление администратору о скором истечении собственного пароля»

Об истечении паролей у других пользователей:

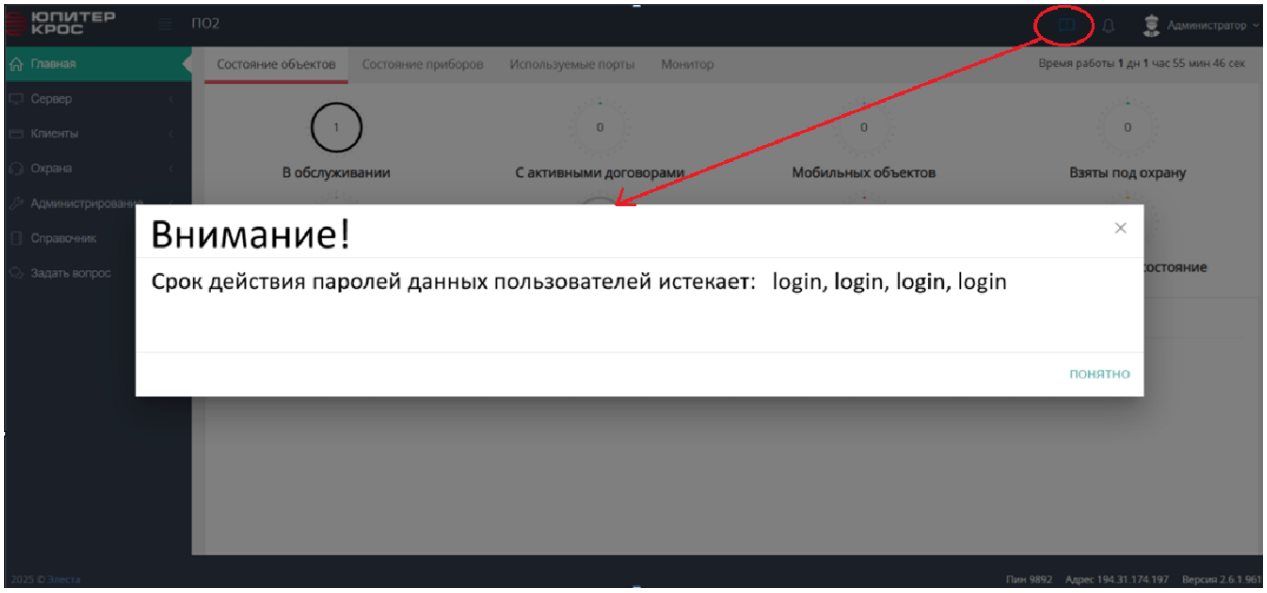


Рис. 126 «Уведомление администратору о скором истечении пароля у подчиненных ролей»

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

Правила формирования списка:

- для **Администратора сервера** — логины Администраторов охранных организаций, у которых истекает пароль;
- для **Администратора охранной организации** — логины всех пользователей его организации, у которых истекает пароль, кроме собственного.

Истечение пароля Администратора сервера: помимо личного уведомления, во **всех** остальных учётных записях на сервере появляется уведомление о скором истечении срока действия пароля администратора сервера.

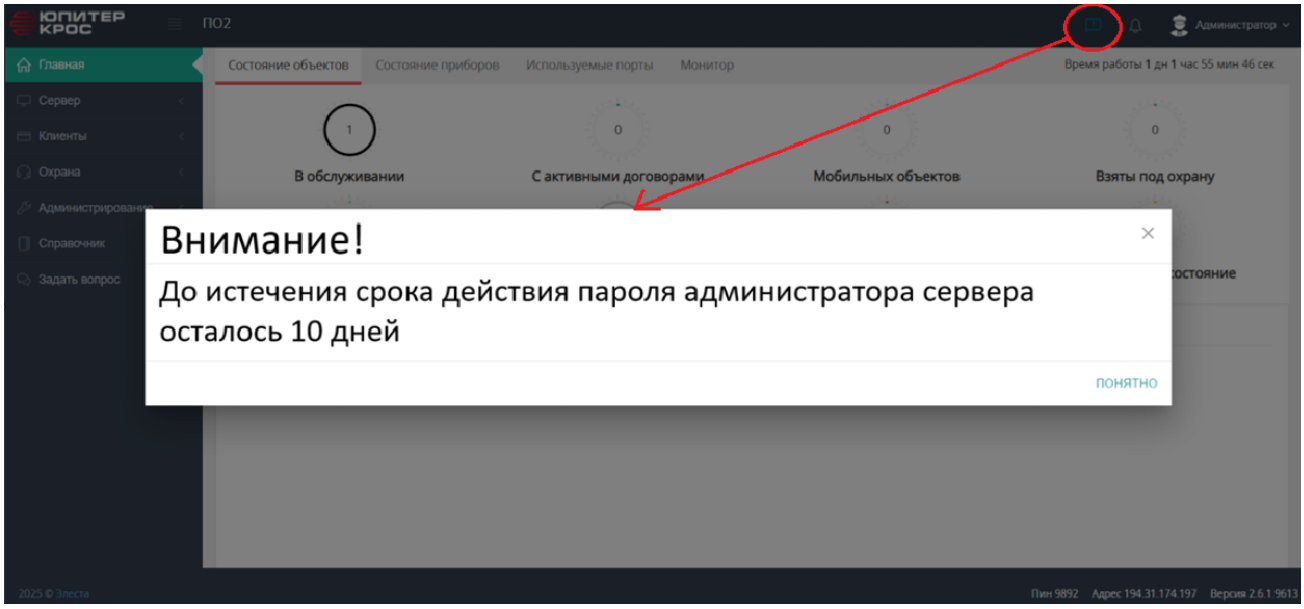


Рис. 127 «Уведомление всем пользователям админ панели о скором истечении пароля у администратора сервера»

8.3.5.9 Создание охранной организации при включенном режиме

При включённой галочке и создании Администратором сервера новой охранной организации:

- Учётная запись Администратора этой организации создаётся автоматически, пароль генерируется автоматически (не соответствующий требованиям усиленной защиты);
- При первом входе выводится модальное окно принудительной смены пароля (аналогично п. 8.3.5.8): окно невозможно закрыть, доступ к функционалу заблокирован до успешной смены;
- После успешной смены пароля пользователь проходит авторизацию заново.

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

8.4 Администрирование. Заявки

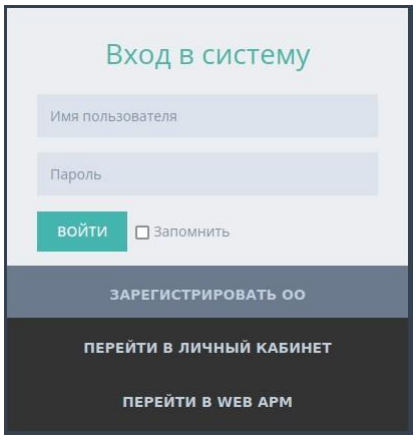


Рис. 128 Окно регистрации и дополнительных действий

8.4.1 Подача заявки на регистрацию

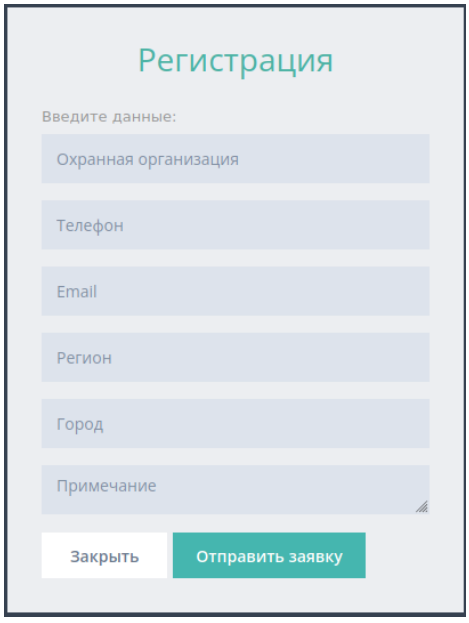


Рис. 129 Форма подачи заявки на регистрацию ОО

Сервер КРОС может работать с несколькими Охранными организациями, поэтому в нём предусмотрена система подачи заявок на регистрацию ОО(рис. 129).

- Для подачи заявки в окне авторизации(рис. 128) достаточно выбрать "ЗАРЕГИСТРИРОВАТЬ ОО", заполнить форму и нажать кнопку "Отправить заявку". На экране появистя сообщение о регистрации заявки и её номер. Для закрытия окна нажать X.

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

8.4.2 Обработка заявки на регистрацию



Рис. 130 Таблица заявок на регистрацию ОО

Для регистрации ОО(рис. 130) необходимо открыть запись, нажав "Редактировать" 

1. Отметить параметр **"Принять"**.
2. Нажать кнопку **"Зарегистрировать предприятие"**.
3. После этого откроется окно для заполнения реквизитов ОО.

После того, как будут введены данные по новой ОО (рис. 131) и сохранены данные, система управления учетными данными КРОС выдаст информацию, необходимую для работы ОО.

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

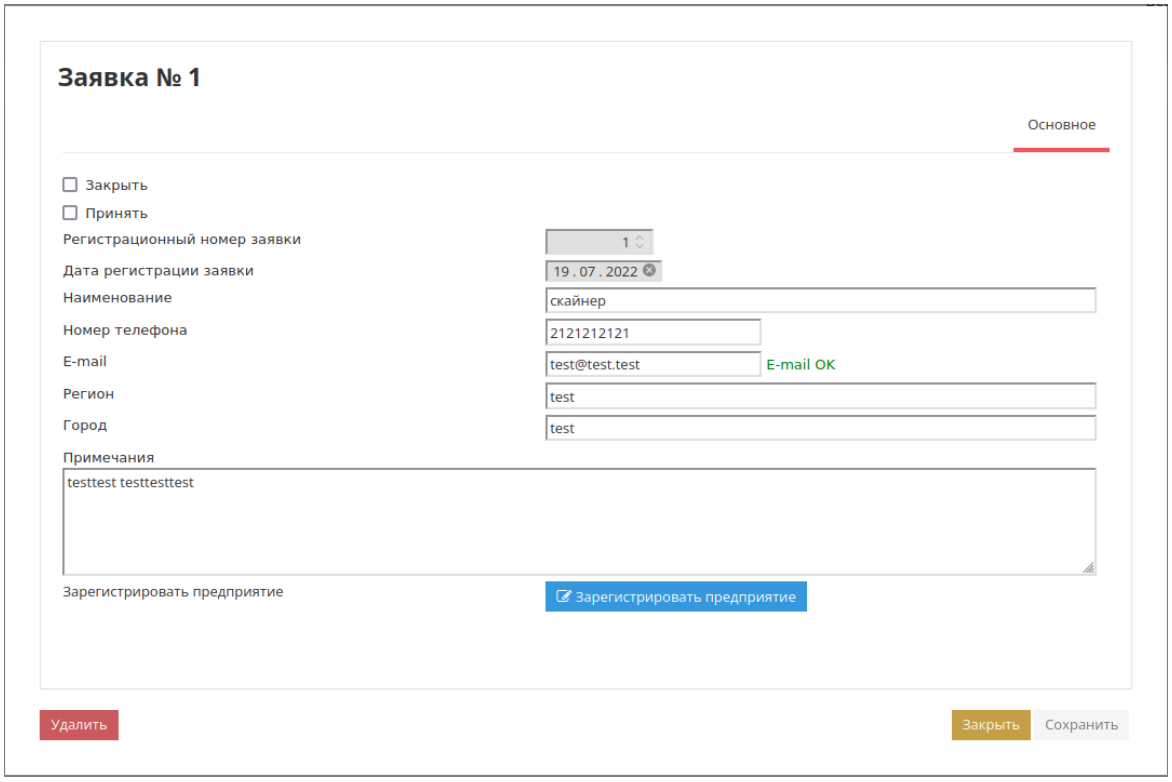
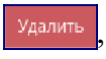


Рис. 131 Карточка регистрации ОО



Рис. 132 Информация по регистрации ОО

Эту информацию можно отправить по электронной почте прямо из карточки ОО. В таблице "Охрана"→"Реквизиты" появится еще одна ОО.

