

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего образования  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
по выполнению лабораторных работ  
по дисциплине  
**ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ ОБЪЕКТОВ**

Направление подготовки	<b>10.03.01 Информационная безопасность</b>
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

## ВВЕДЕНИЕ

Учебное пособие предназначено для студентов очной формы обучения направления 10.03.01 «Информационная безопасность».

В методических указаниях содержатся рекомендации по изучению курса и выполнению лабораторных работ.

Состав и оформление отчётов приводится в соответствие с действующими на сегодняшний день нормами и требованиями государственных стандартов РФ.

## Содержание

<b>Лабораторная работа №1.</b> Изучение системы охранной сигнализации на базе оборудования «Болид». Настройка тактики работы системы охранной сигнализации при помощи программы «Pprog» .....	3
<b>Лабораторная работа №2.</b> Изучение системы Орион Про на базе оборудования «Болид». Настройка уровней доступа для охранной системы при помощи программы «Pprog» .....	12
<b>Лабораторная работа №3.</b> Изучение системы Орион Про на базе оборудования «Болид». Настройка паролей для охранной системы при помощи программы «Pprog» .....	19
<b>Лабораторная работа №4.</b> Конфигурирование системы контроля и управления доступом на базе контроллера доступа С2000-2» .....	29
<b>Лабораторная работа №5.</b> Программирование proximity-карт с помощью контроллера «С2000-2» .....	46
<b>Лабораторная работа №6.</b> Настройка тактики работы системы оповещения при помощи программы «Pprog» и «UProg» .....	61
<b>Лабораторная работа №7.</b> Определение угла обзора видеокамеры .....	92
<b>Лабораторная работа №8.</b> Исследование светового индикатора состояния извещателя охранного в составе охранного шлейфа сигнализации ПКПОП «Сигнал 20М» .....	96
<b>Лабораторная работа №9.</b> Настройка передачи тревожных извещений на базе контроллера охранно-пожарного «Приток-А-КОП-02» .....	102
<b>Приложение</b> .....	124
<b>Литература</b> .....	129

## Лабораторная работа №1

**Тема: Изучение системы охранной сигнализации на базе оборудования «Болид». Настройка тактики работы системы охранной сигнализации при помощи программы «Prrog».**

**Цель работы:** научиться настраивать параметры и тактику работы интегрированной системы «Орион» для системы охранной сигнализации.

### Краткая теория.

Охранная сигнализация – совокупность технических средств для обнаружения появления нарушителя на охраняемом объекте и подачи извещения о тревоге для принятия мер по задержанию нарушителя.

Из определения можно выделить несколько основных задач охранной сигнализации:

Обнаружение нарушителя;

Формирование извещения об обнаружении нарушителя в нужном информационном формате;

Передача извещения в нужном формате в определённое место;

Обеспечение процедуры постановки на охрану и снятия с охраны (взятия/снятия).

Термины и определения

Извещатели - приборы для обнаружения нарушителя. Имеют чувствительные элементы, реагирующие на определённые признаки нарушителя в зоне обнаружения.

Приемно-контрольные приборы (ПКП) – многофункциональные устройства для приёма сигналов от извещателей по шлейфам сигнализации, включения световых и звуковых оповещателей, выдачи информации на пульты централизованного наблюдения, обеспечения процедуры

поставки/снятия с помощью органов управления. В качестве органов управления можно использовать выносные и встроенные пульты и клавиатуры с секретными кодами, а также считыватели совместно с электронными идентификаторами (карточками и ключами).

Оповещатели – устройства для оповещения людей о тревоге на объекте с помощью звуковых или световых сигналов.

Пульты централизованного наблюдения – технические средства (совокупность технических средств), устанавливаемые в пункте централизованной охраны для приёма от приборов (систем) передачи извещений сообщений о тревоге на охраняемых объектах.

Неадресная система охранной сигнализации.

Для построения неадресной охранной сигнализации в ИСО «Орион» можно применить следующие приёмно-контрольные приборы с контролем радиальных неадресных шлейфов сигнализации:

- С2000-4;
- Сигнал-20П;
- Сигнал-20М.

Приборы С2000-4, Сигнал-10 и Сигнал-20М могут работать в автономном режиме, или объединяться с помощью сетевого контроллера (пультов «С2000», «С2000М» или «С2000-КС»). Прибор Сигнал-20П работает только совместно с сетевым контроллером.

Особенностью приборов является возможность программирования (конфигурирования) параметров шлейфов сигнализации, режимов работы релейных выходов, алгоритмов постановки/снятия с охраны.

В зависимости от типа подключаемых извещателей и для удобства управления процедурой постановки/снятия любому шлейфу этих приборов может быть присвоен один из типов:

- Тип 4. Охранный;

- Тип 5. Охранный с распознаванием нарушения блокировочного контакта извещателя;
- Тип 7. Охранный входной;
- Тип 11. Тревожный.

Каждый приёмно-контрольный прибор имеет релейные выходы. Тактику работы любого релейного выхода можно запрограммировать, как и привязку срабатывания (от конкретного шлейфа или от группы шлейфов).

Адресная система охранной сигнализации.

Как правило, адресные системы охранной сигнализации всегда используются совместно с сетевым контроллером (пультом или АРМом). Для построения адресной охранной сигнализации используется контроллер двухпроводной линии связи «С2000-КДЛ» и адресные извещатели:

- «С2000-ИК» - охранный объёмный оптико-электронный извещатель;
- «С2000-ШИК» - охранный оптико-электронный поверхностный;
- «С2000-ПИК» - охранный объёмный потолочный оптико-электронный извещатель;
- «С2000-СТ» - охранный поверхностный звуковой извещатель;
- «С2000-В» - охранный вибрационный поверхностный извещатель;
- «С2000-СТИК» - охранный совмещённый объёмный оптико-электронный и поверхностный звуковой извещатель;
- «С2000-СМК» - охранный магнитоконтактный извещатель («С2000-СМК Эстет» в исполнении для металлических дверей);
- «С2000-КТ» - тревожная кнопка;

Для управления различными исполнительными устройствами (например, световыми и звуковыми могут использоваться сигнально-пусковые блоки «С2000-СП2» и/или «С2000-СП2» исп. 02.

Также в адресную линию контроллера «С2000-КДЛ» можно включать адресные расширители, к которым, в свою очередь, могут подключаться не адресные извещатели с питанием от отдельного источника.

На основе «С2000-КДЛ» и адресных извещателей, а также пульта и обычных неадресных приёмно-контрольных приборов можно построить комбинированную систему охранной сигнализации.

Логика работы адресной системы такова. «С2000-КДЛ» опрашивает подключенные к нему адресные устройства. Когда извещатель формирует сигнал нарушения контролируемой зоны (например, размыкание магнитоконтактного извещателя), «С2000-КДЛ» передаёт сетевому контроллеру (пульту и/или АРМу) соответствующее событие («Тревога входа», «Тревога проникновения»).

В зависимости от типа подключаемых извещателей и для удобства управления процедурой постановки/снятия любому шлейфу этих приборов может быть присвоен один из типов:

- Тип 4. Охранный;
- Тип 5. Охранный с распознаванием нарушения блокировочного контакта извещателя;
- Тип 7. Охранный входной;
- Тип 11. Тревожный;

Адресная система охранной сигнализации под управлением пульта.

Одним из главных критериев построения охранной сигнализации с помощью адресной системы является задача определения места проникновения нарушителя с точностью до места установки сработавшего извещателя, так как в адресной системе каждый извещатель имеет

уникальный адрес. Осуществлять управление такой системой можно как с пульта, так и с помощью бесконтактных идентификаторов или бесконтактных Proху-карт со считывателя, подключенного к контроллеру двухпроводной линии «С2000 КДЛ». При использовании функции управления взятием/снятием со считывателя в память «С2000 КДЛ» можно занести до 512 кодов ключей пользователей. К контроллеру можно подключать любые считыватели ключей Touch Memory или бесконтактных Proху-карт, имеющие на выходе интерфейс Touch Memory (например, «Считыватель-2», «С2000 Proху», «Proху-2А», «Proху-3А» и т. д.). Также при использовании адресной системы нет необходимости подводить отдельно питание к каждому извещателю, так как они питаются непосредственно от двухпроводной линии связи.

В зависимости от типа, используемого извещателя, его зоне можно задать любой тип — 4, 5, 7, 11, а также любые дополнительные параметры. Управлять различными исполнительными устройствами (лампами, сиренами и т. п.) возможно при использовании дополнительных релейных модулей «С2000 СП2» (выходы типа «сухой» контакт) и «С2000 СП2 исп. 02» (выходы с контролем линии на КЗ и обрыв), которые имеют по два реле. С помощью релейных выходов можно также осуществлять передачу извещений на ПЦН. В этом случае релейные выходы сигнально-пусковых блоков включаются в так называемый шлейф «общей тревоги» прибора передачи извещений. Например, при использовании «УО-4С» или «УО-4К» реле можно включить прямо в шлейф сигнализации этих устройств, симитировав таким образом охранный извещатель. Для реле определяется тактика работы, например, включить при тревоге. Таким образом, при переходе прибора в режим «Тревога проникновения» реле замыкается, нарушается шлейф общей тревоги и происходит передача тревожного извещения на ПЦН.

Также на приборе имеются функциональные индикаторы работы и состояния линий связи (RS-485 и ДПЛС). В качестве сетевого контроллера в



такой системе используется пульт и/или компьютер с установленным на нём АРМ «Орион Про».

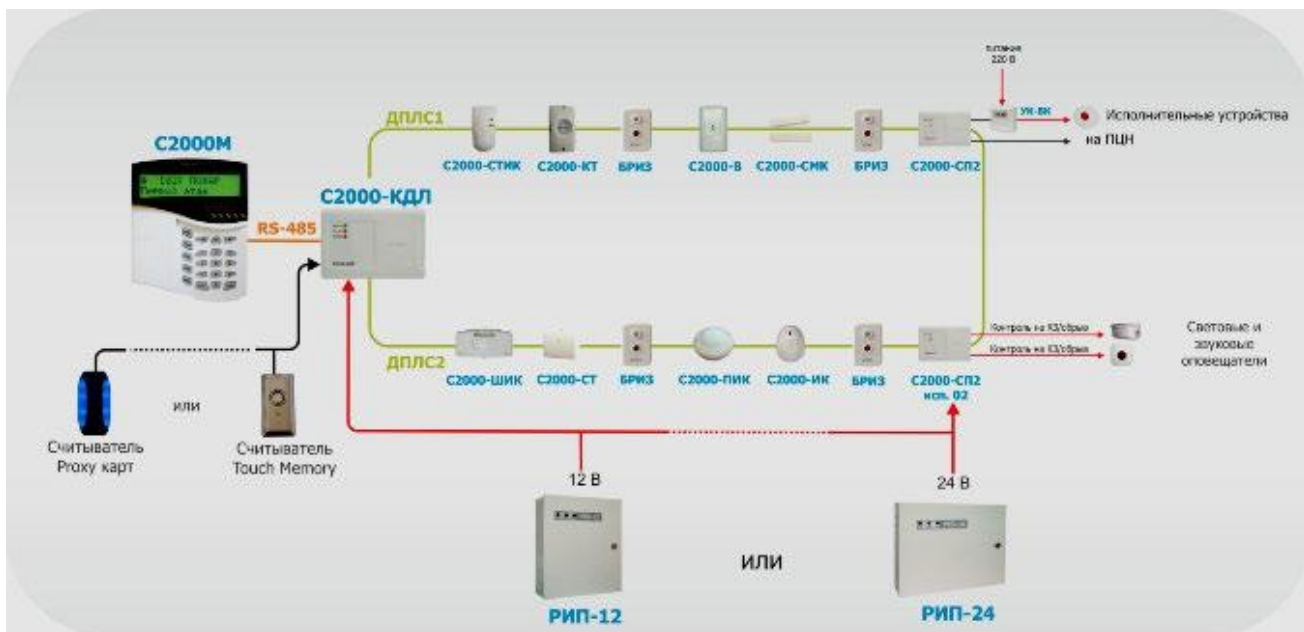


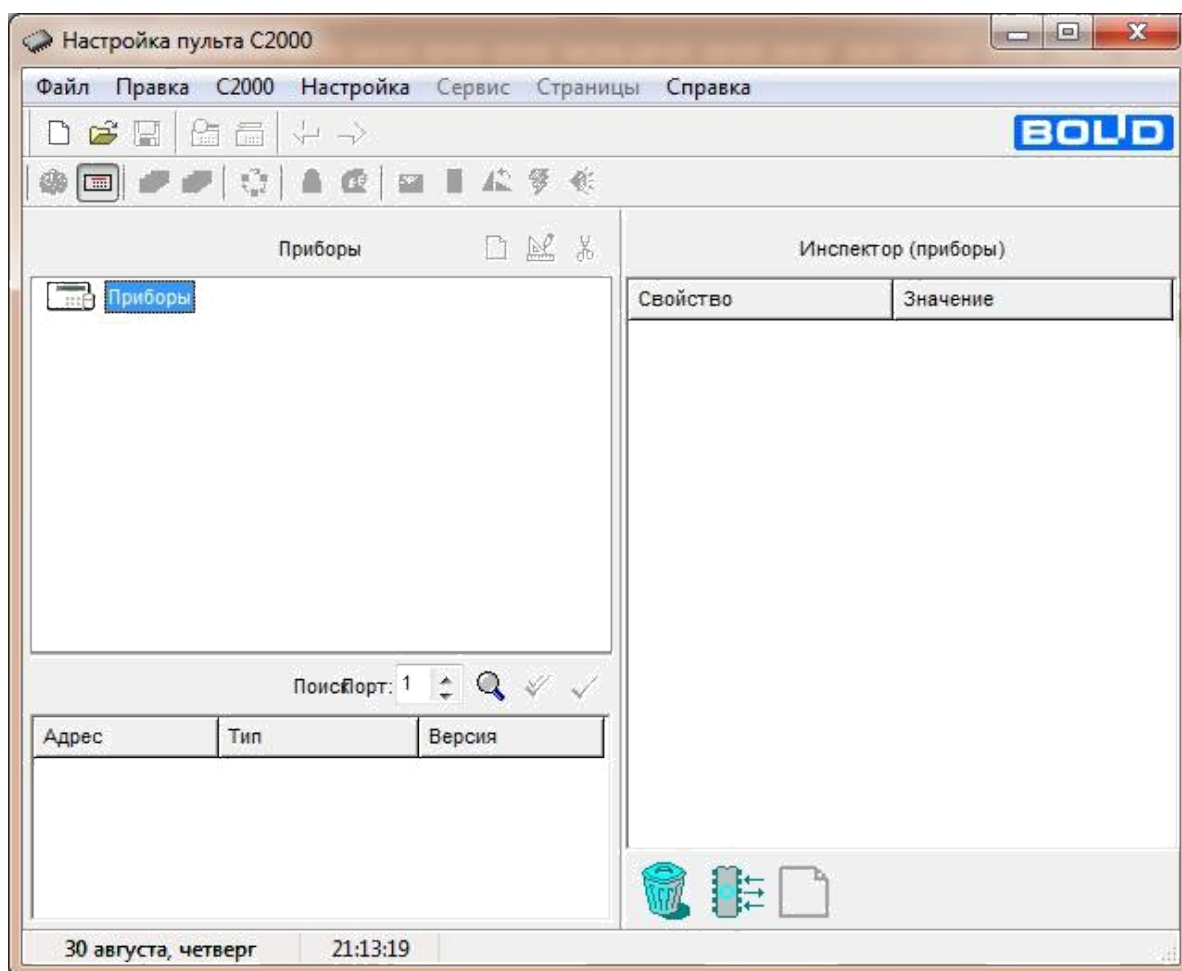
Рисунок 3. Адресная система охранной сигнализации

### Задание к лабораторной работе:

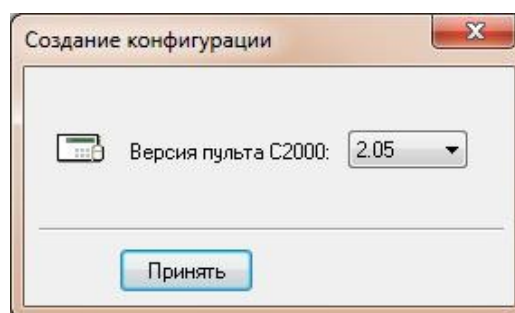
1. Расставить охранные извещатели на плане согласно вашему варианту (см. Приложение А).
2. Задать адрес каждому охранным извещателю.
3. Открыть Pprog.exe
4. Добавить прибор приемно-контрольный охранно-пожарный.
5. Создать разделы для системы охранной сигнализации.
6. Настроить тактику работы реле для включения оповещения.
7. Записать конфигурацию в прибор С2000М.


### Порядок выполнения работы:


Запустить программу «Pprog.exe»

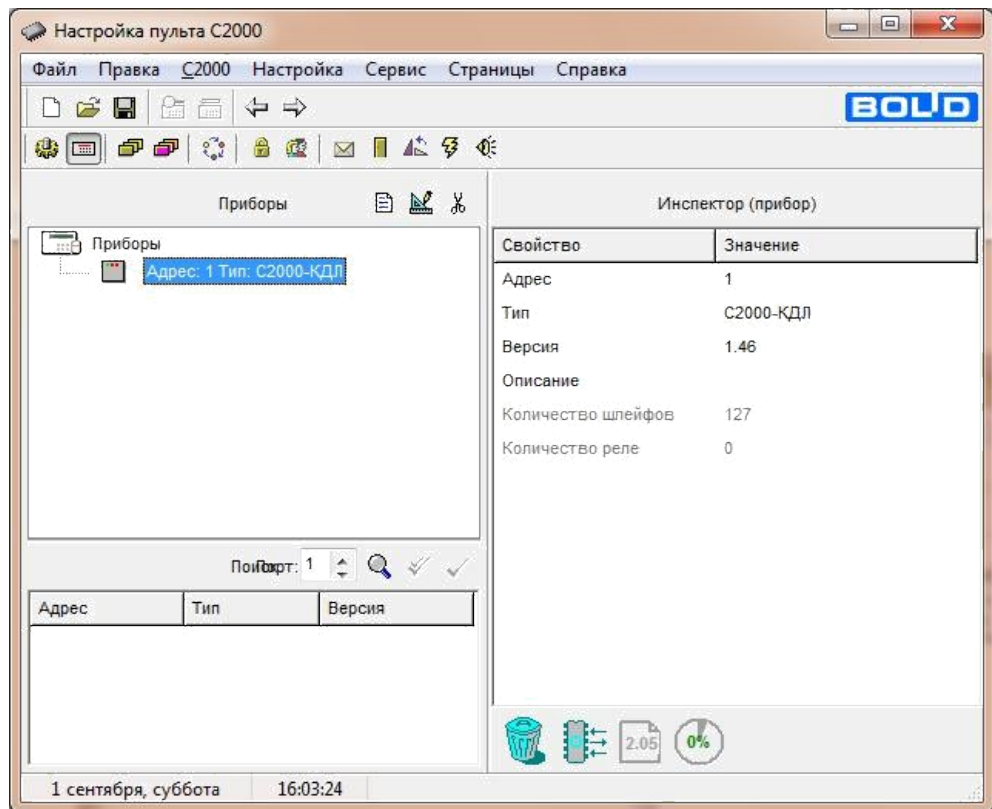





Создать новую конфигурацию при помощи кнопки 



Добавить новый прибор при помощи  кнопки

При помощи кнопки «Править прибор»  в инспекторе приборов изменить свойства и значения прибора. Выбираем тип прибора С2000-КДЛ, потом, согласно исходным данным адресов и версий приборов интегрированной системы «Орион» используемые на стенде, записываем адрес С2000-КДЛ и его версию.

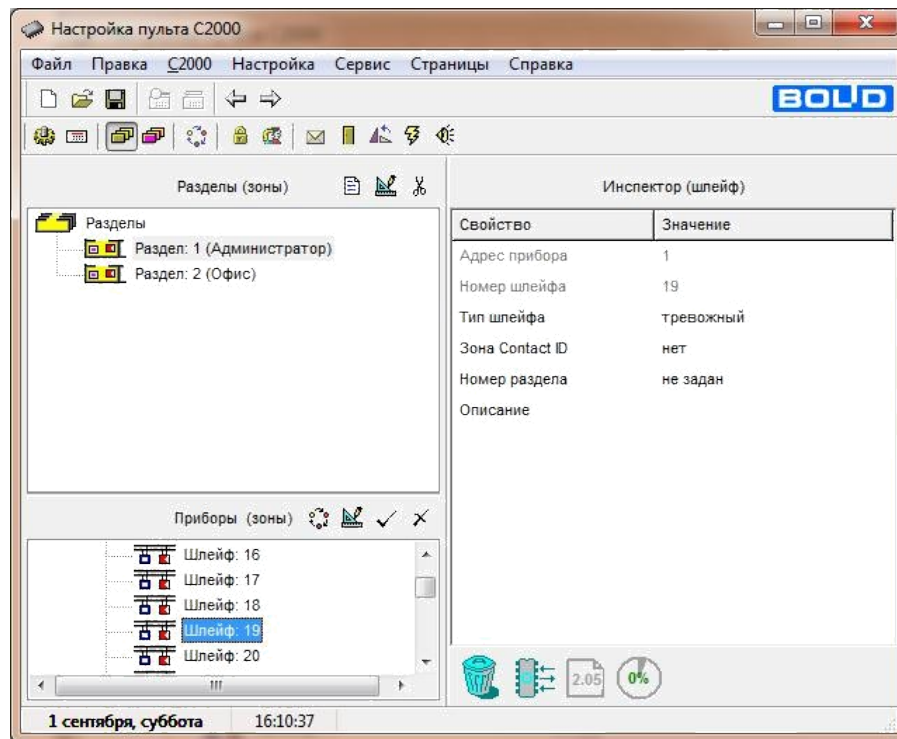





Во вкладке «Разделы» в зоне «Разделы»  добавить несколько разделов при помощи кнопки  и дать им название при помощи кнопки  (согласно индивидуальному заданию).

В зоне «Приборы» раскрыть список шлейфов С2000-КДЛ и согласно исходным данным адресов охранных извещателей интегрированной системы «Орион» используемые на стенде задать тип охранного извещателя (согласно индивидуальному заданию):

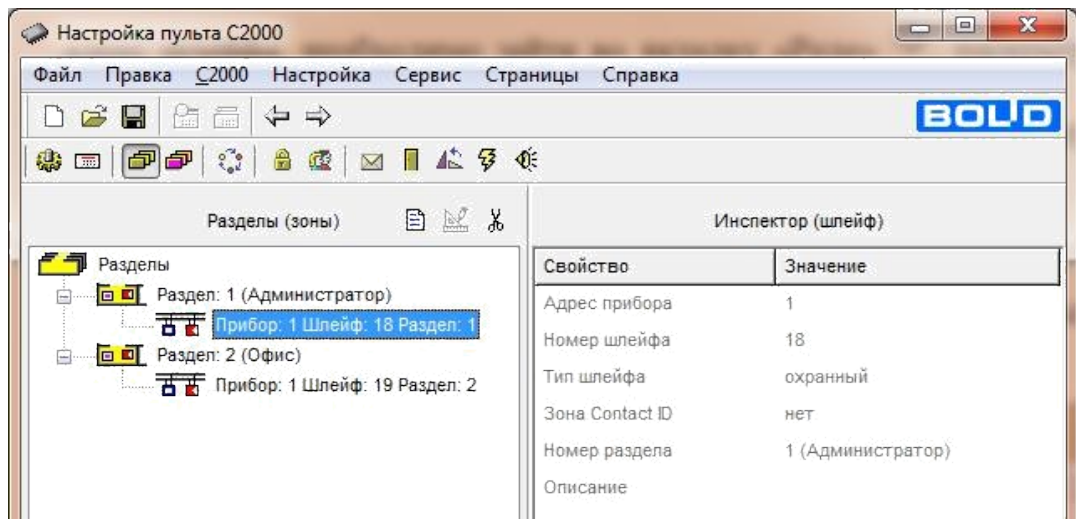
Охранный (С2000-ИК, С2000-СТИК, С2000-ПИК, С2000-СМК, С2000-АР8);


Тревожный (С2000-КТ).

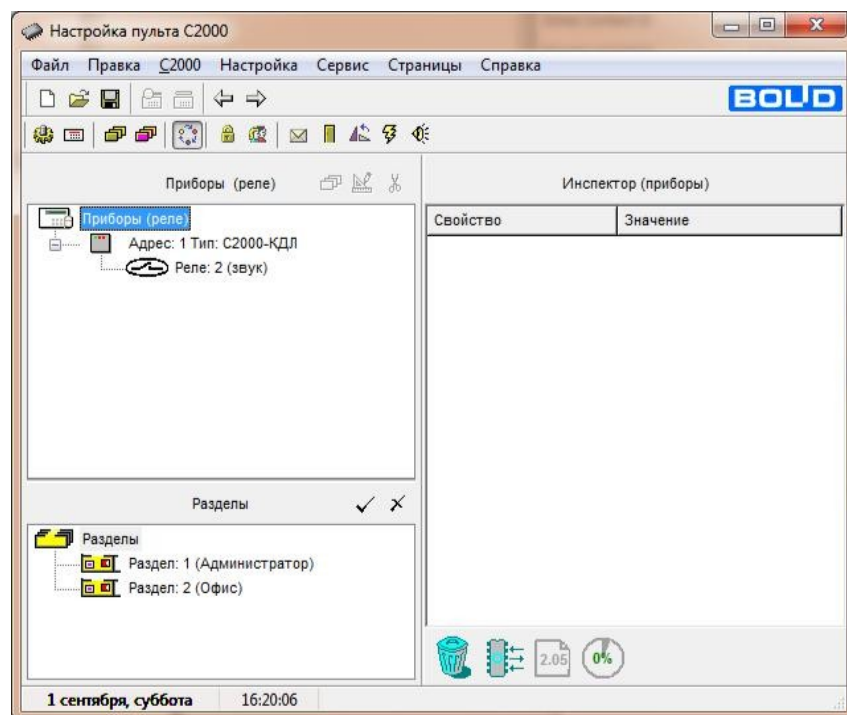



Для того что расписать тактику работы адресного релейного блока С2000-СП2 превращаем 2 адрес шлейфа (согласно исходным данным адресов пожарных извещателей интегрированной системы «Орион» используемые на стенде) прибора С2000-КДЛ в реле при помощи кнопки . Если случайно был превращен в реле не тот адрес шлейфа, необходимо зайти во вкладку «Реле» , раскрыть список С2000-КДЛ выделить необходимое реле и при помощи кнопки  превратить реле обратно в шлейф. Вернуться обратно во вкладку «Разделы».

В созданные разделы в (п. 5) перетаскивание добавляем измененные адреса шлейфов (п.6). Каждый адрес шлейфов перетаскиваем в свой раздел.