Для удаления заявки достаточно открыть заявку на редактирование и нажать на кнопку "Удалить" 

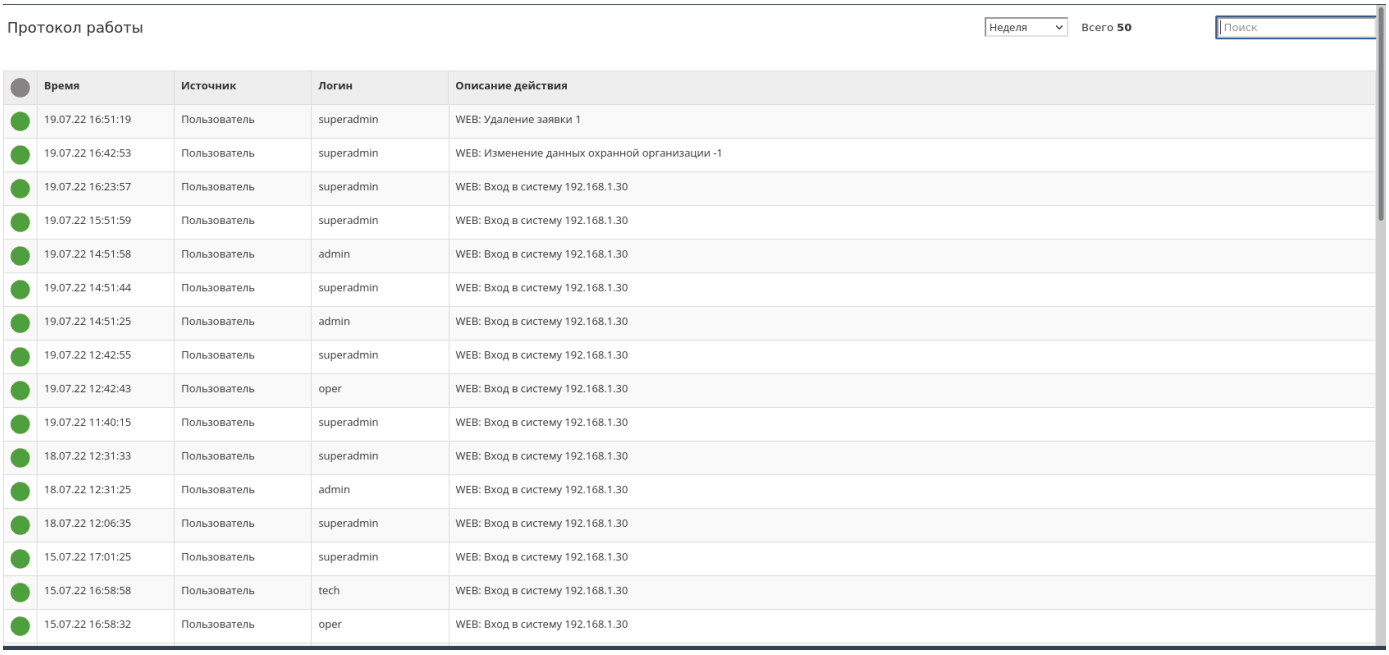
, после чего согласиться с действием.

Для дальнейшего редактирования данных по ОО необходимо войти в её профиль и внести необходимые изменения, так как описано в ***п. 7.1 Реквизиты***.

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

8.5 Администрирование. Протокол

Для того чтобы открыть Протокол событий необходимо в Меню "Администрирование" выбрать раздел "Протокол". В таблице отображается протокол событий, произошедших на сервере и в АРМ, действия которые совершили пользователи непосредственно на сервере КРОС.



Время	Источник	Логин	Описание действия
19.07.22 16:51:19	Пользователь	superadmin	WEB: Удаление заявки 1
19.07.22 16:42:53	Пользователь	superadmin	WEB: Изменение данных охранной организации -1
19.07.22 16:23:57	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
19.07.22 15:51:59	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
19.07.22 14:51:58	Пользователь	admin	WEB: Вход в систему 192.168.1.30
19.07.22 14:51:44	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
19.07.22 14:51:25	Пользователь	admin	WEB: Вход в систему 192.168.1.30
19.07.22 12:42:55	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
19.07.22 12:42:43	Пользователь	oper	WEB: Вход в систему 192.168.1.30
19.07.22 11:40:15	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
18.07.22 12:31:33	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
18.07.22 12:31:25	Пользователь	admin	WEB: Вход в систему 192.168.1.30
18.07.22 12:06:35	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
15.07.22 17:01:25	Пользователь	superadmin	WEB: Вход в систему 192.168.1.30
15.07.22 16:58:58	Пользователь	tech	WEB: Вход в систему 192.168.1.30
15.07.22 16:58:32	Пользователь	oper	WEB: Вход в систему 192.168.1.30

Рис. 133 Администрирование. Протокол

При просмотре событий (рис. 133), в выпадающем списке фильтра(рис. 134), можно определить временной интервал поиска событий. После чего в информационном сообщении **"Всего"** будет показано число найденых сообщений. **"Поиск "** поможет найти события по каким-либо известным признакам.

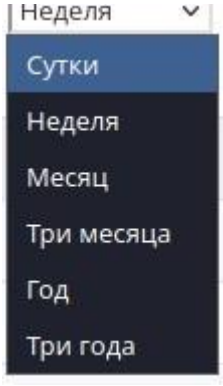


Рис. 134 Фильтр временного интервала событий

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

В протоколе указаны:

- **Статус события**

● - Действие не содержит ошибок.
● - Произведено действие, затрагивающее информацию ОО, например, удаление прибора, объекта.

- **Дата и время события**
- **Источник события**
- **Логин** пользователя, вызвавшего событие
- **Описание действия**, произошедшего события

Изначально право просмотра протокола есть у учетных записей с правами "Администратор предприятия" и "Администратор сервера", однако права доступа к протоколу можно поменять во вкладке "Администрирование → Безопасность"

8.6 Администрирование. Сообщения

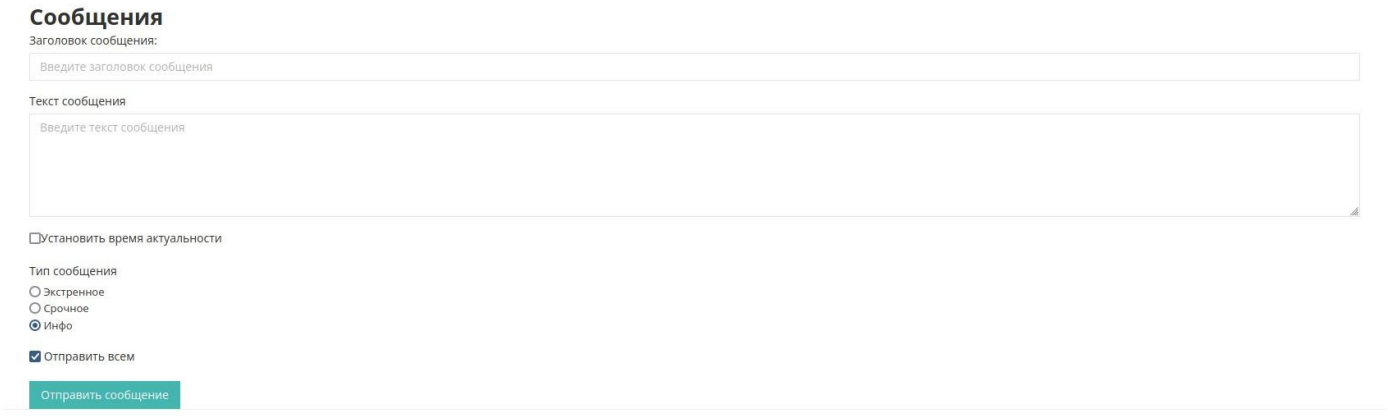


Рис. 135 Администрирование:Сообщения

С помощью пункта меню "Сообщения"(рис. 135) имеется возможность отправлять информационные сообщения от имени Администратора сервера (superadmin - логин и пароль по умолчанию) всем или по выбору охранным организациям , заведенным на сервер КРОС. Для отправки сообщения необходимо:

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

2. Зайти в меню Администрирование ---> Сообщения

3. Ввести сообщение, установить тип сообщения, а также выбрать кому отослать это сообщение:

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

- **Заголовок сообщения:** - Краткое определение сообщения
- **Текст сообщения** - Тело сообщения
- **Установить время актуальности** - установка данного параметра позволяет определить дату и время до которого действует это сообщение.
- **Тип сообщения** - Определяет каким цветом будет определен статус сообщения:
  - ***Экстренное*** - ;
  - ***Срочное*** - ;
  - ***Инфо*** - 
- **Отправить всем** - По-умолчанию этот параметр выбран и сообщение будет отправлено всем ОО, зарегистрированным на сервере КРОС. Однако, если есть необходимость отправить сообщение конкретной ОО, тогда необходимо снять выделение с этого параметраи в открывшемся списке выбрать ОО, которой надо отправить сообщение.

4. Нажать кнопку **"Отправить сообщение"**.

8.7 Администрирование. Справочники

В разделе «Справочники» (меню «Административные»→«Справочники») редактируются различные справочники, используемые при работе с Сервер-КРОС(рис. 136).

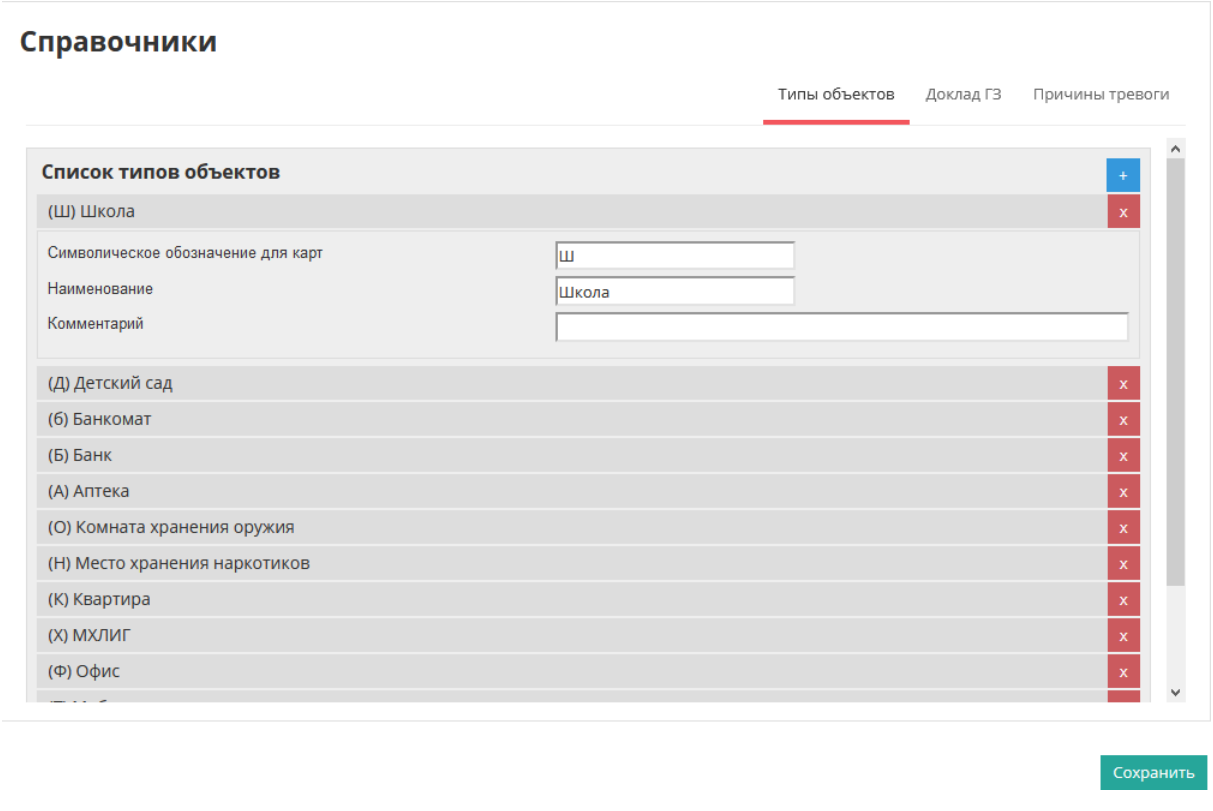


Рис. 136 Администрирование. Справочники

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

К окну «Справочники» имеет доступ только **Администратор предприятия**. Таким образом получается, что у каждой ОО, свои справочники. Справочники создаются для того, чтобы ускорить обработку информации, и как правило включают в себя наиболее часто встречающиеся шаблоны.

8.7.1 Справочники. Вкладка «Типы объектов»

Во вкладке "Типы объектов" имеется возможность создавать, редактировать существующие и удалять типы объектов(рис. 137), отображающиеся в карточке объекта в графе "Тип объекта", а также в АРМ ДПУ и ДО.

Для добавления нового типа объектов нажать на кнопку "Добавить" и согласитесь с добавлением записи, нажав "Да".

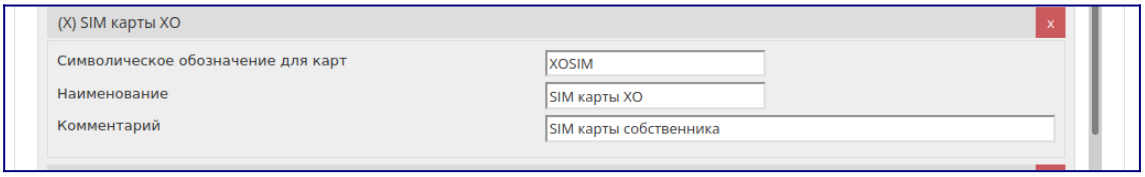


Рис. 137 Форма редактирования типа объектов

Далее следует заполнить поля:

- **Символическое обозначение для карт** - аббревиатура или иное обозначение типа, принятое для лёгкого определения типа.
- **Наименование** - развернутое наименование типа.
- '*Комментарий*- описание типа или замечания к нему.