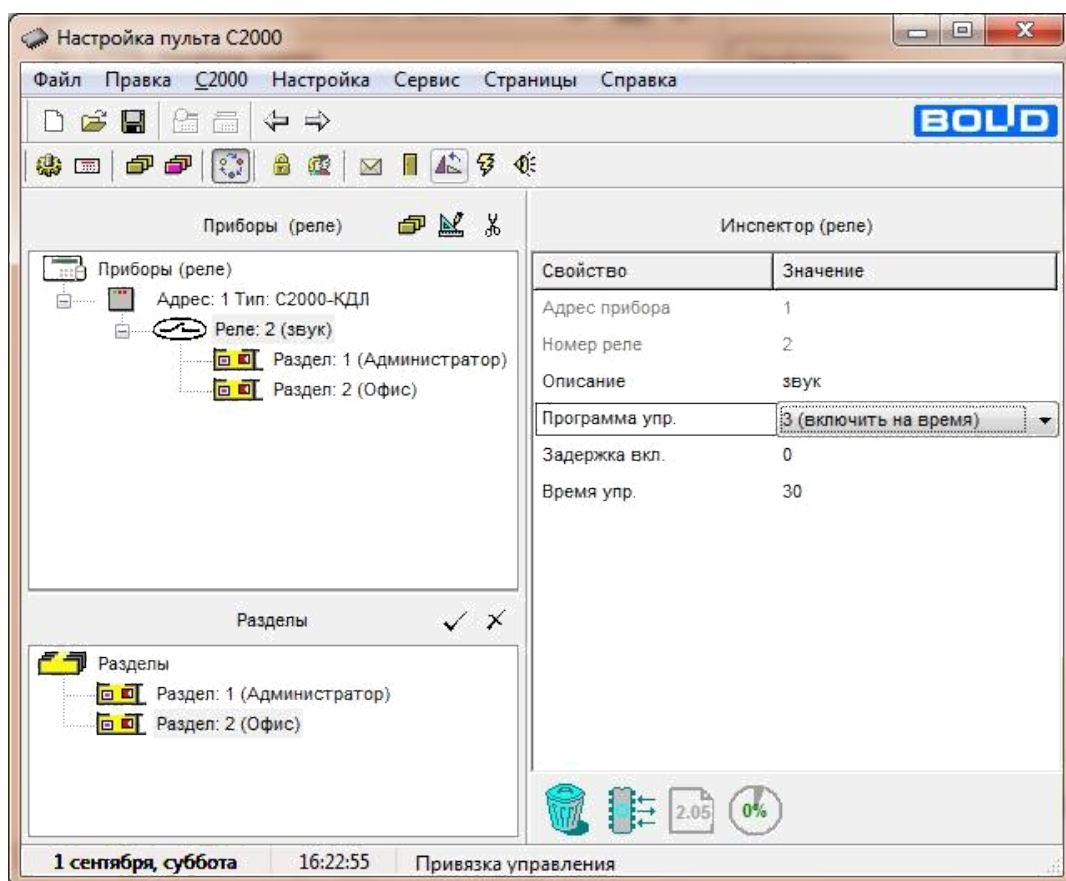


Во вкладке «Реле» раскрываем список реле прибора C2000-КДЛ и изменяем название реле  при помощи кнопки :  
Реле:2 (Звук).



Задаем тактику работы реле при помощи кнопки  в «Инспекторе реле» задаем программу управления для реле2 – «включить на время», задержку управления и время управления.

Добавляем в реле2 перетаскиванием созданные ранее разделы.



Сохранить конфигурацию в формате txt.

Открыть вкладку «С2000» и выбрать «Записать Конфигурацию».

### **Оформление отчета:**

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

### **Отчет должен содержать:**

1. Название, цели и задачи лабораторной работы;
2. Скриншоты о проделанной работе;
3. Заключение и выводы.

### **Контрольные вопросы:**

1. Дайте определение охранной сигнализации?

2. Дайте определение пульта централизованного наблюдения?
3. Какие приборы используются для построения неадресной охранной сигнализации в ИСО «Орион»?
4. Из каких основных устройств строится адресно-аналоговая охранная сигнализация?

## **Лабораторная работа №2**

**Тема: Изучение системы Орион Про на базе оборудования «Болид».**

**Настройка уровней доступа для охранной системы при помощи программы «Pprog».**

**Цель работы:** научиться настраивать уровни доступа интегрированной системы «Орион» для системы охранной сигнализации.

### **Краткая теория.**

**Права доступа** — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (информации, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации.

Уровни доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам (например, пользователям системы) над объектами данных. Для этого требуется некая система для предоставления субъектам различных прав доступа к объектам. Это система разграничения доступа субъектов к объектам, которая рассматривается в качестве главного средства защиты от несанкционированного доступа к информации.

Существует три модели управления доступом:

1. дискреционная;
2. мандатная;
3. ролевая.

## **Дискреционное управление доступом**

Данная модель характеризуется разграничением доступа между поименованными субъектами и объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Для каждой пары (субъект-объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту). Возможны, по меньшей мере, два подхода к построению дискреционного управления доступом:

- каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту;
- система имеет одного выделенного субъекта – суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем (UNIX или Windows семейства NT).

Дискреционное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений согласно требованиям к системе защиты информации.

## **Мандатное управление доступом**

Для реализации этого принципа каждому субъекту и объекту должны сопоставляться классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток



субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа:

- субъект может читать объект, только если иерархическая классификация субъекта не меньше, чем иерархическая классификация объекта, и неиерархические категории субъекта включают в себя все иерархические категории объекта;
- субъект осуществляет запись в объект, только если классификационный уровень субъекта не больше, чем классификационный уровень объекта, и все иерархические категории субъекта включаются в неиерархические категории объекта.

Реализация мандатных правил разграничения доступа должна предусматривать возможности сопровождения изменения классификационных уровней субъектов и объектов специально выделенными субъектами. Должен быть реализован диспетчер доступа, то есть средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном его разрешении и дискреционными, и мандатными правилами разграничения доступа. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

### **Ролевое разграничение**

Основной идеей управления доступом на основе ролей является идея о связывании разрешений доступа с ролями, назначаемым каждому пользователю. Эта идея возникла одновременно с появлением многопользовательских систем. Однако до недавнего времени исследователи мало обращали внимание на этот принцип.

Ролевое разграничение доступа представляет собой развитие политики дискреционного разграничения доступа, при этом права доступа субъектов системы на объекты группируются с учетом их специфики их применения, образуя роли.

Такое разграничение доступа является составляющей многих современных компьютерных систем. Как правило, данный подход применяется в системах защиты СУБД, а отдельные элементы реализуются в сетевых операционных системах.

Задание ролей позволяет определить более четкие и понятные для пользователей компьютерной системы правила разграничения доступа. При этом такой подход часто используется в системах, для пользователей которых четко определен круг их должностных полномочий и обязанностей.

Роль является совокупностью прав доступа на объекты компьютерной системы, однако ролевое разграничение отнюдь не является частным случаем дискреционного разграничения, так как ее правила определяют порядок предоставления прав доступа субъектам компьютерной системы в зависимости от сессии его работы и от имеющихся (или отсутствующих) у него ролей в каждый момент времени, что является характерным для систем мандатного разграничения доступа. С другой стороны, правила ролевого разграничения доступа являются более гибкими, чем при мандатном подходе к разграничению.

Если подвести итог, то у каждой из перечисленных нами систем есть свои преимущества, однако ключевым является то, что ни одна из описанных моделей не стоит на месте, а динамично развивается. Приверженцы есть у каждой из них, однако, объективно посмотрев на вещи, трудно отдать предпочтение какой-то одной системе. Они просто разные и служат для разных целей.

Механизм контроля доступа пользователей в системе «Орион» базируется на создании уровней доступа, каждый из которых включает в себя

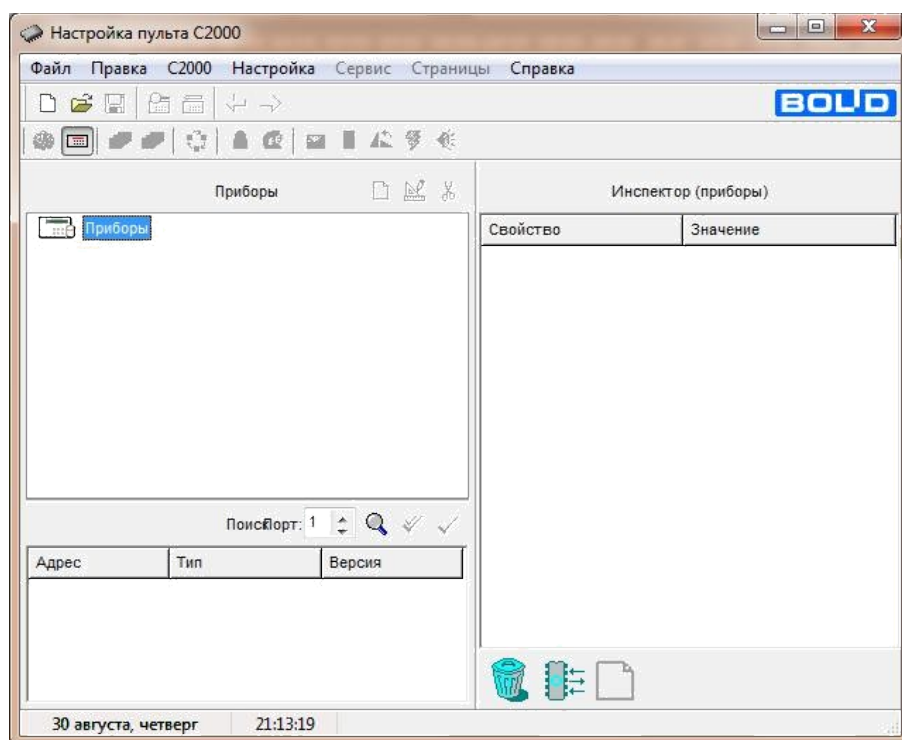
ряд разделов системы, которыми будет управлять какой-либо пользователь (несколько пользователей), а также права на конкретные разрешенные действия по управлению каждым из перечисленных разделов. Затем номера уровней доступа связываются с паролями (ключами) конкретных пользователей, которым пульт будет предоставлять доступ к указанным при описании уровня доступа разделам по соответствующим правилам.

Работа с уровнями доступа (создание/редактирование/удаление) и привязка к ним правил управления определенными разделами системы «Орион» производится на странице «Уровни доступа» программы Pprog, а добавление зарегистрированных пользователей и выбор для них уровня доступа – на странице «Пароли».

**Задание к работе:**

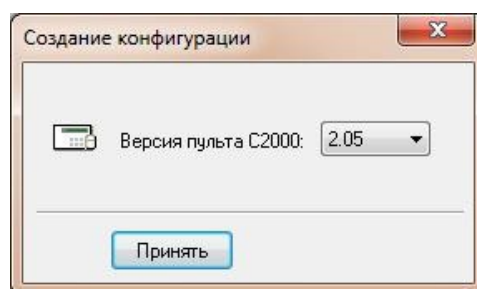
1. Добавить пульт контроля и управления;
2. Добавить прибор приемно-контрольные охранно-пожарный;
3. Создать разделы для системы пожарной и охранной сигнализации;
4. Добавить три уровня доступа;
5. Настроить уровни доступа для охранно-пожарных разделов;

**Порядок выполнения работы:**




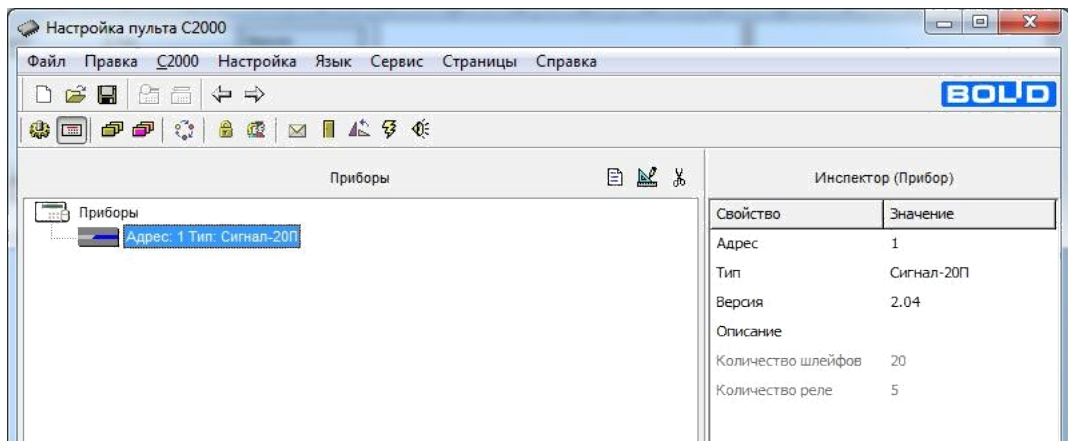
1. Запустить программу «Prrog.exe»




2. Создать новую конфигурацию при помощи кнопки 

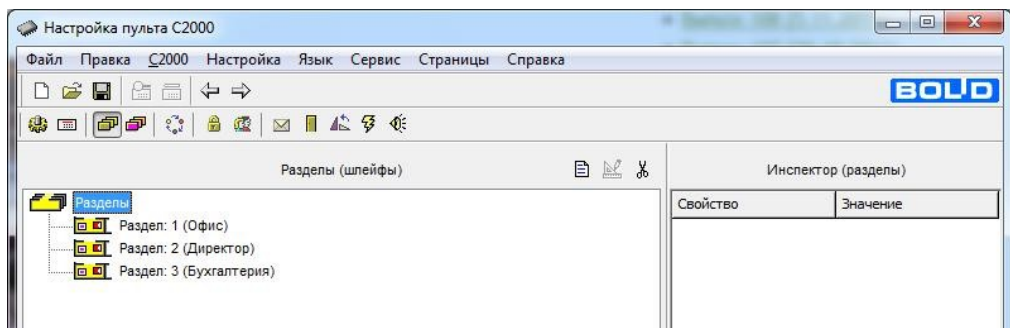


3. Добавить один новый прибор при помощи  кнопки

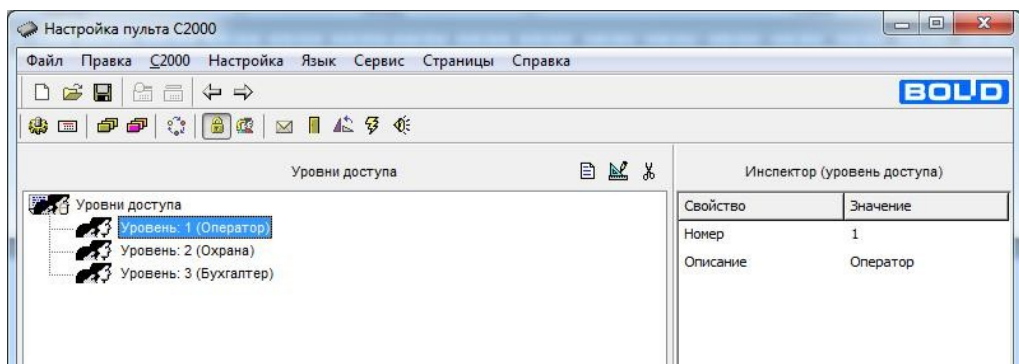
4. При помощи кнопки «Править прибор»  в инспекторе приборов изменить свойства и значения прибора. Для первого выбираем тип прибора Сигнал-20П.



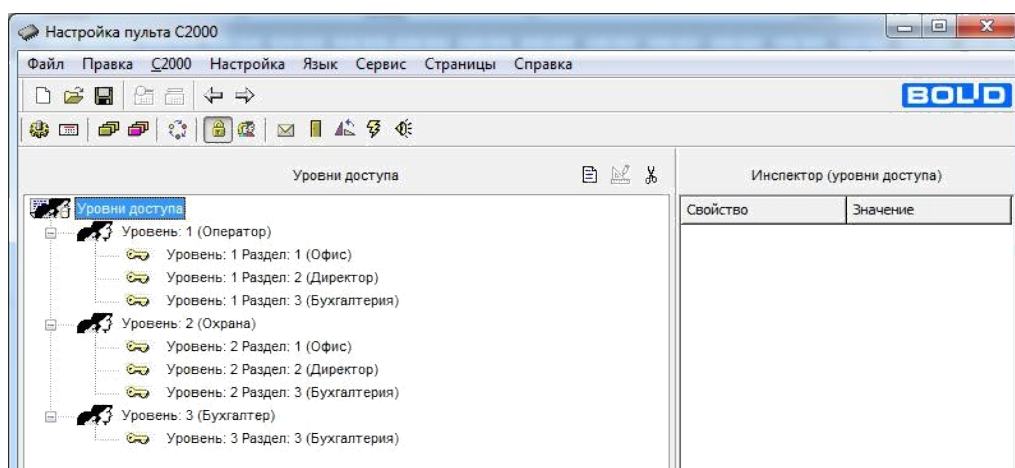
5. Во вкладке «Разделы» в зоне «Разделы»  добавить несколько разделов при помощи кнопки  и дать им название при помощи кнопки  создать три раздела (офис, директор и бухгалтер)



6. Во вкладке «уровни доступа» добавляем три уровня (оператор, охрана и бухгалтер)

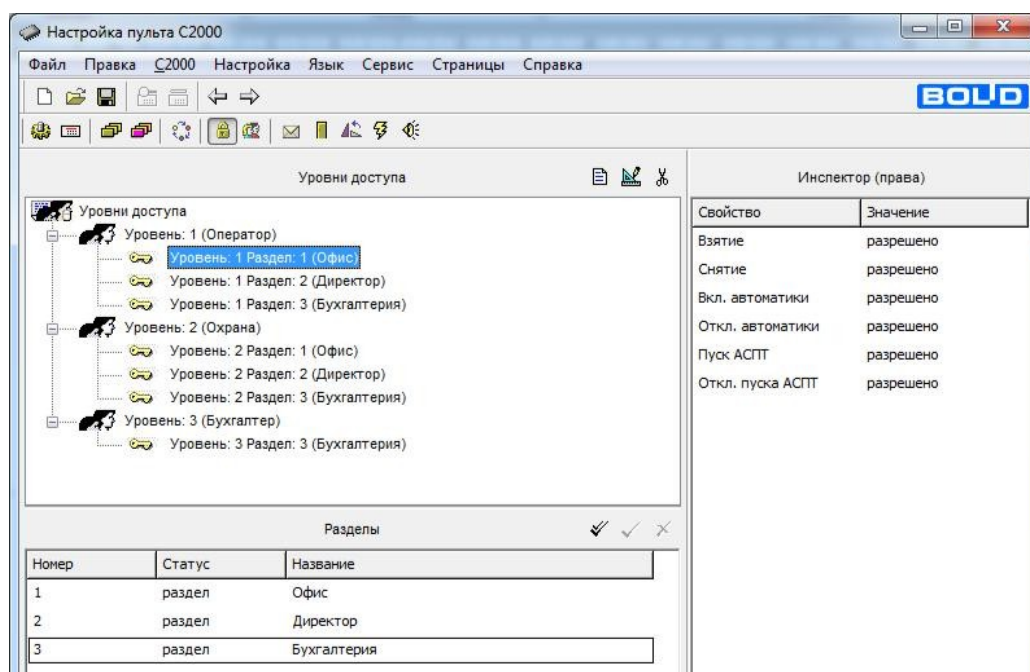


7. Далее добавляем все разделы (перетаскиванием) в уровень оператор и охрана, а в уровень бухгалтер добавляем только раздел бухгалтер.



## 8. Настраиваем права доступа:

1. Уровень оператор – разрешаем все;
2. Уровень охрана – разрешаем только «Взятие» и «Снятие»;
3. Уровень бухгалтер – разрешаем только «Взятие» и «Снятие»;



## Оформление отчета:

Отчет по практическому занятию оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

## Отчет должен содержать:

1. Название, цели и задачи практического занятия;

2. Скриншоты о проделанной работе;
3. Заключение и выводы.

**Контрольные вопросы:**

1. Дайте определение права доступа?
2. Рольное разграничение доступа?
3. Мандатное разграничение доступа?
4. Дискреционное разграничение доступа?

### **Лабораторная работа №3**

**Тема: Изучение системы Орион Про на базе оборудования «Болид». Настройка паролей для охранной системы при помощи программы «Pprog».**

**Цель работы:** научиться настраивать пароли интегрированной системы «Орион» для системы охранно-пожарной сигнализации.

#### **Краткая теория.**

В программе Pprog есть функциональная возможность по работе с паролями (ключами) пользователей, предоставляющая доступ к системным операциям – конфигурирования, взятию/снятию системы или ее отдельных частей на охрану и др. Для работы с паролями (ключами) предназначена страница «Пароли» программы Pprog.

Пульт поддерживает два способа аутентификации пользователей при работе с системой:

🌐С помощью заданных PIN кодов (цифровых паролей), вводимых с клавиатуры пульт, клавиатур «С2000-К» или «С2000-КС»;

🌐Посредством предъявления зарегистрированных устройств Touch Memoгу или Proximity-карт на считывателях приборов «С2000-4», «С2000-2» и других.

Всего в системе, работающей под управлением пульта, можно задать/зарегистрировать до 2047 паролей (ключей) пользователей.

Пароль с номером 1 зарезервирован в конфигурации пульта и представляет собой пароль установщика (Главный пароль). Этот пароль используется только для программирования пульта и приборов системы. Только владелец пароля установщика может настраивать адреса приборов и адресных расширителей, задавать, менять и удалять пароли пользователей, менять код своего пароля, задавать и менять конфигурацию пульта с помощью программы Pprog. Заводское значение пароля 123456 рекомендуется переопределить перед началом эксплуатации на новое значение (от 1 до 8 цифр).

В конфигурации пульта, имеется также предустановленный пароль пользователя с номером 2 и значением (кодом) 1234, для которого по умолчанию задан уровень доступа 255, дающий право на взятие/снятие шлейфов сигнализации приборов системы и некоторые операции с пультом. Параметры пароля №2 можно переопределить.

Для остальных паролей пользователей их права задаются через описание связанных с ними уровней доступа, каждый из которых представляет собой правила доступа к определенным элементам системы. Три уровня доступа (253, 254 и 255), описывающие управление приборами системы, зарезервированы и не могут быть переопределены. Остальные уровни с 1 по 252 могут быть запрограммированы и не могут быть переопределены. Остальные уровни с 1 по 252 могут быть запрограммированы в системе для управления ее разделами.

Окно «Пароли», включающее список паролей и ключей пользователей, зарегистрированных в конфигурации пульта. Справа от заголовка окна находятся его инструменты:

- Добавить пароль
- Редактировать пароль
- Удалить пароль
- Выбрать/Обратить выбранное
- Считать ключ



- Загрузить коды и имена ключей из файла

На странице «Пароли» можно:

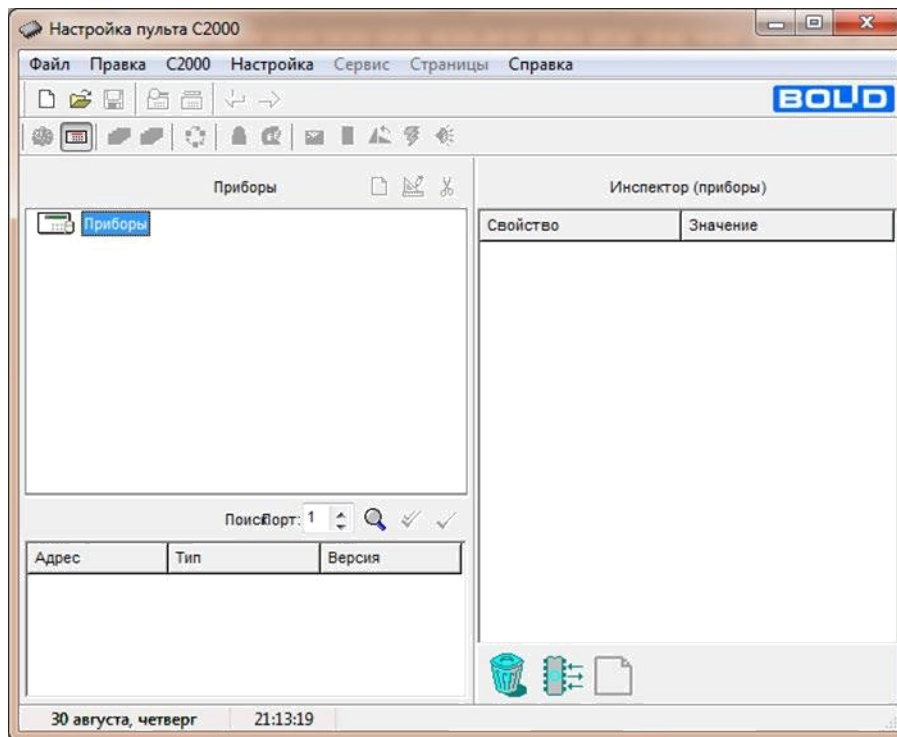
- Посмотреть список заданных в конфигурации пульта паролей (ключей) пользователей и их параметры;
- Изменить код Главного Пароля или переопределить пользовательский пароль 2;
- Создать/зарегистрировать пароль или ключ пользователя;
- Отредактировать параметры выбранного пароля или ключа;
- Удалить пароль/ряд паролей из конфигурации пульта;
- Считать электронную таблетку/ карту;
- Загрузить коды электронных ключей из файла с расширением .ki.


#### **Задание к работе:**

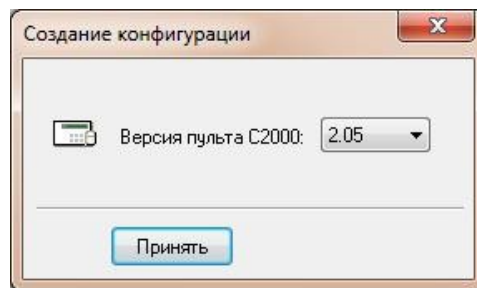
1. Добавить новый пульт контроля и управления;
2. Добавить прибор приемно-контрольные охранно-пожарный «Сигнал-20П»;
3. Создать разделы для системы пожарной и охранной сигнализации;
4. Занести два новых пароля в конфигурацию пульта;
5. Задать новым паролям стандартные уровни доступа;
6. Создать два новых уровня доступа.

#### **Порядок выполнения работы:**


1. Запустить программу «Pprog.exe»

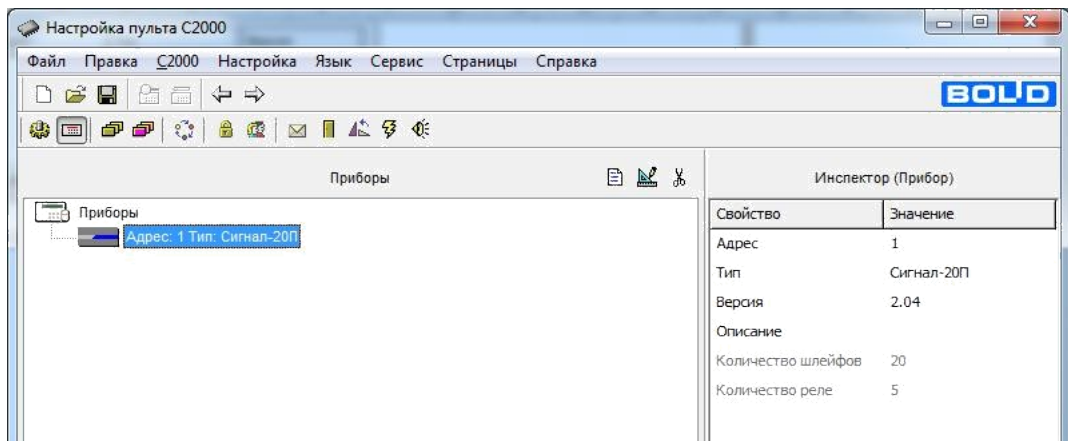





2. Создать новую конфигурацию при помощи кнопки 

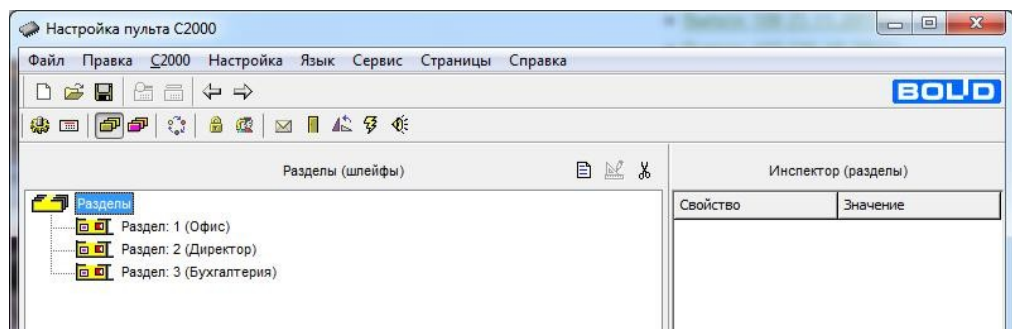


3. Добавить новый прибор при помощи кнопки 

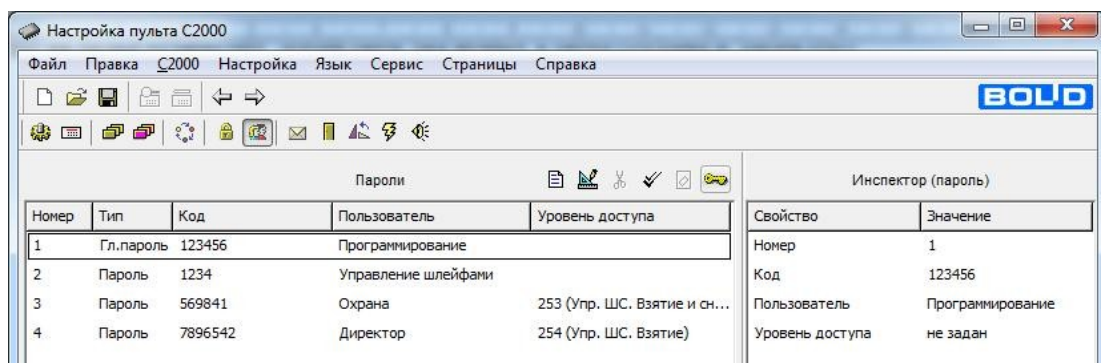
4. При помощи кнопки «Править прибор»  в инспекторе приборов изменить свойства и значения прибора. Выбираем тип прибора Сигнал-20П.