Тип объекта - используется для облегчения поиска или группирови объектов по единому признаку. Для удаления типа объекта нажать кнопку "Удалить" . После добавления нового типа объекта и заполнения всех полей нажать "Сохранить" Сохранить.

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

8.7.2 Справочники. Вкладка «Доклад ГЗ»

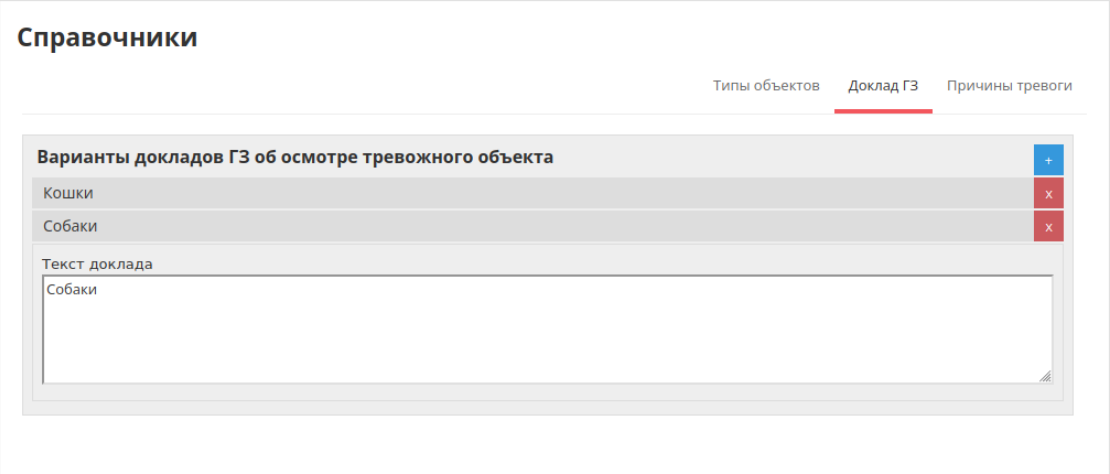


Рис. 138 Форма создания сообщений ГЗ

Во вкладке "Доклад ГЗ"(рис. 138 имеется возможность создавать, редактировать существующие и удалять варианты докладов ГЗ, применяемые дежурным оператором в АРМ ДПУ и ДО, а также отображающиеся в отчетах.

- Для добавления нового доклада ГЗ, нажать на кнопку "Добавить" . В поле **Текст доклада** ввеси вариант доклада. Точно так же можно внести изменения при редактировании.
- После добавления нового доклада ГЗ и заполнения всех полей, а так же после редактирования записи, нажать "Сохранить" Сохранить.
- Для удаления доклада ГЗ нажать кнопку "Удалить" .

8.7.2 Справочники. Вкладка «Причины тревоги»

В данной вкладке имеется возможность создать, изменить существующие или удалить варианты причин тревоги, применяемые дежурным оператором в АРМ ДПУ и ДО, а также отображающиеся в отчетах(рис. 139).

- Для добавления новой причины тревоги нажать на кнопку "Добавить" . В поле **Текст доклада** ввеси вариант доклада. Точно так же можно внести изменения при редактировании сообщения.
- После добавления новой причины тревоги и заполнения всех полей, а так же после редактирования существующей записи, нажать "Сохранить" Сохранить.
- Для удаления причины тревоги нажать кнопку "Удалить" .

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

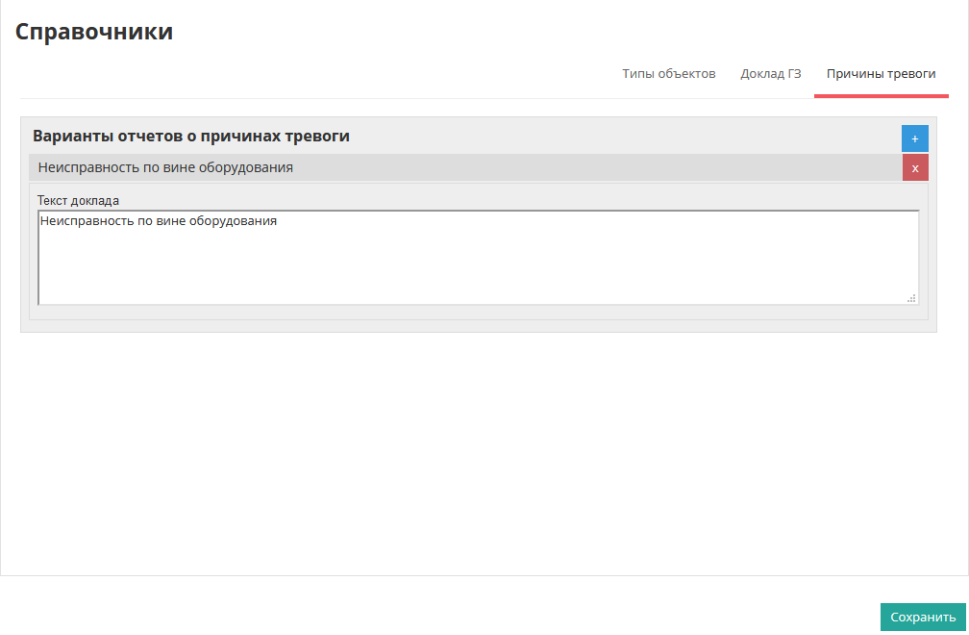


Рис. 139 Форма создания сообщений причины тревоги

9. Отчеты. Конструктор отчетов

В меню "Отчеты"(рис. 140) 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.

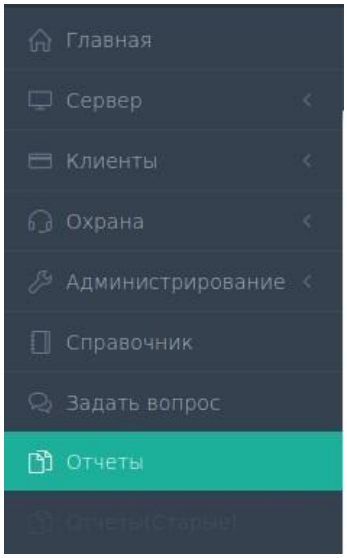


Рис. 140 Меню «Отчеты»

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

9.1 Общий вид конструктора отчетов



Рис. 141 Отчёты.

В конструкторе отчетов предусмотрены базовые, предустановленные шаблоны(рис. 141), отчетов (1). Базовые шаблоны невозможно удалить.

При нажатии на кнопку с вопросительным знаком (2), сервер КРОС перенаправит запрос на справочную статью в Википедии сервера КРОС.

Кнопка с изображением щита (3) позволяет строить отчеты по оперативным карточкам. После нажатия на кнопку с пиктограммой шестеренки (4), система открывает конструктор отчетов, в котором можно настроить форму отчета, полностью отвечающую запросам пользователя.

При открытии встроенного шаблона на редактирование (5) , будет создана копия базового отчета, с возможностью гибкой настройки полей.

9.2 Создание отчета по базовому шаблону

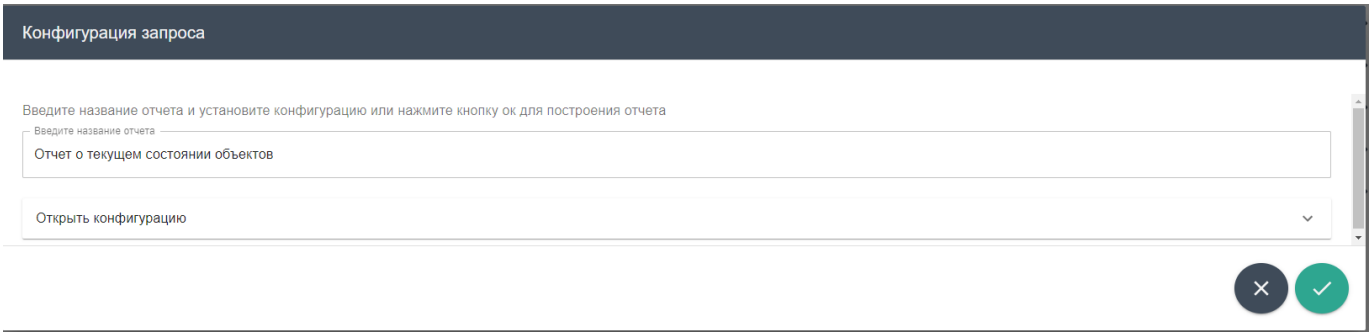


Рис.142 Форма выбора отчёта

Для построения отчета по базовому шаблону необходимо выбрать шаблон, один раз кликнуть на него левой кнопкой "мыши". Будет открыто окно, в котором необходимо задать название отчета, либо оставить стандартное (рис. 142).

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

При нажатии кнопки **"Открыть конфигурацию"** появляется возможность задавать фильтры и сортировки для отчета. Единственным обязательным для заполнения полем является поле "применить фильтр\время события", остальные поля в строке "применить фильтр" по умолчанию выберут все возможные значения. Для построения отчета необходимо нажать кнопку "Выполнить" или "Закрыть", если построение отчёта не требуется.

Так же, появляется возможность задать дополнительные параметры отчёта, для этого необходимо нажать кнопку "Добавить поле отчёта" .

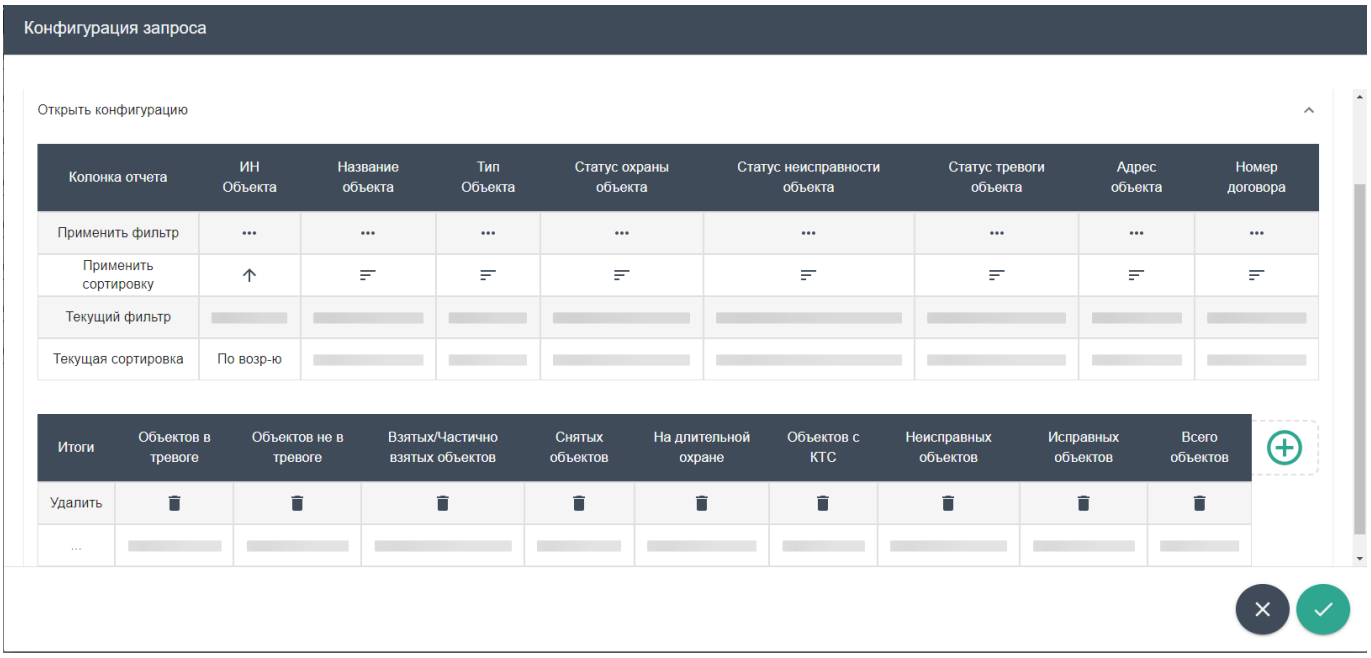


Рис. 143 Редактирование шаблона отчёта

В настройке формы отчёта (рис. 143) предусмотрены возможности:

- **Применить фильтр** - позволяет использовать фильтр на приборы, объекты, даты и некоторые другие параметры отчёта, что позволяет конкретизировать данные.
- **Удалить колонку** - Позволяет исключить данные из отчёта.
- **Применить сортировку** - Данные можно расположить по-возрастанию, по-убыванию, и оставить "как есть".
- **Текущий фильтр** - Показывает какой фильтр установлен в настоящий момент.
- **Текущая сортировка** - Показывает какая сортировка используется в настоящий момент.