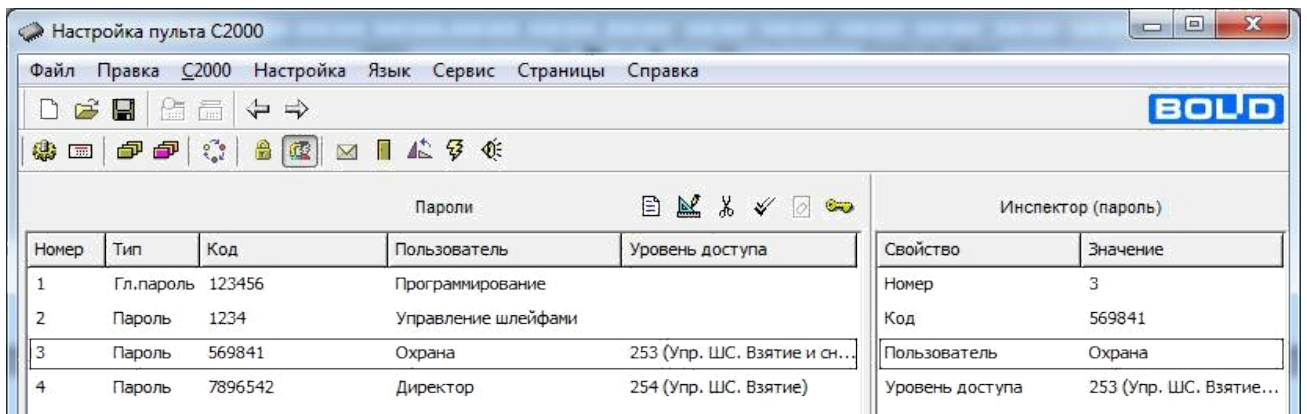
5. Во вкладке «Разделы» в зоне «Разделы»  добавить несколько разделов при помощи кнопки  и дать им название при помощи кнопки , создать три раздела (офис, директор и бухгалтер)



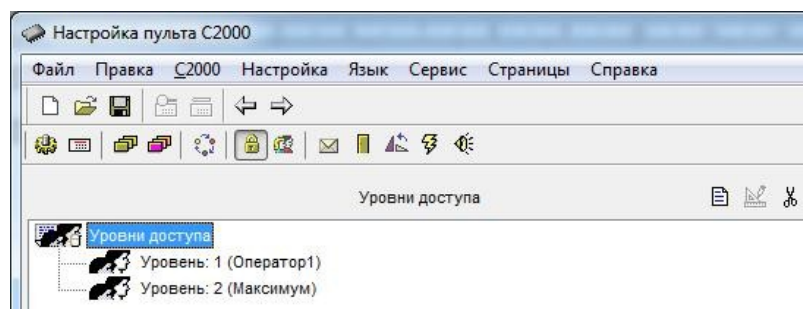
6. Во вкладке «Пароли» добавляем два новых ключа (охрана и директор)



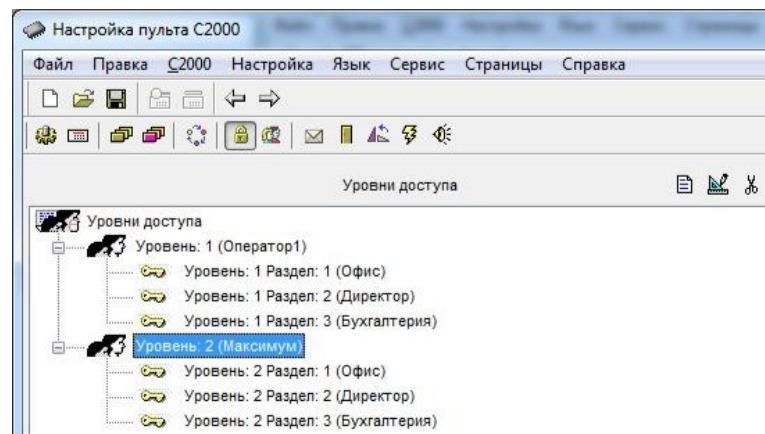
7. Пользователю «охрана» задаем код и уровень доступа 253 (взятие и снятие)
8. Пользователю «директор» задаем код и уровень доступа 254(взятие)



9. Во вкладке «уровни доступа» добавляем два уровня (максимум, оператор1)



10. Далее добавляем все разделы (перетаскиванием) в уровень максимум и оператор1.

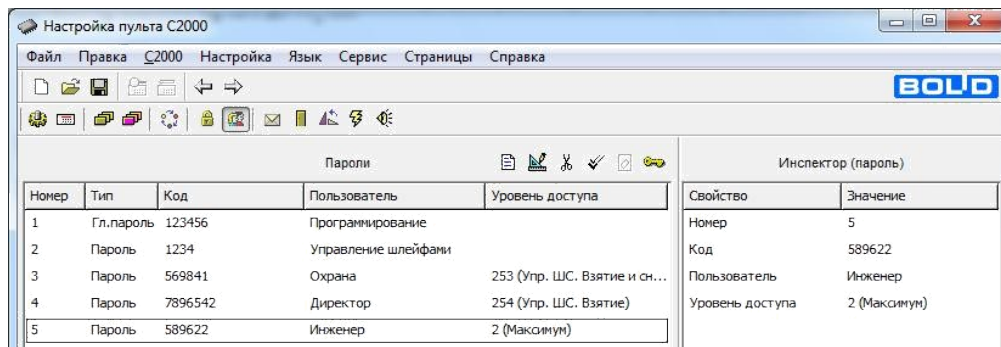


11. Настраиваем права доступа:

- Уровень максимум – разрешаем все;
- Уровень Оператор1 – разрешаем только «Взятие», «Снятие» и «Вкл. автоматику».

12. Во вкладке «Пароли» добавляем новый ключ (Инженер)

13. Пользователю «Инженер» задаем код и уровень доступа «Максимум»



### Оформление отчета:

Отчет по работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

### Отчет должен содержать:

1. Название, цели и задачи работы;
2. Скриншоты о проделанной работе;
3. Заключение и выводы.

### Контрольные вопросы:

1. Какие два способа аутентификации пользователей поддерживает пульт?
2. Сколько можно зарегистрировать паролей в системе?
3. Три стандартных уровня доступа в системе?
4. Сколько можно задать уровней доступа?

## Лабораторная работа №4

**Тема: Конфигурирование системы контроля и управления доступом на базе контроллера доступа «С2000-2».**

**Цель работы:** изучение технологии конфигурирования приборов для построения системы контроля и управления доступом.

## Теория

Система контроля и управления доступом (СКУД) — это совокупность программных и технических средств, а также организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением охраняемого объекта.

Современные системы контроля доступа призваны решать три основные задачи:

- **Организация контроля перемещения персонала.** Правильная организация труда. Каждому пользователю достаточно выдать один ключ («Touch Memory» или карту «Proximity») для его идентификации системой охраны объекта. Исключение возможности праздно шатания сотрудников.
- **Организация учета.** Создание системы учета рабочего времени (на основе анализа времени прихода/ухода сотрудника с территории предприятия или рабочего места). Контроль места нахождения сотрудника на объекте с точностью до зоны доступа.
- **Организация охраны предприятия.** Интеграция СКД с системой охранно-пожарной сигнализации для комплексного решения задач безопасности. Обеспечение реакции охранной составляющей системы на попытки несанкционированного доступа, взлома дверей и т.д. Возможность автоматической постановки/снятия с охраны помещений по факту прохода в зону доступа сотрудника. Предоставление свободного доступа в случае возникновения пожара.

### Термины и определения

- **Контроллер доступа** – это устройство, предназначенное для управления доступом через контролируемые точки доступа путём анализа считанных с помощью считывателей идентификаторов пользователей (проверки прав). Контроллеры доступа могут сами принимать решения предоставлять или не предоставлять доступ в случае, если идентификаторы пользователей хранятся в памяти контроллера (в таком случае говорят, что используется локальный доступ). Также идентификаторы пользователей могут быть записаны только в сетевом контроллере (в базе данных программного обеспечения). В этом случае контроллер доступа выполняет функции ретранслятора – отправляет код

сетевому контроллеру и получает от него решение о предоставлении или не предоставлении доступа (в таком случае говорят о централизованном доступе). Контроллеры доступа управляют преграждающими устройствами с помощью контактов реле;

- **Идентификаторы** – уникальные признаки пользователей СКУД. Идентификатором может быть электронный ключ Touch Memory, бесконтактная Proxu-карта, радио-брелок, PIN-код, биометрические данные (отпечаток пальца, ладони, рисунок радужной оболочки или сетчатки глаза, геометрические характеристики лица и т.п.). В СКУД каждому идентификатору присваиваются определённые полномочия, в соответствие с которыми контроллерами доступа разрешается или запрещается проход;
- **Считыватели** – устройства, предназначенные для считывания кода идентификатора пользователя и передачи его контроллеру доступа;
- **Точка доступа** – логический объект СКУД, фактически представляет собой физическую преграду, оборудованную контроллером доступа и считывателем. Точкой доступа может являться дверь, калитка, турникет, шлагбаум, шлюз, и т.п. Точки доступа, могут работать в двух режимах: с контролем и без контроля направления прохода. Точки доступа с контролем направления прохода могут быть как двунаправленными (оборудованными двумя считывателями), так и однонаправленными (с одним считывателем, без возможности прохода в обратном направлении). Выход через точки доступа без контроля направления прохода чаще всего осуществляется по кнопке.
- **Зона доступа** – логический объект СКУД. Зоны доступа – это участки, на которые разбита территория охраняемого предприятия. На границах зон доступа всегда располагаются точки доступа с направлением прохода. Зоны доступа настраиваются для точек доступа в случае, если в системе используются такие функции, как расчёт рабочего времени и запрет повторного прохода (правило antipassback);
- **Уровень доступа** – индивидуальные права доступа, которые определяют правила прохода через точки и присутствия в зонах доступа, назначенные идентификатору пользователя. На основе этих прав контроллеры доступа (или сетевые контроллеры) принимают решение о предоставлении или не предоставлении доступа;

- **Окна времени** – совокупность временных интервалов, в течение которых разрешён проход. Временные интервалы могут устанавливаться для каждой точки или зоны доступа индивидуально;

#### **Типовые режимы работы СКУД:**

- Стандартный режим прохода.
- Запрет повторного прохода (правило antipassback).
- Доступ по правилу двух (или более) лиц.
- Доступ с подтверждением.
- Двойная идентификация.
- Закрытый режим доступа.
- Открытый режим доступа.

Контроллер имеет возможность работать в нескольких режимах: «две двери на вход», «одна дверь на вход/выход», «турникет», «шлагбаум», «шлюз».

**Одна дверь на вход/выход.** Данный режим предназначен для управления доступом через одну дверь, у которой имеется только одно запорное устройство, и которая контролируется одним датчиком прохода (рисунок 1). Предоставление доступа в обоих направлениях требует предъявления идентификаторов пользователей. Для предоставления доступа также могут использоваться кнопки выхода (например, для открывания двери с поста охраны).



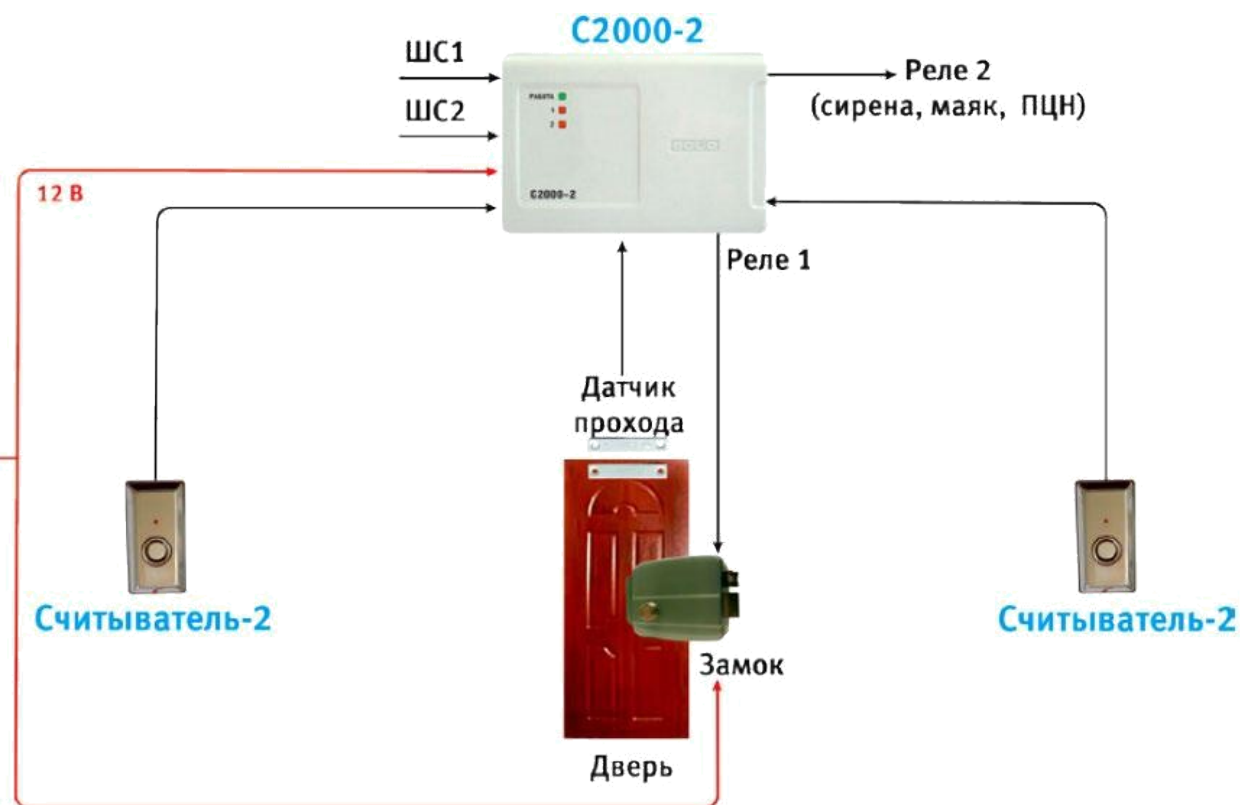


Рисунок 1 – Схема режима Одна дверь на вход/выход

Контроллер доступа "С2000-2" (в дальнейшем – контроллер) предназначен для управления доступом (рисунок 2).