Если в базовый шаблон было внесено изменения, то возможно, его потребуется сохранить.

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

9.3 Создание шаблона отчета в конструкторе отчетов

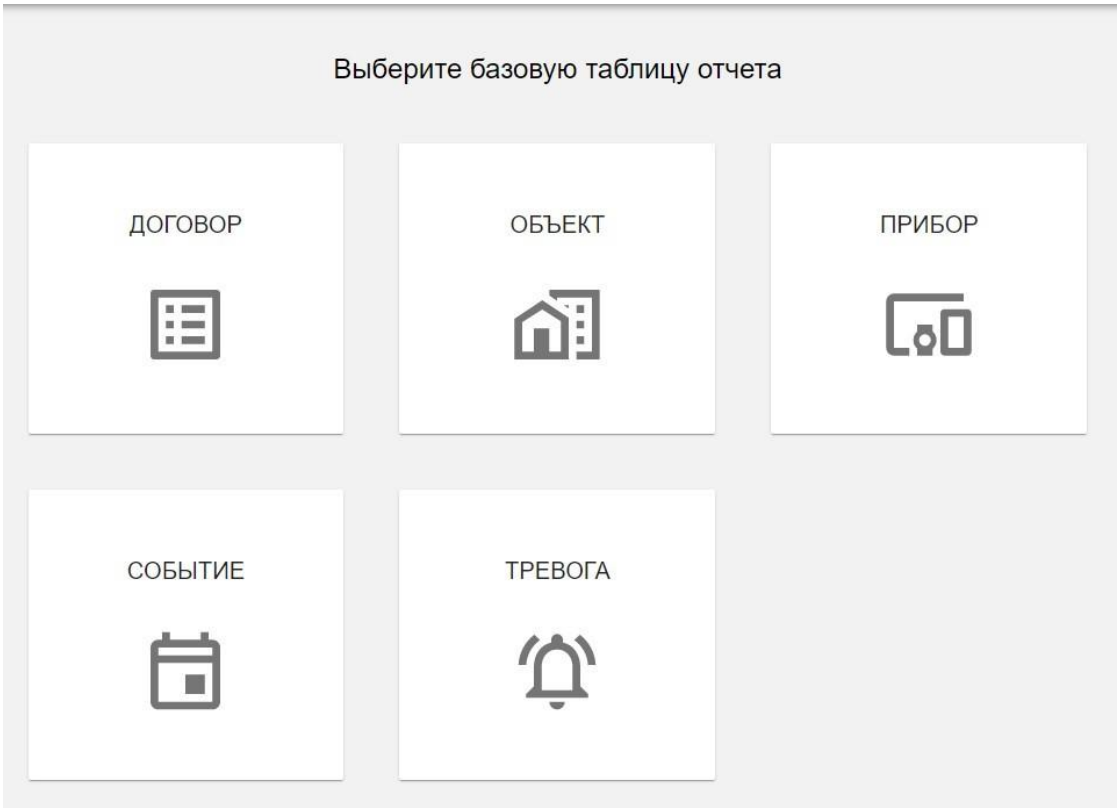


Рис. 144 Выбор базовой таблицы отчёта

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(рис. 144) для отчета. На основе этой таблицы будет построен отчет.
3. Выбрать необходимые поля(рис. 145), задать сортировки и фильтры. Ненужные колонки можно убрать, нажав на значок "Удалить" , или же включить необходимые, нажав на кнопку "Добавить" .
4. После добавления всех необходимых колонок и фильтров, шаблон отчета необходимо сохранить, для дальнейшего использования.

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

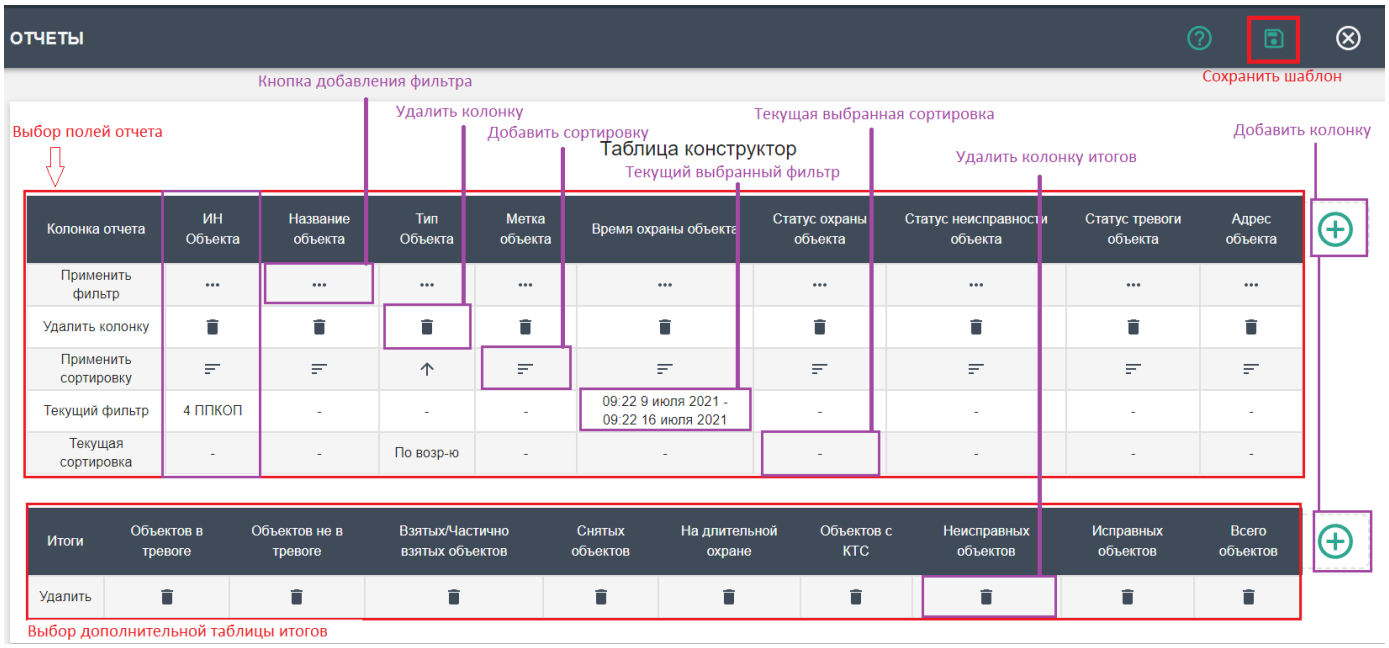


Рис. 145 Общий вид формы конструктора отчётов

9.4 Запись шаблона отчета

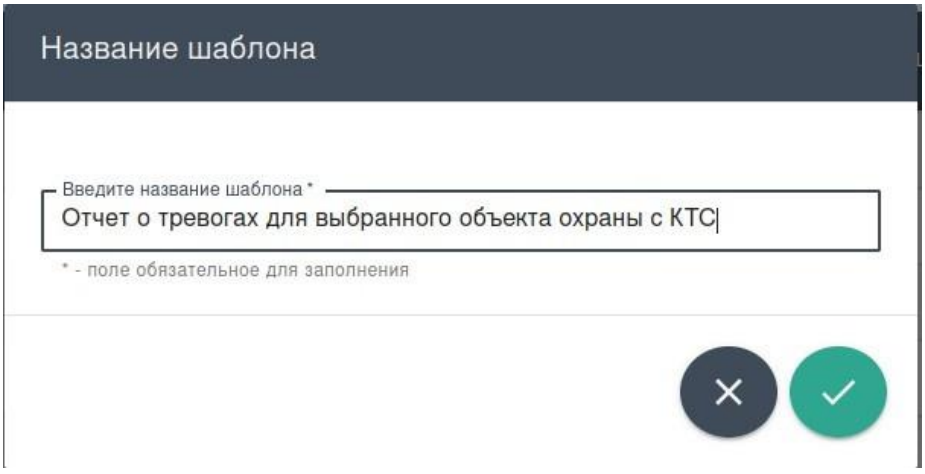


Рис. 146 Ввод наименования собственного шаблона

Если форму отчёта требуется сохранить, нажмите на символ и в открывшейся форме, 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

9.5 Оперативная карточка объекта

Для построения оперативной карточки(рис. 147) объекта необходимо:

1. Нажать на кнопку "Оперативная карточка" (1).
2. Ввести ИН объекта.(2).
3. Нажать кнопку "Подтвердить".(3).

В результате, выполненных действий, будет сформирован отчет, по указанному объекту.

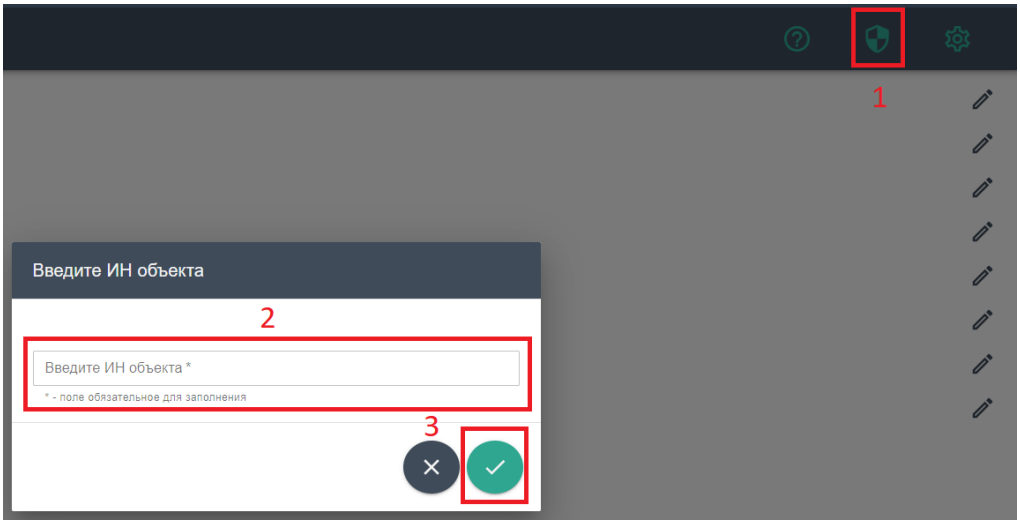


Рис. 147 Вызов оперативной карточки объекта

Основное пространство занимает тело оперативной карточки(рис. 148) (1), где отображается вся доступная по объекту информация. Для того, чтобы распечатать оперативную карточку, необходимо нажать на кнопку "Распечатать" (2) и выбрать установленный принтер. Для закрытия оперативной карточки нажать кнопку "Закрыть" (3).

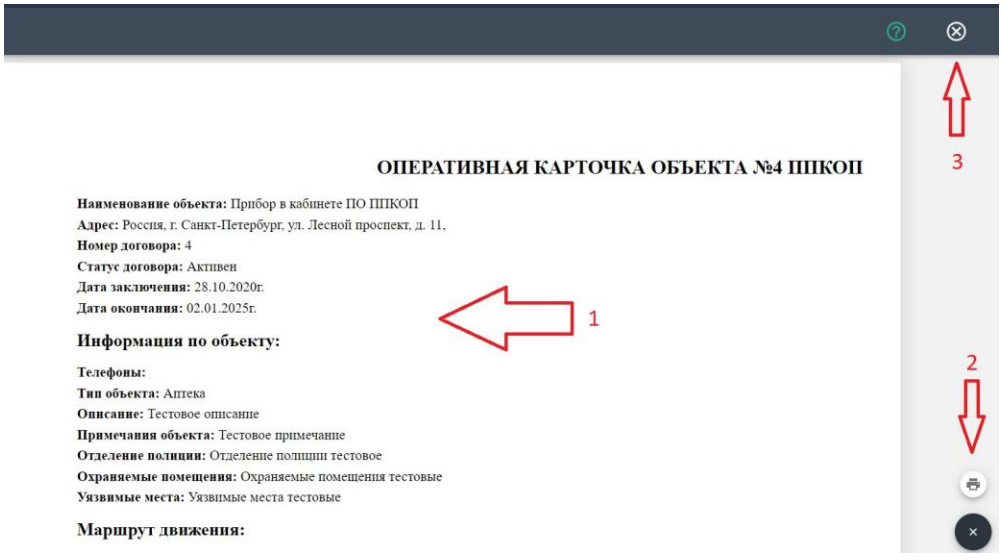


Рис.148 Оперативная карточка объекта

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

9.6 Сохранение и печать отчета

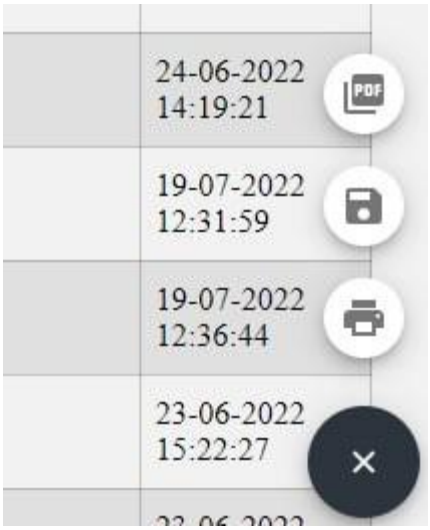


Рис. 149 Сохранение и печать отчета

После того, как отчет будет построен, в правой нижней части экрана появится символ  После наведения на него маркера "мыши" символ изменит внешний вид(рис. 149) и появится возможность:

- **Сохранить данные в формате PDF** - сохранить отчёт в формате PDF без форматирования.
- **Сохранить данные в формате CSV** - сохранить отчёт в универсальном формате электронных таблиц. Файл сохраняется в универсальной кодировке UTF-8.
- **Распечатать** - при этом открывается форма, отправки документа на печать, где можно выбрать принтер, на который следует отправить документ или драйвер конвертации документа в файл формата PDF с форматированием.

Для того чтобы выйти из текущего отчёта следует нажать на символ "Закрыть отчёт" 

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

10. Регистрация прибора на сервере КРОС

Последовательность действий при вводе прибора в эксплуатацию, определяется регламентом охранного предприятия. Последовательность может быть примерно следующая:

10.1 Оформление договора на обслуживание

Менеджер или **Администратор предприятия** заполняет форму договора на обслуживание. После создания объектов инженером, они указываются в договоре.

При создании карточки договора рекомендуется сразу указывать основные параметры договора, как то номер договора, лицо с которым заключается договор, контактные номера телефонов.

10.2 Регистрация объекта

В соответствии с договором инженерная служба обследует объект, определяет потребности в оборудовании.

После этого **инженер** заполняет карту объекта в соответствии с результатами обследования и направляет на объект **техника** для установки и настройки оборудования.

Инженер информирует менеджера о новых объектах и названиях, после чего менеджер указывает объекты в карточке договора. Так же, договор можно указать при заполнении карточки объекта.

10.3 Настройка прибора

Техник может выполнить настройку прибора, как на самом объекте, так и в помещении ОП, воспользовавшись ПО "Конфигуратор". Для подключения прибора к системе необходимо:

1. Установить в настройках прибора ключ шифрования или установить значения параметров шифрования по-умолчанию, что рекомендуется делать для корректного подключения.
2. Настроить прибор на передачу данных на сервер, указав в настройках адрес сервера и номер порта, назначенный ОО.

Если все настроено правильно то прибор сразу начинает слать данные серверу. При этом, прибор с параметрами шифрования, выставленными по-умолчанию, начинает работать в ***Инженерном Режиме***. Техник информирует инженера о подключении к системе нового прибора.

Для визуального контроля на некоторых приборах ППКОП и УОО присутствуют индикаторы «LAN», «GPRS», «DATA».

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

10.4 Активация прибора

Получив сообщение от техника и убедившись, что вновь подключенный прибор появился в списке инженерного режима, и проверив полученную с прибора конфигурацию, инженер активирует прибор. Для этого в карточке объекта нужно открыть вкладку "Приборы" и выделить прибор, установленный на объекте. После этого открыть вкладку "Зоны и разделы" - здесь будет виден список ранее подключенных разделов приборов, если таковые уже были, а также список неактивных разделов. Нужно отметить нужные разделы и сохранить информацию. После этих действий в приборе изменится "ключ шифрования" и он начнёт работать в штатном режиме, передавая сообщения на активные пульты в соответствии с правилами фильтрации. Если на приборе прописывается ключ шифрования в ручную, то в этом случае карточку учета прибора необходимо создать так же в ручную, правильно прописав его ключ шифрования и идентификатор.

Разделы одного прибора могут быть назначены нескольким объектам. Так же, на одном объекте могут находится несколько приборов.

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

11. Зеркалирование («Горячий» резерв)

11.1 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 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:

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

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.

11.2 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).

11.3 Создание трансляции

На ведущем компьютере:

1. Перейти Меню: Сервер -> Трансляции (рис. 150).
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.

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

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.

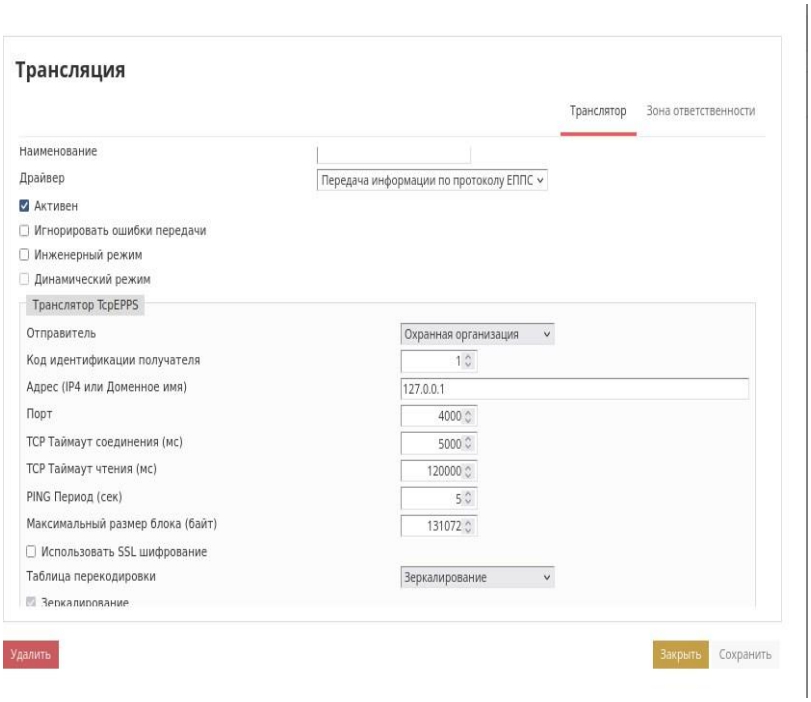


Рис. 150 Карточка создания трансляции протокола ЕППС

11.4 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 (рис. 151).

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

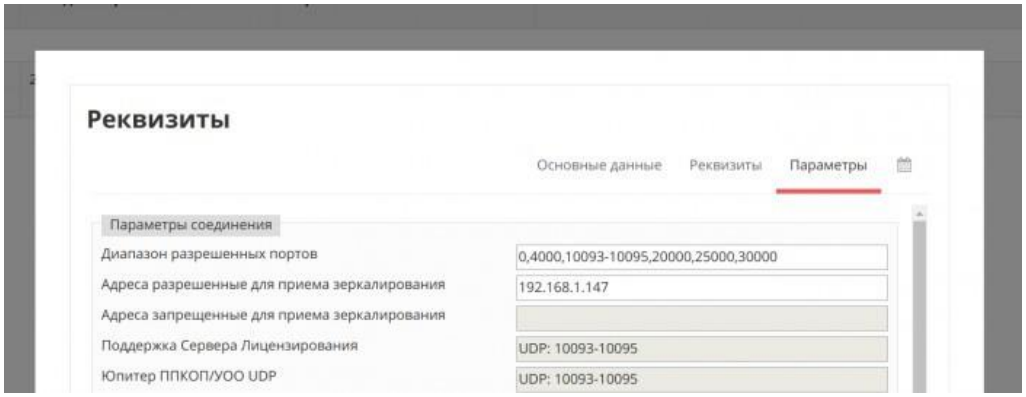


Рис. 151 Разрешение приема данных

Система зеркалирования готова к работе. Возможно потребуется несколько минут для установки первого соединения и начальной синхронизации данных.

Необходимо обратить отдельное внимание на тот момент, что при настройке взаимного зеркалирования(режим **full duplex**), в начале необходимо запустить трансляцию с основного сервера и после того, как данные будут синхронизированы, запустить трансляцию на ведомом сервере.

12. Импорт базы данных из Юпитер-7

12.1 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. Архивный zip-файл состоит из xml-файла и может содержать картинки объектов.

12.1.1 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.

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

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 в таблице «Объекты» при использовании фильтра «Импортированные» и «Групповых операций».

12.1.2 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. Обновите АРМ ДПУ до версии 7.19.0.28 или выше;

2. Войдите в АРМ ДПУ пользователем с правами администратора.
2. Откройте меню «Файл»;
3. Выберите пункт меню «Экспорт»;
4. Выберите пункт меню «Конфигурация для Юпитер-КРОС» или «Выбранные ключи для Юпитер-КРОС», если есть необходимость в переносе отдельных ключей(рис. 152);

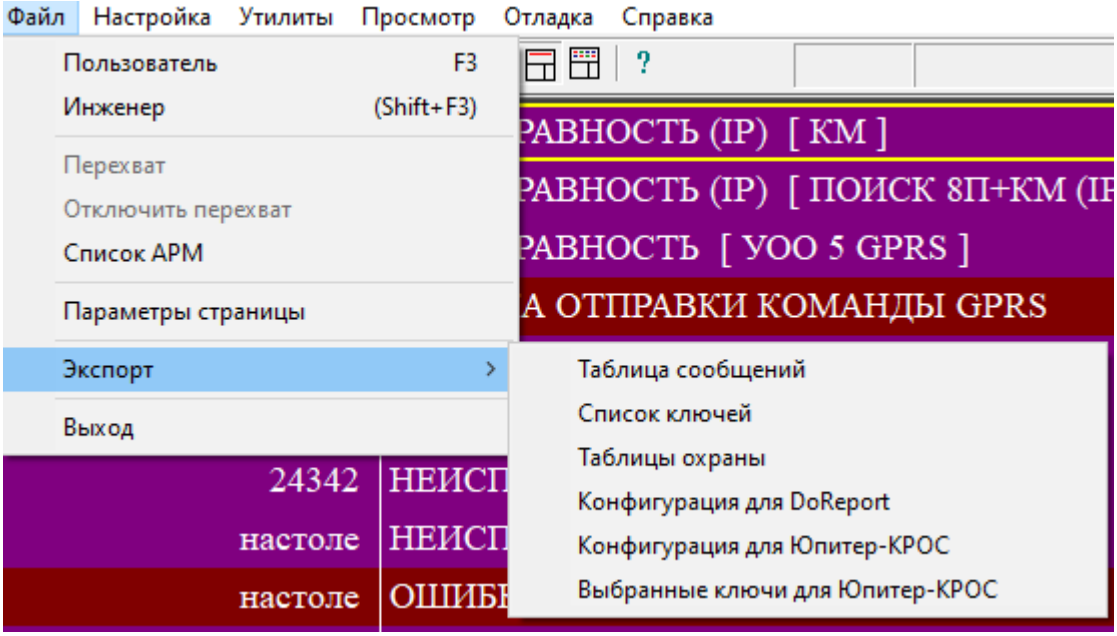


Рис. 152 Экспорт файла конфигурации для КРОС

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

12.1.2 Импорт файла конфигурации в Юпитер-КРОС

Для выгрузки базы данных Юпитер-7 в Юпитер КРОС необходимо (рис. 153):

1. Заходим под **администратором охранной организации** (admin-логин и пароль по умолчанию).
2. Переходим «Клиенты» → «Объекты»(1).
3. В правом верхнем углу нажимаем «Импорт»(2).
4. Выбираем файл с конфигурацией(3) и нажимаем «Загрузить».
5. После окончания импорта необходимо нажать «Обновить» или перезагрузить страницу.

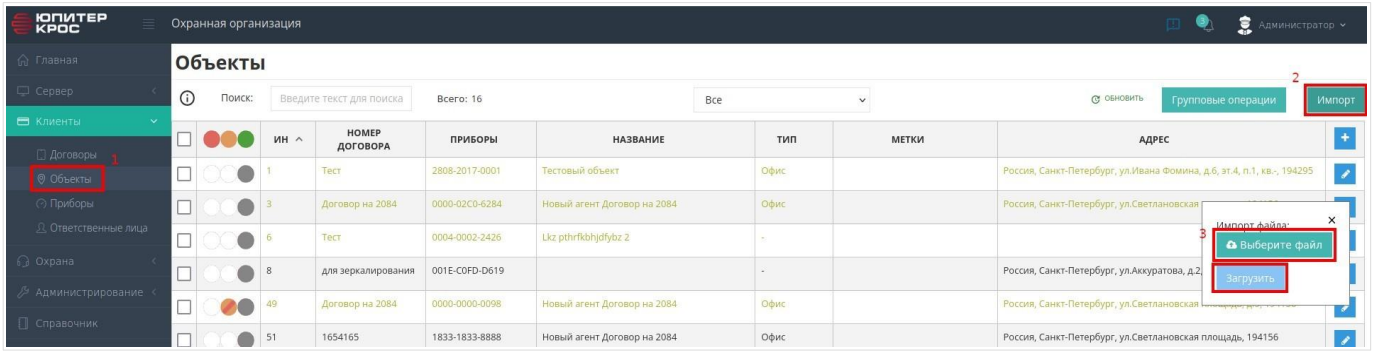


Рис. 153 Импорт базы данных из Юпитер-7

Информацию по импорту можно увидеть в http логе, расположенном на сервере в папке Log.