Рисунок 2 – Внешний вид контроллера доступа "С2000-2"

Контроль доступа осуществляется путем считывания кодов предъявляемых идентификаторов (карт Proximity, ключей Touch Memoгу и PIN-кодов), проверки прав доступа и замыкания (размыкания) контактов реле, управляющих запорными устройствами (электромеханическими и электромагнитными замками и защелками, турникетом, шлагбаумом). В

нашем случае используются Считыватель "Считыватель-2" и электронный ключом-идентификатор типа Dallas DS1990A (рисунок 3).



Рис. 3 - Touch Memory Считыватель "Считыватель-2" с электронным ключом-идентификатором типа Dallas DS1990A



Рис - Проху-Н1000 считыватель проксимити карты, выходной код – Touch Memory, накладной

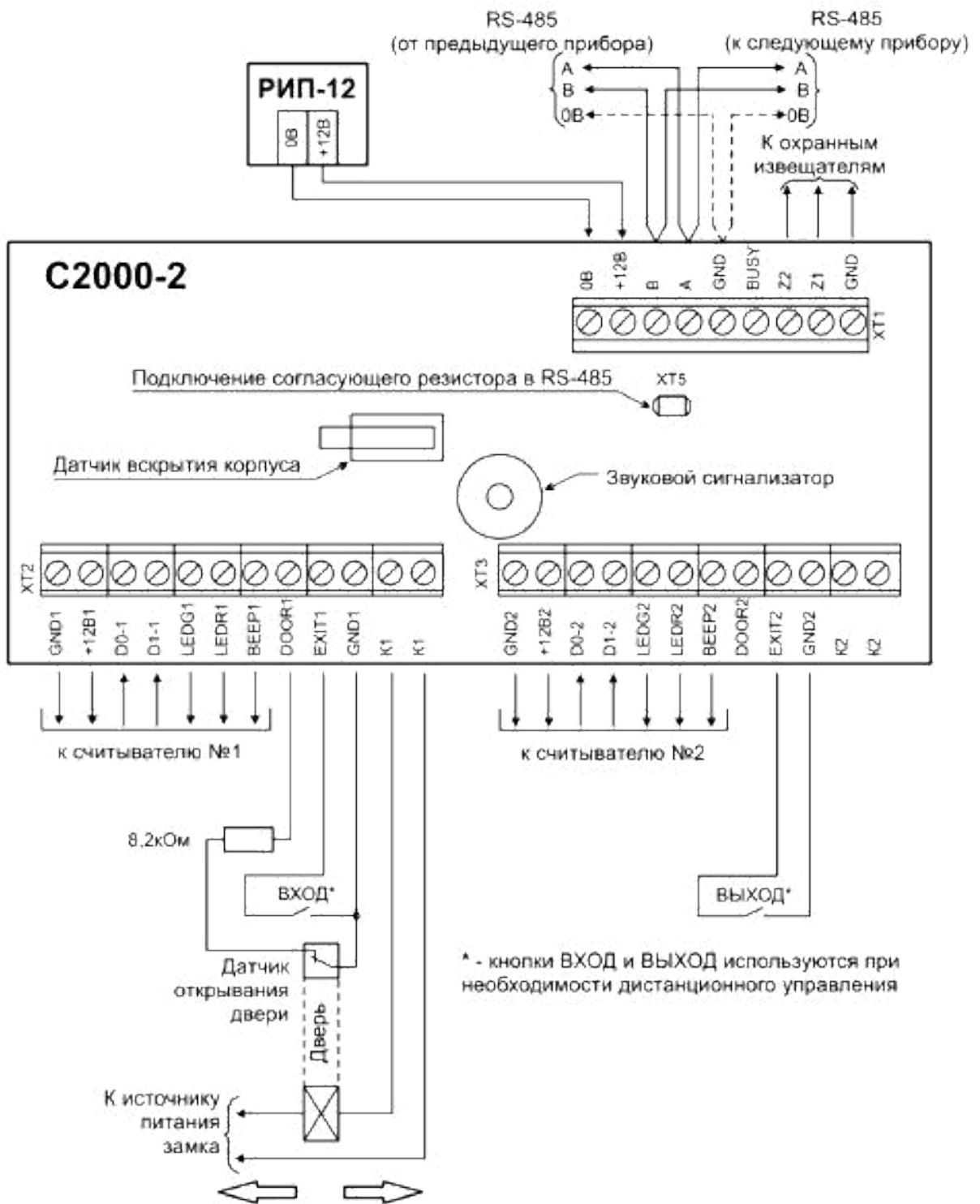
Свое название Touch Memory (тач мемори или точ мемори) ключи получили в 1991 году от полного названия Dallas Touch Memory, где:

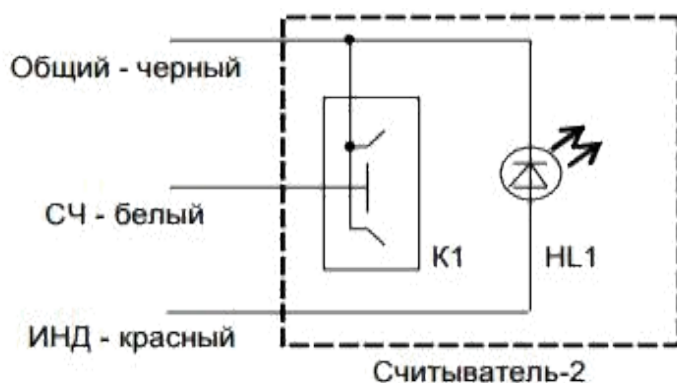
- Dallas – компания производитель (Dallas Semiconductor);
- Touch – метод считывания (касанием считывателя Touch Memory);

- Memory – встроенная память (справедливо для электронных ключей с памятью, например - DS1991, DS1992, DS1993, DS1994, DS1995, DS1996).

Каждый ключ DS-1990 touch memory имеет индивидуальный код, который присваивается еще на заводе-изготовителе. Ключ считывается через контактор и со считывателя на контроллер передается сигнал. Контроллер индексирует свою память и в случае наличия в его памяти именно этого ключа, дает команду на открытие замка.

Локальный контроль доступа – предоставление либо запрет доступа по идентификатору (ключу), занесенному в базу данных контроллера, в зависимости от прав доступа данного ключа, текущего режима доступа и наличия нарушений режима доступа у предъявленного ключа. На рисунке 4 показана схема подключения контроллера "С2000-2" в режиме "Одна дверь на вход/выход".





HL1 – индикатор единичный Kingbright L-934ID

K1 – контактное устройство "Touch Memory"

Рисунок 5 - Схема подключения считывателей с интерфейсом Touch Memory.

Контроллер С2000-2 может работать в автономном режиме. Однако для задания параметров работы необходим Пульт контроля и управления охранно-пожарный (ПУ) С2000 (или С2000М). ПУ С2000М (рисунок 6) предназначен для работы в составе адресной системы охранной сигнализации и объединения различных приборов интегрированной системы охраны (ИСО) Орион. Так же ПУ используется для постановки на охрану, снятия с охраны и отображения происходящих в системе событий.



Рисунок 6 - Внешний вид пульта контроля и управления охранно-пожарного С2000М

Информационное взаимодействие между пультом "С2000М" и приборами ИСО "Орион" осуществляется по проводной линии связи RS-485.

Итак, для задания параметров работы всех приборов, которые требуется использовать в Системе Орион необходимо осуществить конфигурирование пульта С2000М с помощью персонального компьютера и программы "rprog.exe" версии от 2.00 и выше.

Далее потребуется программа rprog.exe, предназначенная для настройки конфигурационных параметров адресных приборов.

Для связи ПУ С2000 с ПК нам потребуется преобразователь интерфейсов С2000-USB (либо USB-RS 485) для преобразования сигналов интерфейса USB в сигналы двухпроводного магистрального интерфейса RS-485 (рис. 7).

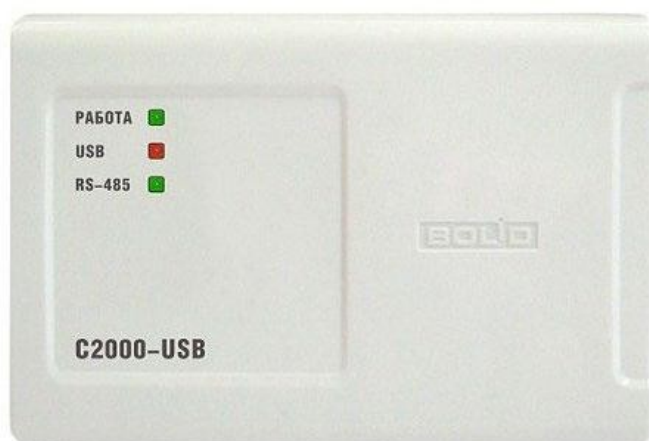


Рисунок 7 - Внешний вид преобразователя интерфейсов С2000-USB

Схема соединений интерфейса посредством С2000-USB показана на рисунке 8.

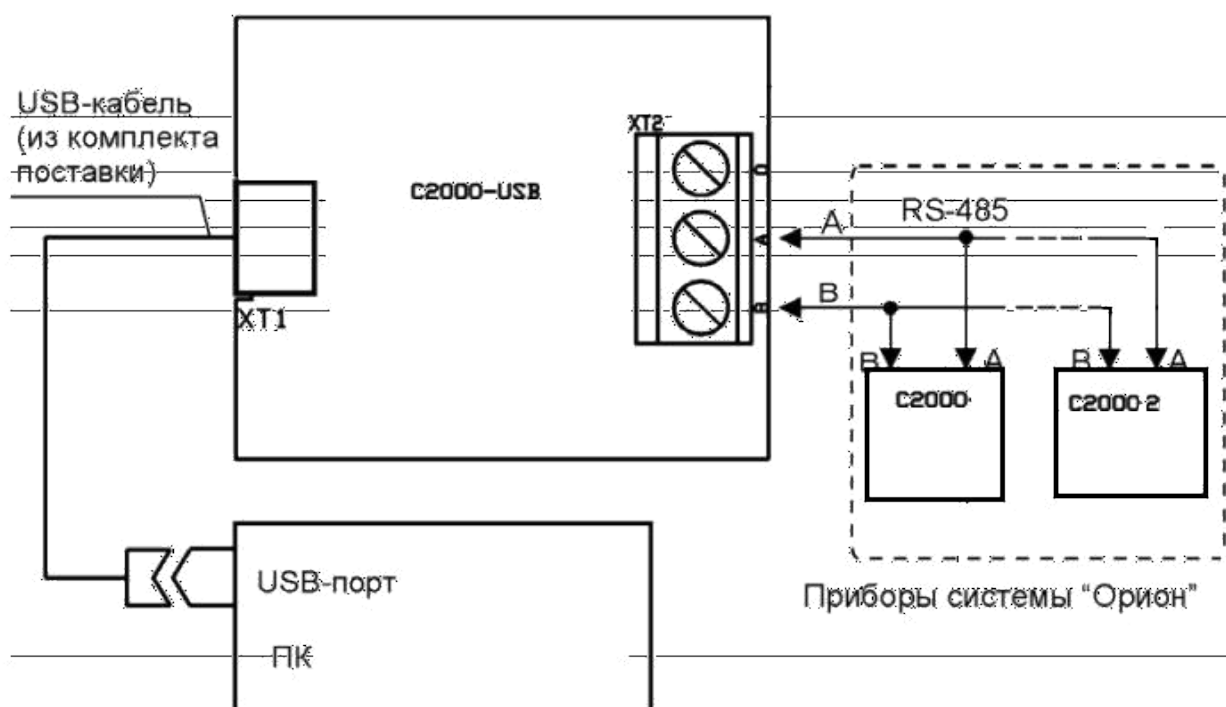



Рисунок 8 - Схема соединений интерфейса с ПК.

**Сценарии управления доступом** на вкладке **Входные зоны** помечаются в списке сценариев пиктограммой . Такие сценарии создаются для автоматического управления режимом доступа контроллеров «С2000-2». При этом считывателям, подключенным к указанным контроллерам, могут автоматически выдаваться команды на создание режима свободного прохода (двери/турникеты открыты и предъявление ключа не требуется) и восстановления режима управляемого прохода с проверкой ключей и блокировкой доступа неизвестным пользователям.

Типичный пример необходимости создания сценария управления доступом – управление доступом на путях эвакуации при пожаре, когда при наличии сигнала о пожаре в связанном разделе на все связанные со сценарием считыватели выдается команда «Открыть доступ», а при сбросе пожарной тревоги считыватели возвращаются в исходное состояние «Контролируемый доступ».

Чтобы создать сценарий управления доступом, следует:

*Задать исходное состояние для режима доступа считывателя и (опционально) текстовое описание для создаваемого сценария в окне «Инспектор» (см. Рисунок 49). Параметр «Исходное состояние» может принимать одно из двух значений: «Нет» или «Восстановить доступ»; оно означает состояние считывателей, в котором они будут находиться то время, когда ни одно из условий сценария не выполняется. Значение «Нет»*

означает, что никаких централизованных команд считывателю со стороны пульта не выдается.