В приборах:

- IP/GPRS создаются 3 канала связи: ЕППС(если включена трансляция), РК4, CSD(если не отключен в настройках ОО).
- 18 кГц – ЕППС(если настроена трансляция с Юпитер-7 в КРОС)

Примечание:
Если в карточке объекта Юпитер-7 указан адрес без города, то Автоматически подставляется город из Охранной организации, а именно: «Охрана» → «Реквизиты» → Редактирование ОО → «Реквизиты» → «Юридический адрес»

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

12.1.2.1 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 -

12.2 Трансляция из Юпитер-7 в 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.
Служба технической поддержки: тел. 8-800-250-87-27 доб. 2

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

12.2.1 Настройка трансляции

Трансляция настраивается пользователелем с правами администратора.

В Юпитер-7 выбрать: «Настройки» → «Соединение с КРОС» (рис. 154).

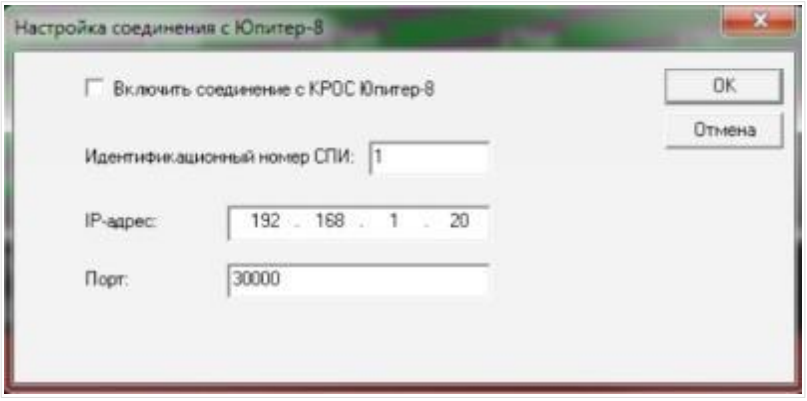


Рис. 154 Настройка трансляции с КРОС

- 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.

12.3. 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.

12.4. Замена серверов

Если трансляция с Юпитер-7 на КРОС не используется и база данных перенесена, то 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.

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.

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

13. Использование мобильного приложения «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.
5. Выбрать ответственное лицо, которому необходимо предоставить доступ к личному кабинету и открыть карточку на редактирование.
6. Открыв нужное ответственное лицо, задать ему логин и пароль на вход в личный кабинет, а также поставить галочку "Доступ в личный кабинет"(рис. 155). Прописать логин и пароль.
7. Нажать кнопку "Сохранить".

   После этих действий пользователь сможет зайти в мобильное приложение "Личный кабинет" и управлять объектом.

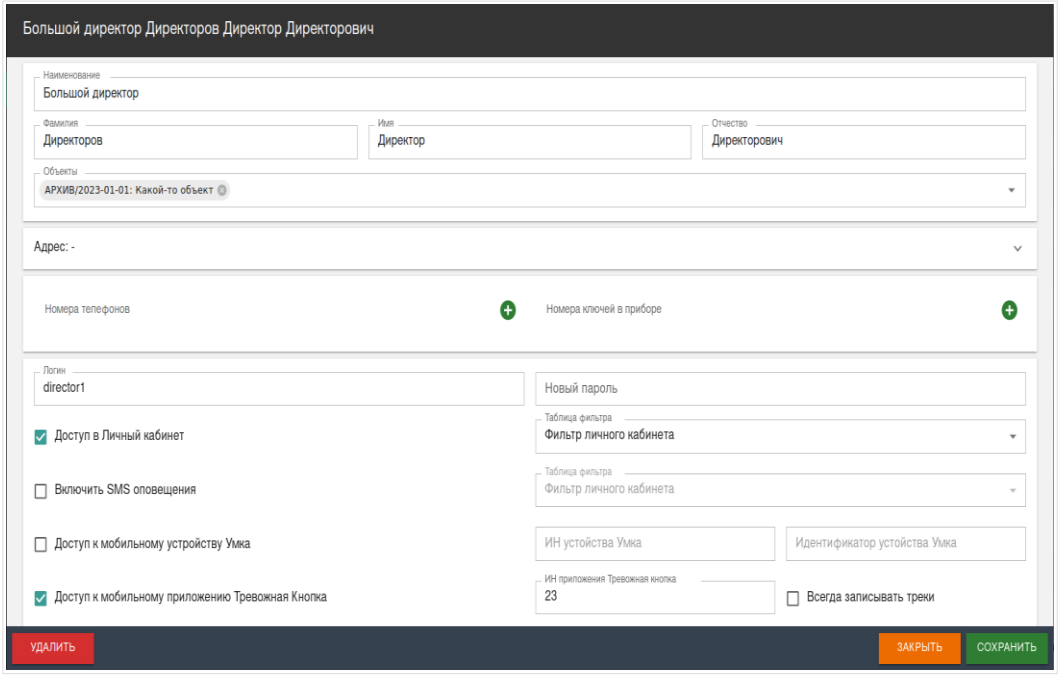


Рис. 155 Карточка ХО

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

14. Настройка часов УМКА для работы на сервере КРОС

14.1 Первоначальная настройка часов

Сервер «Юпитер-КРОС» имеет возможность работы с устройством мониторинга координат и адресной безопасности «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:

   - pw: пароль доступа к конфигурации, по умолчанию 123456.
   - 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, так как описано в разделе «Договоры».

   В договоре необходимо указать номер договора и поставить состояние договора "Активен".
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» (рис. 144).
6. Ввести ID или REGCODE часов, наклеен с оборотной стороны часов (пункт 5 на изображении выше), после чего нажимаем кнопку Сохранить. Для непрерывной записи трека часов «Умка» в настройках ответственного лица установить галочку “Всегда записывать трек перемещения”, трек начинает передаваться каждые 20 сек.

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

7. В окне регистрации(рис. 156) выбрать пункт «Перейти в Личный кабинет». В новом окне ввести логин и пароль, созданного Ответственного лица.

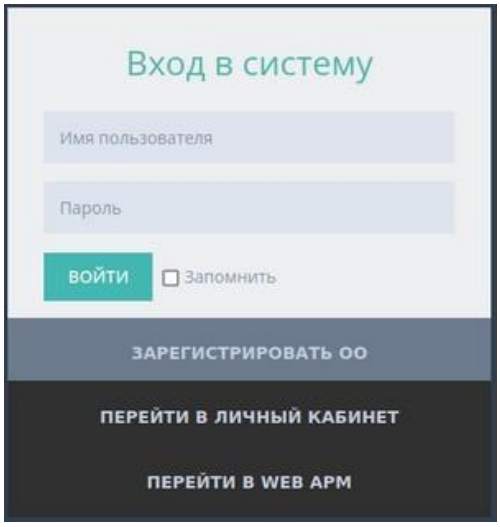


Рис. 156 Переход в личный кабинет

В результате откроется форма управления личным кабинетом (рис. 157), в которой будет отображаться мобильный Объект с названием "УМКА".

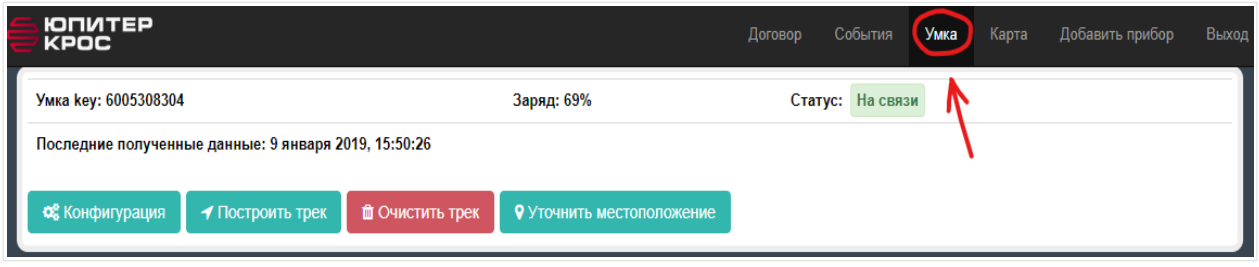


Рис.157 Отображение часов

После регистрации часов «Умка» в сервере КРОС в таблице «Приборы» появится соответствующая запись. После этого, получившийся прибор можно прикрепить к уже существующему или новому объекту.

14.2 Настройка отслеживания часов

Перед настройкой часов для работы предполагается, что первоначальная настройка часов проведена корректно согласно инструкции выше.

Для настройки часов рекомендуется выполнить следующие действия:

1. Зайти в личный кабинет созданного ответственного лица и выбираем пункт «Конфигурация» (рис. 157).

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

2. В меню "Конфигурация" устанавливаем центральный номер «SOS1», так как без него не будет работать передача координат и тревоги(рис. 158).

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.

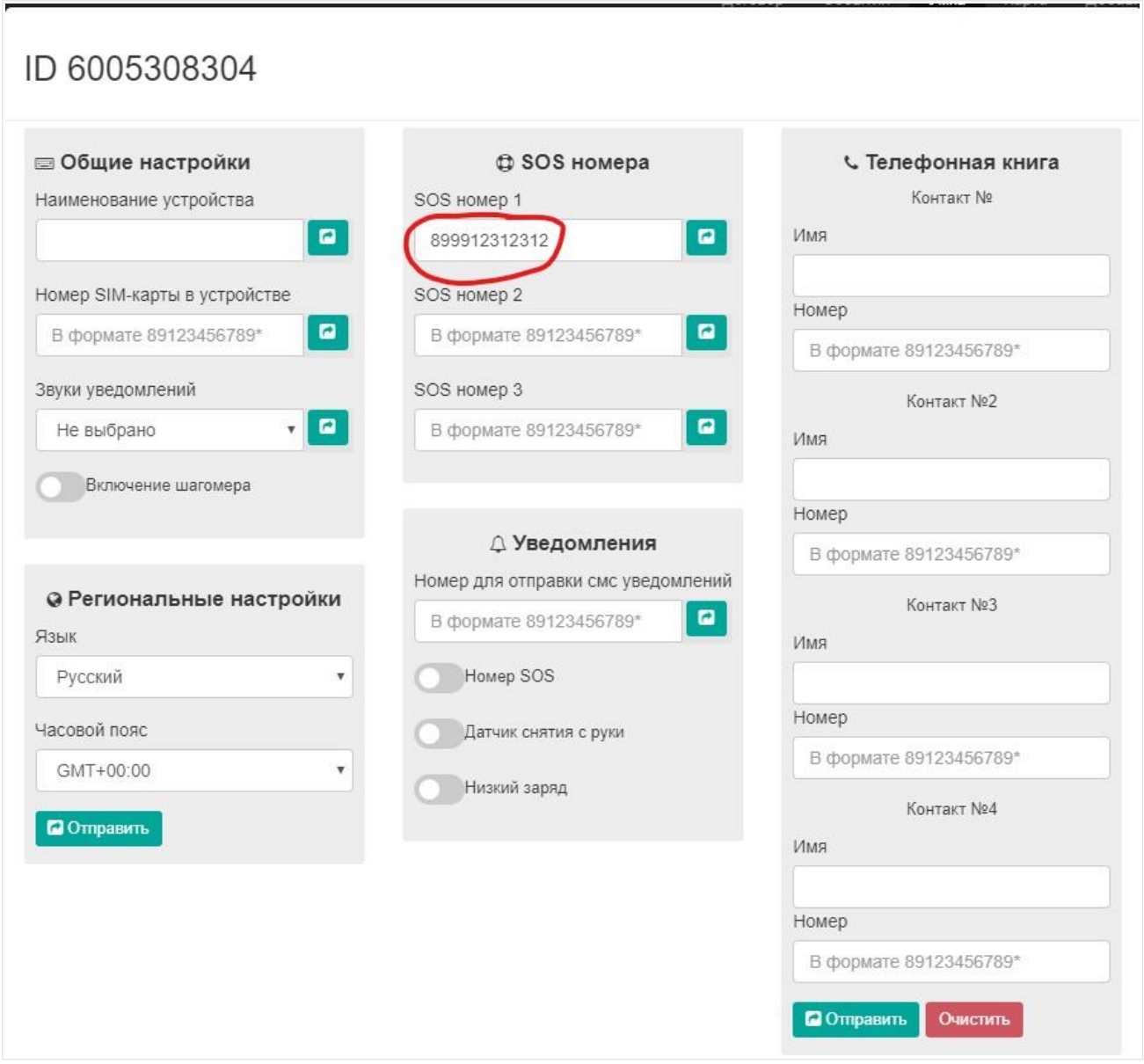


Рис. 158 Установка номера

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

3. При нажатии кнопки «SOS» на часах, на сервер КРОС отправляется тревога. Соответственно в АРМ отобразится тревога «Нападение». Так же, будет доступна информация по объекту и иная информация, в том числе и геолокация объекта.

4. Для просмотра подробной информации по тревоге необходимо дважды кликнуть на активную тревогу, после чего откроется окно тревоги.

Дальнейшее взаимодействие с тревогой происходит по тому же принципу, как и с обычной тревогой с прибора.

В случае появления ошибки «Нет подключения к сети», необходимо удостовериться в том что:

1. Часы включены.
2. Поступает входящий звонок на часы.
3. SIM-карта имеет положительный баланс и доступ в интернет.
4. Соответствие ID на часах и в личном кабинете.

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

Приложение №1. 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 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»
    - 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 Поэтапный перевод оборудования с Юпитер-7 на Юпитер-КРОС

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

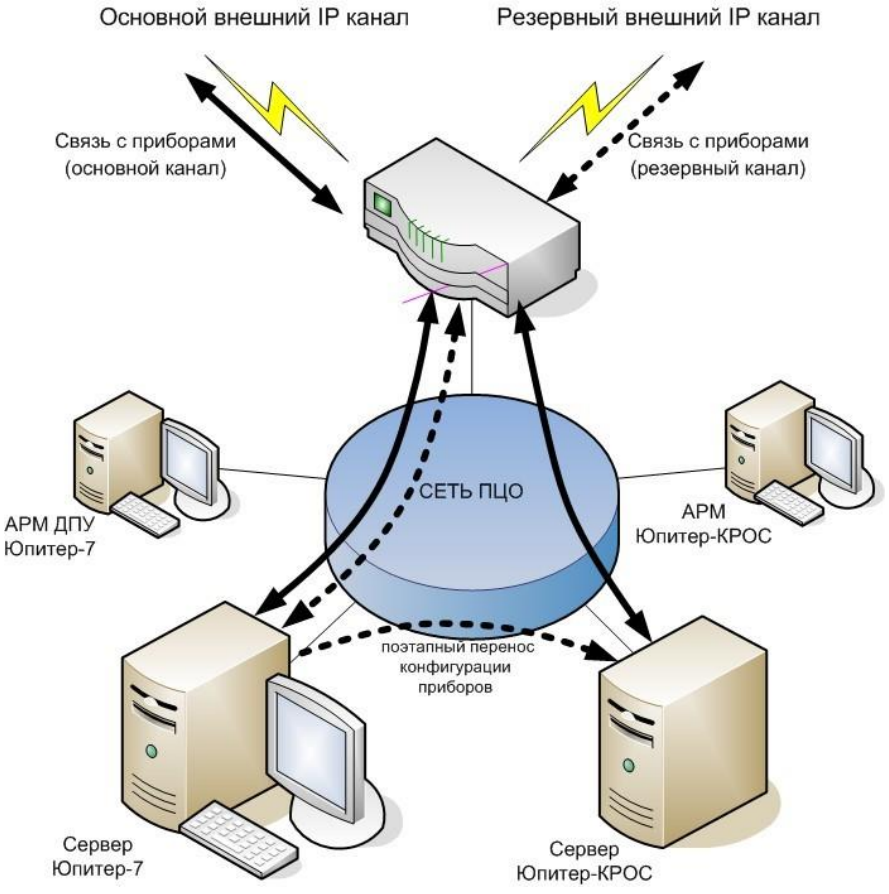


Рис. 1 Структура взаимодействия

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

Сервер Юпитер-КРОС разворачивается параллельно с существующим сервером Юпитер-7(рис. 1).

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.

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.

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

Для осуществления переноса приборов необходимо:

1. В Юпитер-7, в меню «Настройка» выбрать пункт «Перенос приборов в Юпитер-КРОС»(рис. 2).

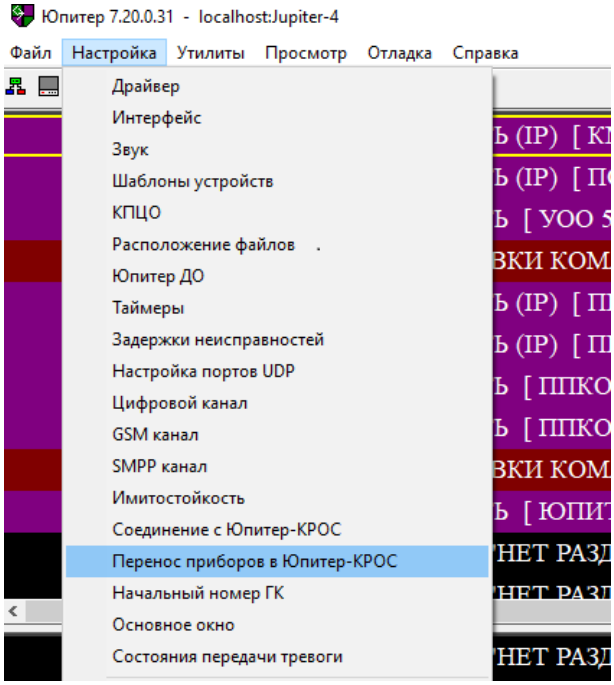


Рис. 2 Выбор режимы переноса данных

2. В появившемся окне(рис. 3) нажать на кнопку «Выбрать ключи приборов для передачи в КРОС».

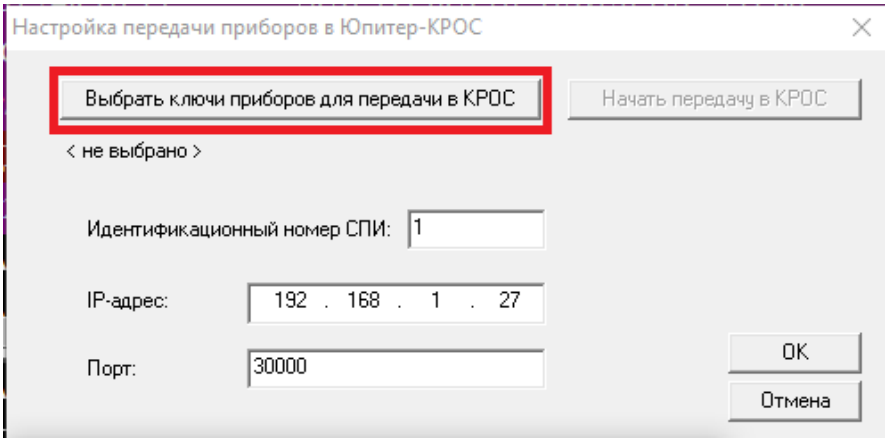


Рис. 3 Параметры подключения к серверу КРОС

3. Если какие-либо приборы не могут быть переданы в Юпитер-КРОС, то появится предупреждение с указанием причины(рис. 4).

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

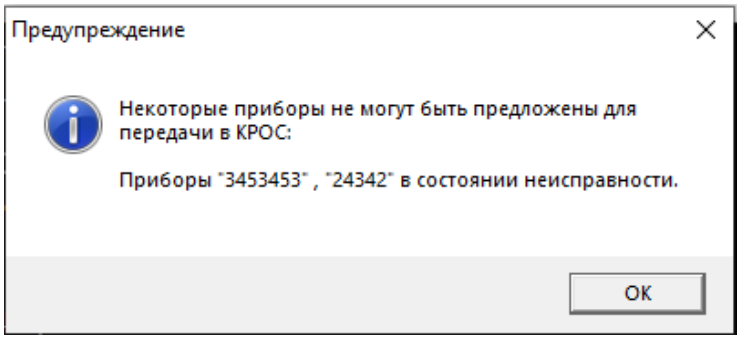


Рис. 4 Сообщение о блокировке возможности переноса приборов

4. В появившемся окне выбрать приборы(рис. 5), которые необходимо перенести в Юпитер-КРОС, и нажать кнопку «ОК».

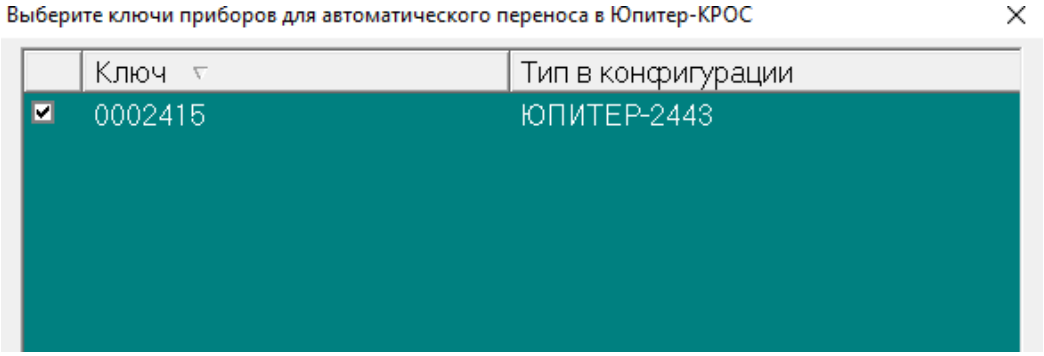


Рис.5 Форма выбора ключей для переноса в КРОС

5. Внести данные для соединения Юпитер-7 и Юпитер-КРОС(рис. 6):

a) Идентификационный номер СПИ — по умолчанию 1(необходимо указать номер ОО в КРОС)
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»

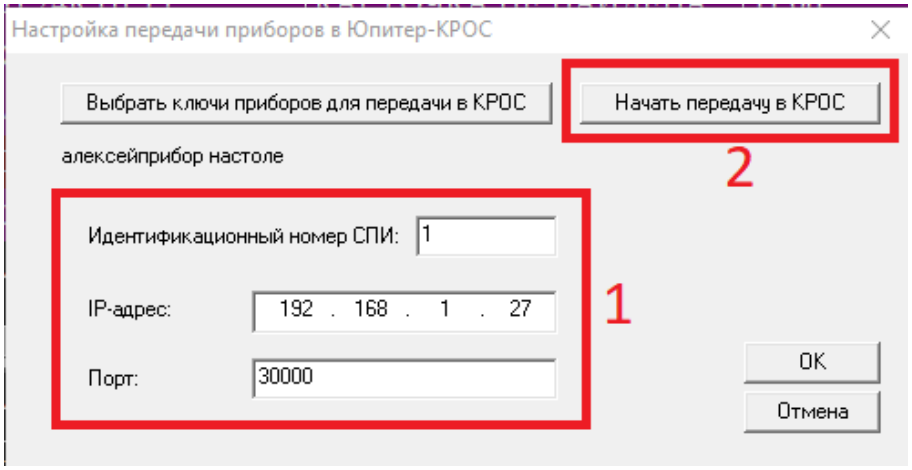


Рис 6. Перевод приборов в КРОС

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

6. После передачи команд на смену IP-адресов будет предложено заблокировать переведенные приборы в Юпитер-7(рис. 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.