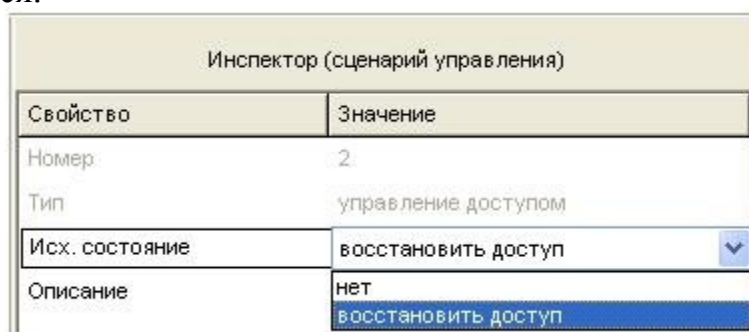


Рисунок 4.2

*Привязать создаваемый сценарий управления к считывателю/считывателям*, которым пульт будет синхронно выдавать управляющие команды в рамках создаваемого сценария. Для этого следует в окне сценариев управления отметить нужный сценарий управления, затем в нижнем окне выбрать нужный считыватель/считыватели и либо нажать кнопку в палитре инструментов окна привязки, либо выбрать нужное значение параметра «Сценарий» в окне «Инспектор» (см. Рисунок 50).

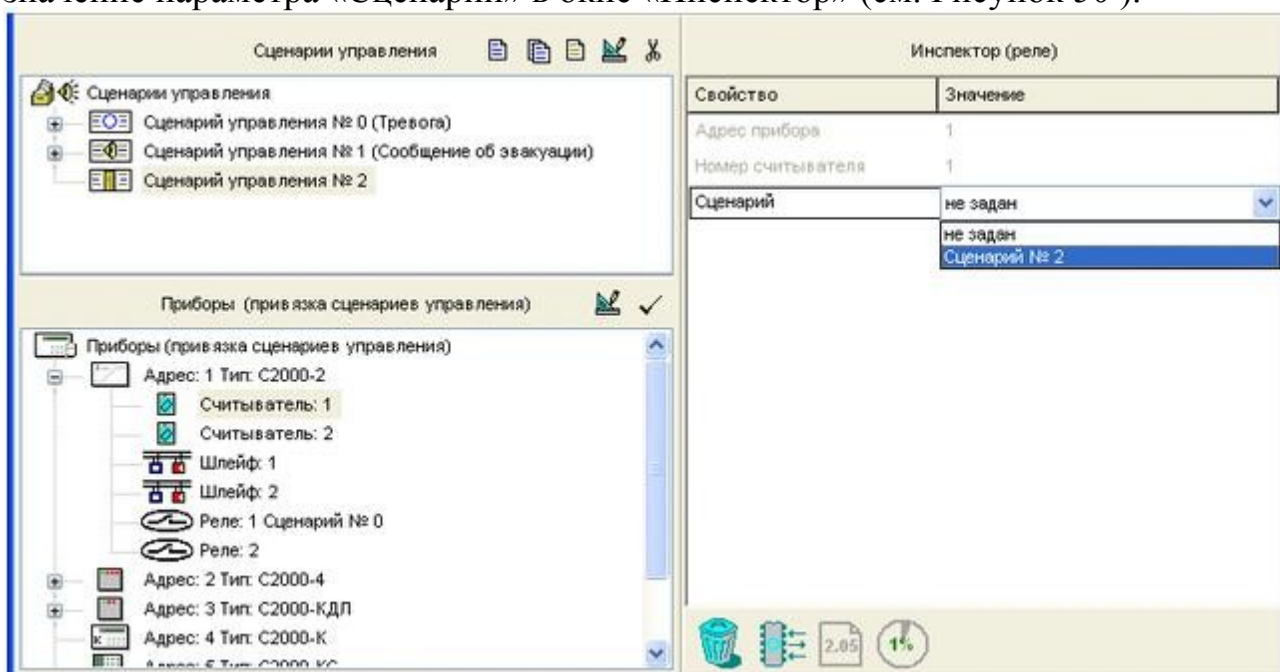


Рисунок 4.3

*Задать необходимые компоненты сценария управления связанными считывателями*

Чтобы задать каждый из компонентов сценария, воспользуйтесь кнопкой (третья кнопка из палитры инструментов окна сценариев), либо клавишей <Insert> или командой меню «Правка» → «Добавить» (при условии, что сценарий выбран и активен). При этом в окне сценариев для



создаваемого сценария появится новый компонент, окно «Приборы (привязка сценариев управления)» сменится на окно «Состояния и разделы для шага сценария», а окно «Инспектор» будет отображать параметры управления связанными считывателями (см. Рисунок 51).

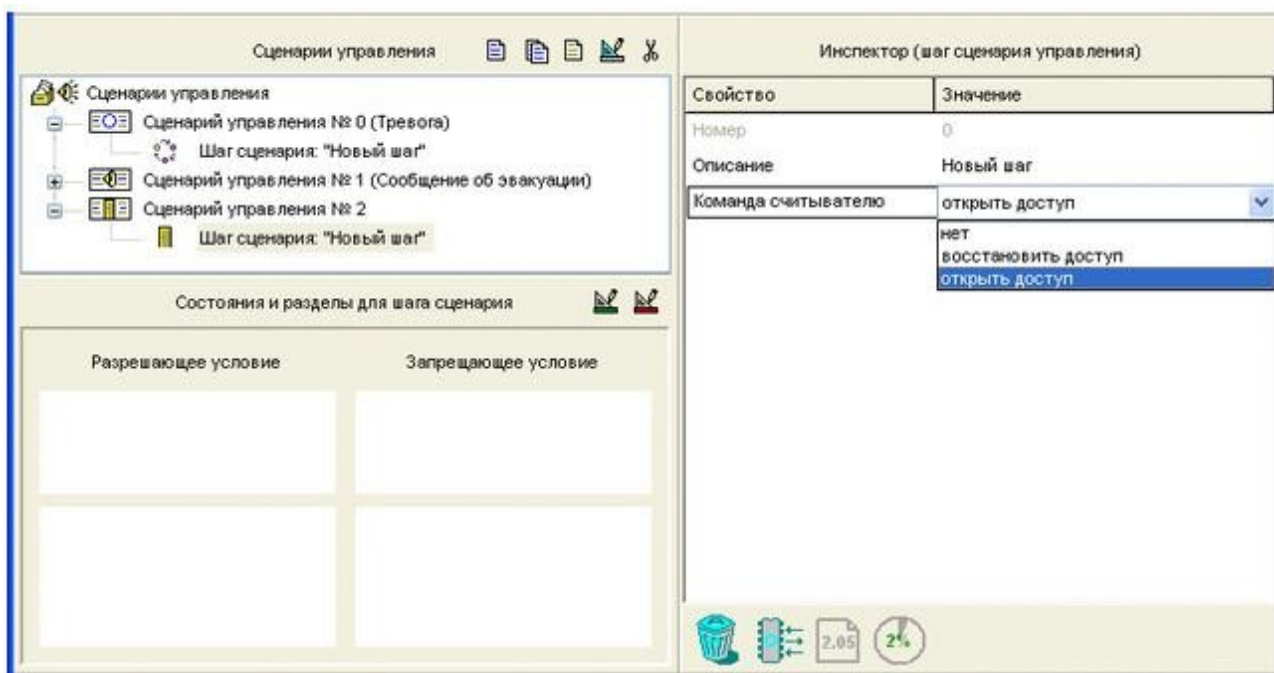


Рисунок 4.4

Задайте в окне «Инспектор» параметры управления для программируемого компонента сценария:

*Описание:* Задайте (опционально) текстовое описание для программируемого компонента сценария. По умолчанию каждому компоненту сценария присваивается имя «Новый шаг». Заданное имя не сохраняется в памяти в памяти пульта, но записывается в файл конфигурации.

*Команда считывателю:* Задайте команду, которую пульт будет отправлять связанным со сценарием считывателям при выполнении условия управления для описываемого компонента. По умолчанию для каждого компонента сценария задана команда «Открыть доступ», которую можно изменить на команду «Восстановить доступ» или значение «Нет».

*Далее следует задать условие управления* для описываемого компонента сценария, то есть то состояние системы, которое будет вызывать срабатывание данного компонента сценария.

После описания первого компонента можно описать следующий компонент данного сценария. Формально каждый из сценариев управления может содержать до 255 компонентов, но общее количество и сложность сценариев ограничиваются выделенной для этих целей памятью, доступный размер которой можно отслеживать по значению индикатора в



информационной строке. Если память заполнена, инструменты создания новых сценариев и новых шагов становятся недоступными.

### **Задание условий управления для компонентов сценариев.**

В данном разделе описывается задание условий управления для каждого из компонентов сценариев управления любого типа.

Условия управления, или, другими словами, состояние системы, которое должно вызвать выполнение одного из компонентов сценария управления, представляет собой совокупность двух частей: разрешающей и запрещающей. Каждая из частей условия включает определенные разделы системы и состояния, в которых эти разделы должны находиться.

Разрешающая часть условия считается выполненной, если хотя бы одна зона из разделов, включенных в эту часть, оказалась в заданном состоянии. Запрещающая часть условия описывает состояние системы, которое должно блокировать выполнение соответствующего компонента сценария, и может отсутствовать. Компонент сценария запускается на исполнение, если справедлива разрешающая часть условия и при этом не выполняется его запрещающая часть.

Обе части условия управления для определенного компонента сценария, как разрешающая, так и запрещающая, формируются одинаково, по нажатию кнопок  и  из палитры инструментов окна «Состояния и разделы для шага сценария». Для простоты приведем описание задания только разрешающей части условия. В верхней части окна редактирования условия (см. Рисунок 55) содержится список состояний, а в левой нижней части – список заданных в конфигурации пульта разделов.

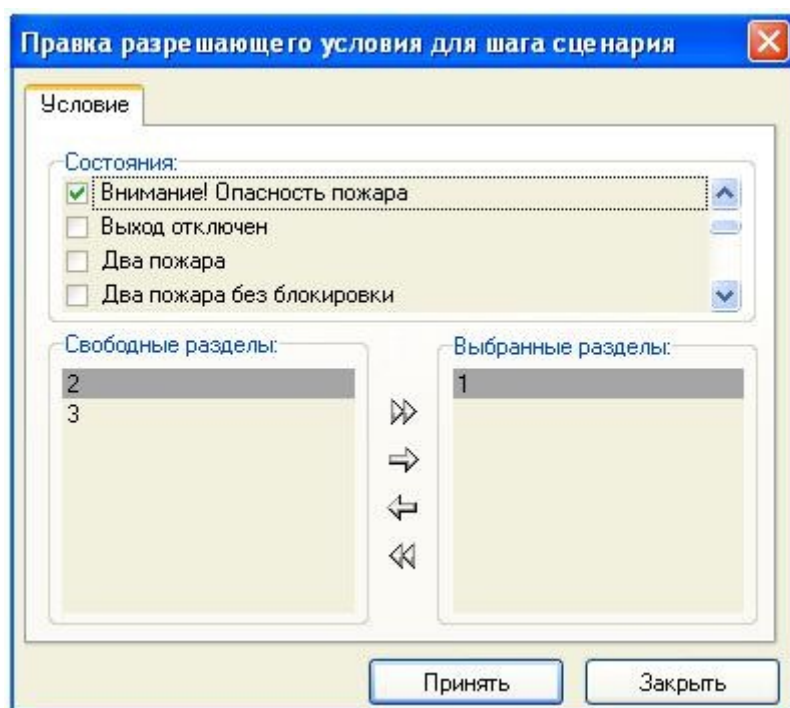


Рисунок 4.5

Отметьте «птичкой» то состояние (состояния) разделов, которое будет определять состояние системы для данной части условия. Для выбора разделов из списка в левой нижней части окна воспользуйтесь нужными инструментами окна (выбранные разделы будут отображаться в правой нижней части окна):

 Выбрать все

 Выбрать выделенный раздел

 Отменить выбор выделенного раздела

 Отменить выбор всех разделов

После того как требуемые разделы и состояния указаны, нажмите кнопку «Принять», и созданная часть условия будет отображаться в окне «Состояния и разделы для шага сценария» (см. Рисунок 4.6).



Рисунок 4.6

### **Задание к работе:**

1. Создать новую конфигурацию
2. Добавить Контроллер С2000-2.
3. Создать раздел для системы контроля и управления доступом.
4. Настроить тактику работы реле для управления реле.