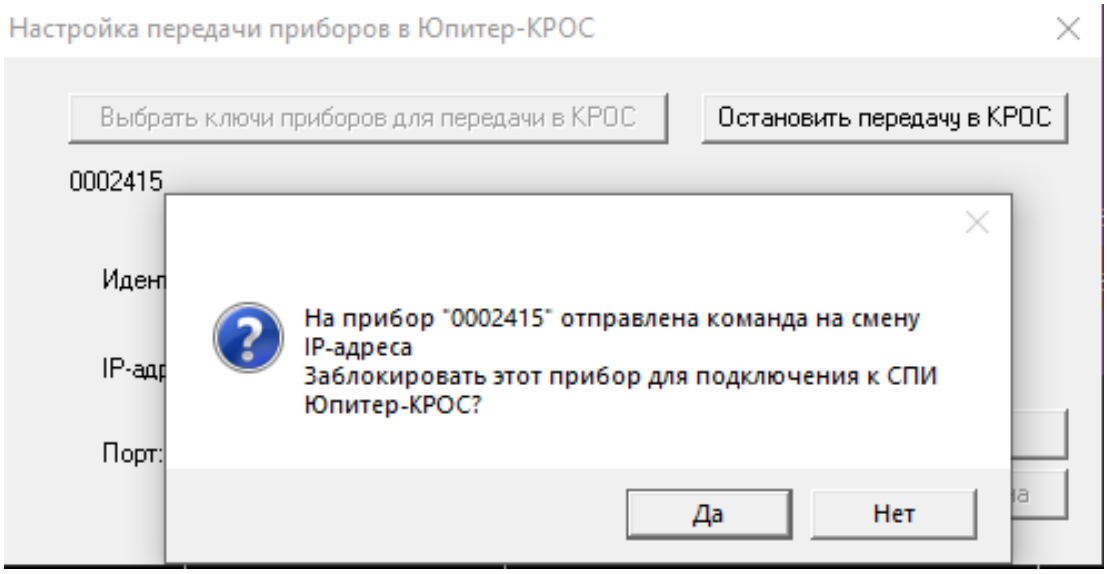


Рис.7 Результат перевода приборов в КРОС

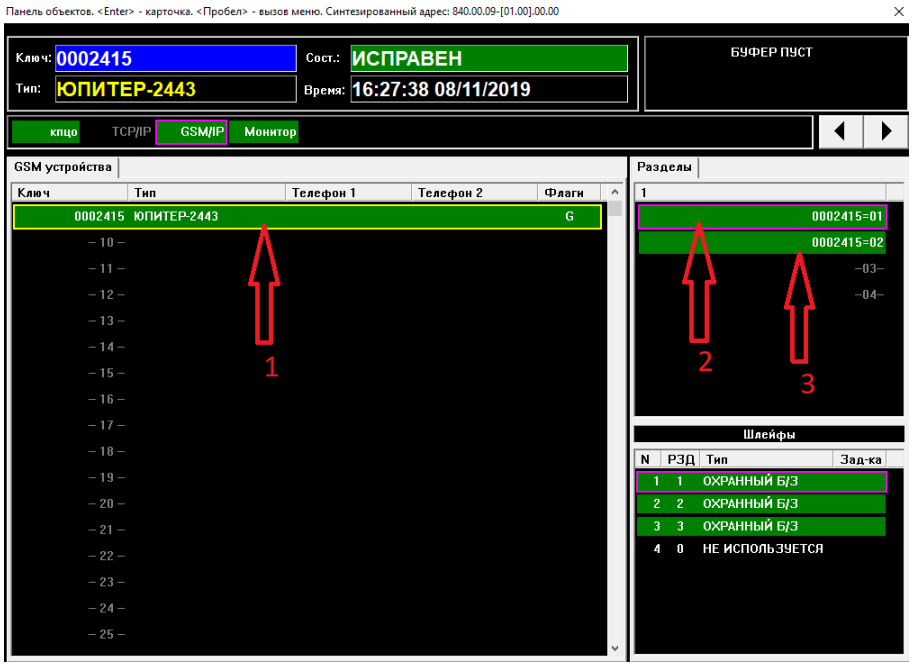
7. Необходимо зайти на сервер КРОС под учетной записью администратора охранной организации (*admin**admin* - логин и пароль по умолчанию). Импортированные в Юпитер-КРОС карточки объектов будут отображаться на сервере КРОС(рис. 8) в меню «Клиенты»→«Объекты». Из-за особенностей переноса карточек из Юпитер-7 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.

	настоле	настоле		голова прибора на столе
	настоле	настоле=01	настоле	раздел на охрану отдела по2
	настоле	настоле=02	настоле	Охрана отдела по3

Рис. 8 Таблица объектов в КРОС после импорта

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

Рис. 9 Соответствие карточек Юпитер-7 и КРОС

1 — «Головная» карточка прибора с ключом «0002415»
2 — Раздел №1 прибора «0002415»
3 — Раздел №2 прибора «0002415»

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»(рис. 10).

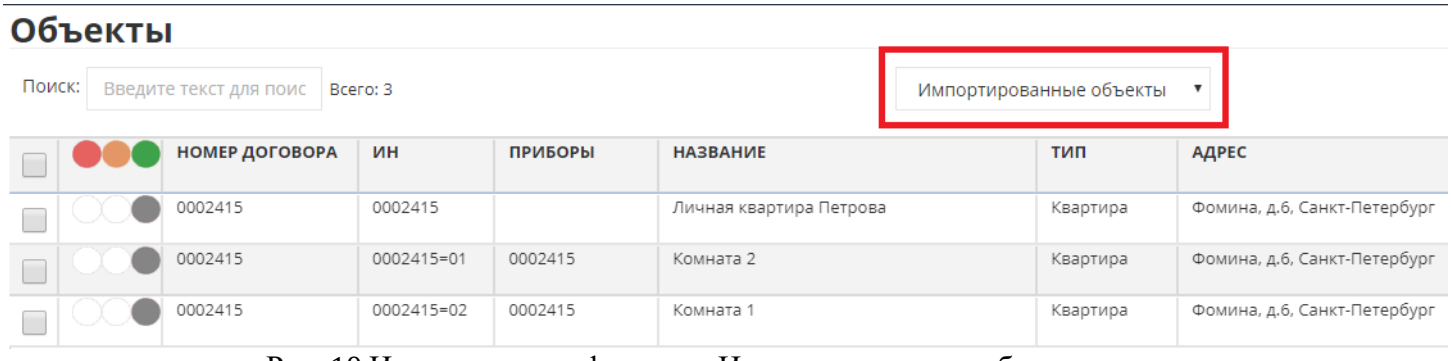


Рис. 10 Использование фильтра «Импортированные объекты»

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

Выбрать все карточки объекта, который необходимо объединить, после чего нажать кнопку «Групповые операции» и кнопку «Объединить»(рис. 11).

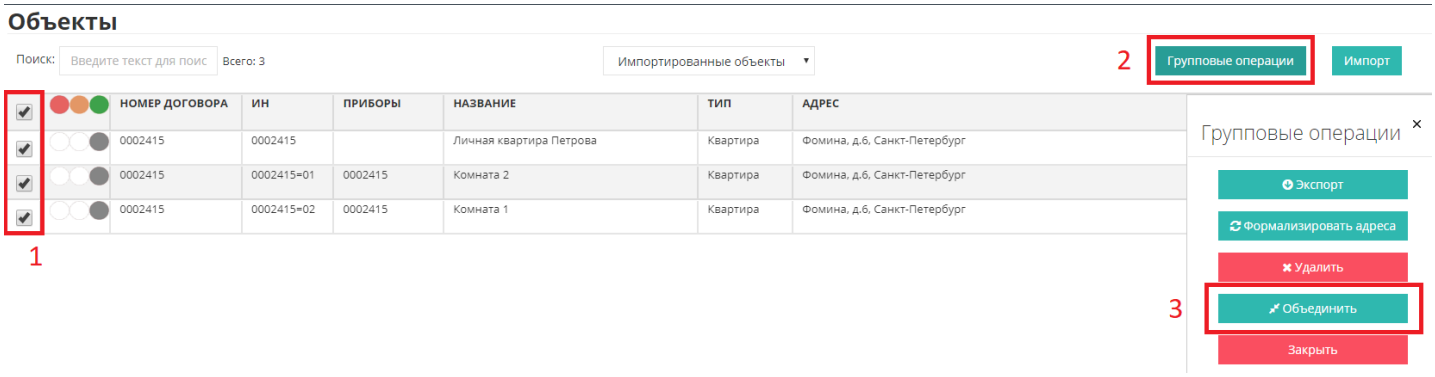


Рис. 11 Порядок действий при объединении импортированных записей

8.1. Откроется окно объединения карточек(рис. 12).
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».

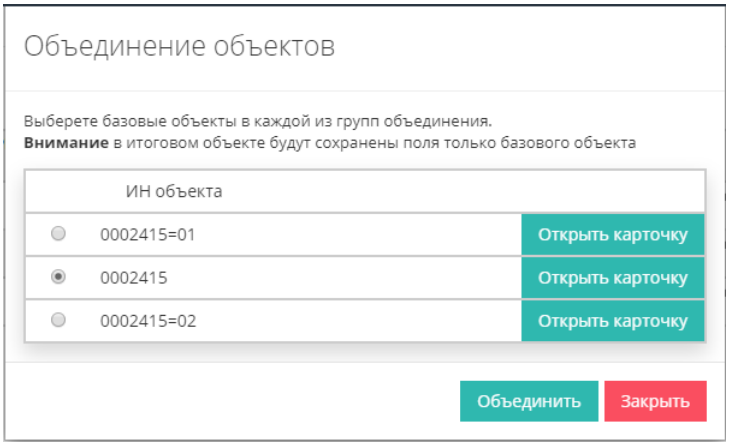


Рис. 12 Форма объединения записей

8.2. Будет запрошено подтверждение операции(рис. 13). Нажать «Да».

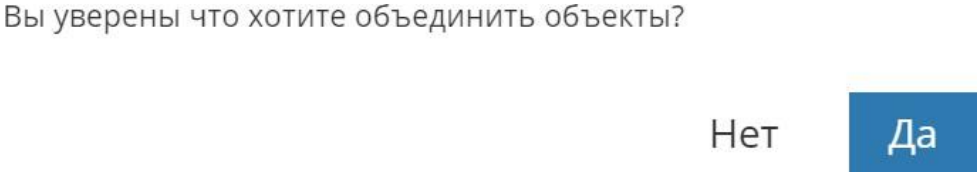


Рис. 13 Запрос на подтверждение операции

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

8.3. После объединения карточка прибора изменит свой вид(рис. 14):

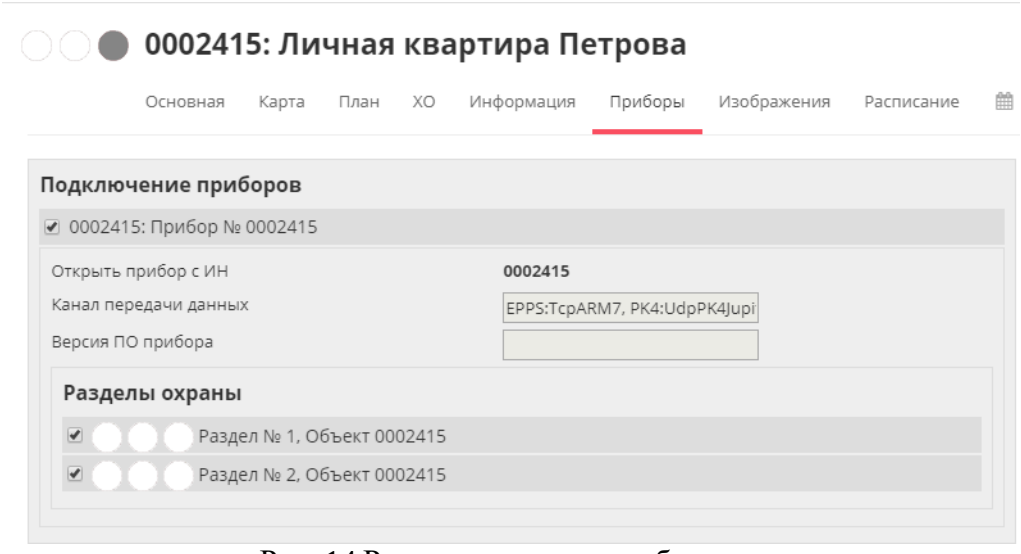


Рис. 14 Результат операции объединения

В результате, остаётся только одна карточка объекта к которой привязаны разделы прибора.

9. 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(рис. 15).
Для этого нужно:

a) Выбрать приборы(1), в которых необходимо поменять IP-адреса
b) Нажать кнопку «Групповые операции»(2), далее выбрать вкладку «Смена IP»(3)
c) Внести резервный IP-адрес и порт(4); в поле №1 внести основной IP-адрес и порт, в поле №2 внести резервный IP-адрес и порт, в поле №3 удалить информацию.
d) После внесения адресов и портов нажать кнопку «Установить параметры»(4).
e) 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.

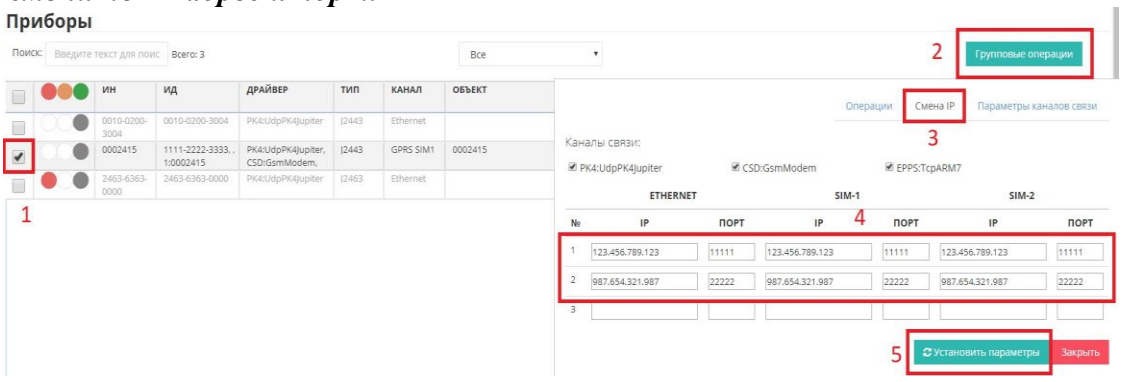


Рис. 15 Изменение IP-адреса сервера приёма сообщений в приборах

Данный механизм позволяет осуществить поэтапный перенос объектов. Когда процесс переноса будет завершен, сервер Юпитер-7 может быть отключен.

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