### **Порядок выполнения работы:**

## 1. Запустить программу «Pprog.exe»

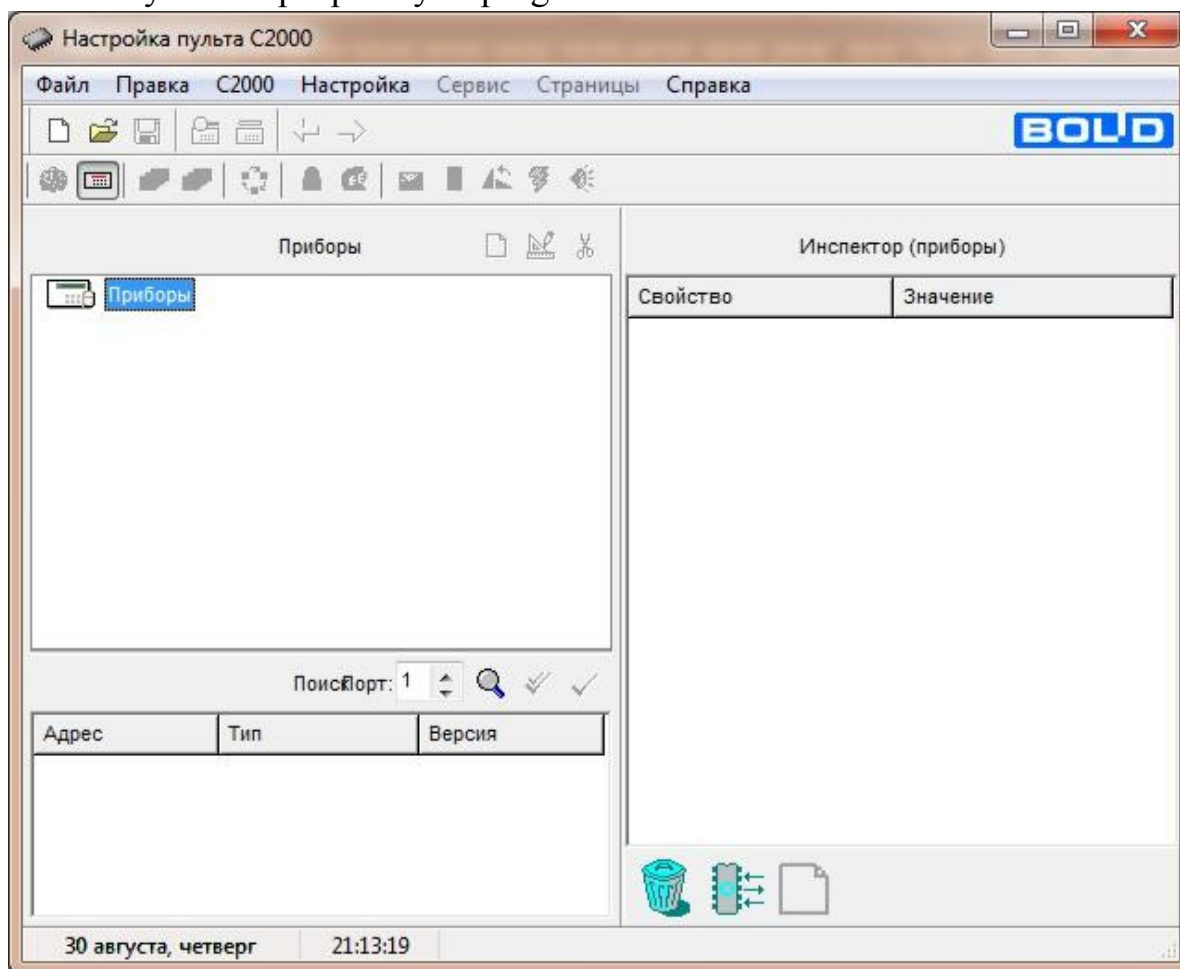


Рисунок 4.7

## 2. Создать новую конфигурацию при помощи кнопки

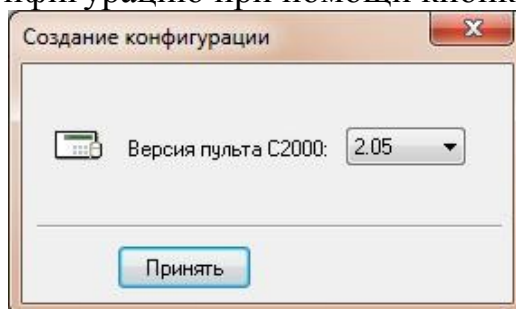




Рисунок 4.8

3. Добавить новый прибор при помощи кнопки . При помощи кнопки «Править прибор»  в инспекторе приборов изменить свойства и значения прибора. Выбираем тип прибора C2000-2, адрес задаётся автоматически – 1.

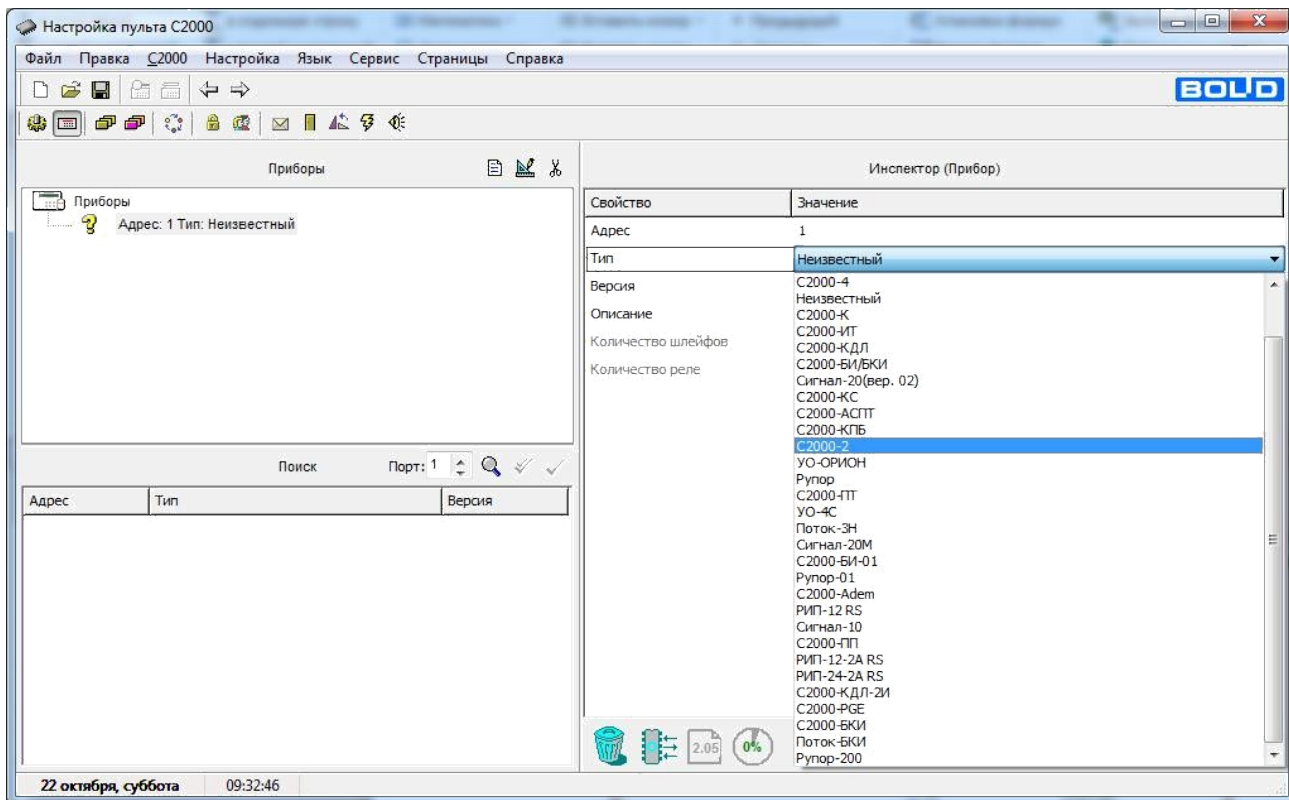





Рисунок 4.9

4. Во вкладке «Разделы» в зоне «Разделы»  создать раздел при помощи кнопки  и дать ему название при помощи кнопки  (Входная дверь).

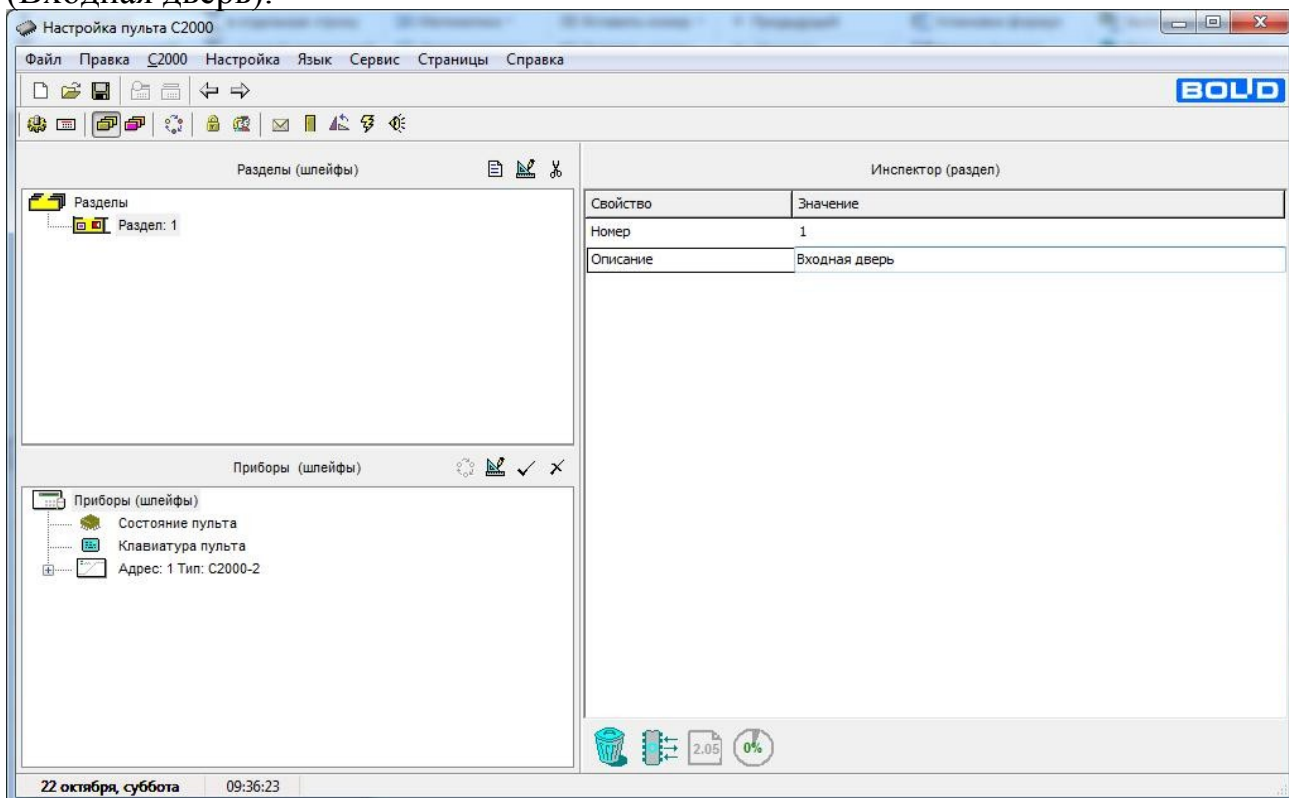


Рисунок 4.10

5. В зоне «Приборы» раскрыть список шлейфов C2000-2 задать тип шлейфа:

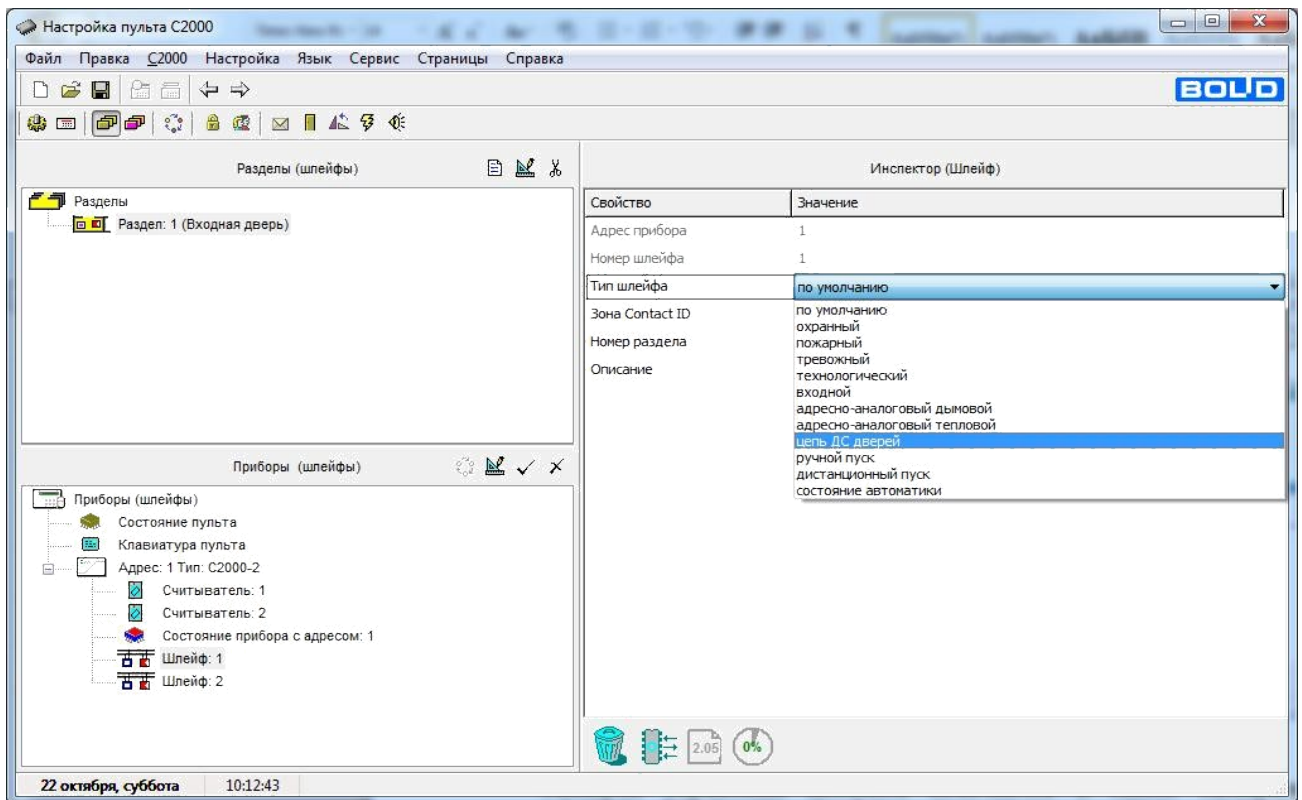


Рисунок 4.11


6. Назначаем управление Разделом 1(Входная дверь) Шлейфом 1 путём перетаскивания Шлейфа 1 в Раздел 1.

7. Назначаем управление Разделом 1(Входная дверь) Считывателями 1 и 2 путём перетаскивания их в Раздел 1.

8. На вкладке Реле задаём Программу управления дверным замком для Реле 1:

Инспектор (реле)	
Свойство	Значение
Адрес прибора	1
Номер реле	1
Описание	Управление замком
Программа упр.	3 (включить на время)
Задержка вкл.	0
Время упр.	30

Рисунок 4.12

9. На вкладке Уровни доступа  создаём уровень доступа для Директора:

- Нажимаем  и даём описание

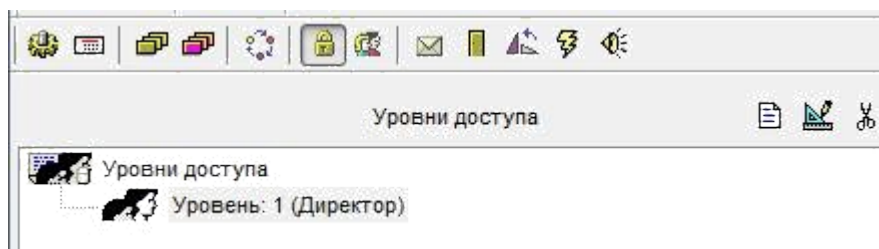


Рисунок 4.13

- Назначаем раздел для данного уровня доступа путём перетаскивания Раздела 1 из окна Разделы на Уровень 1 в окне Уровни доступа

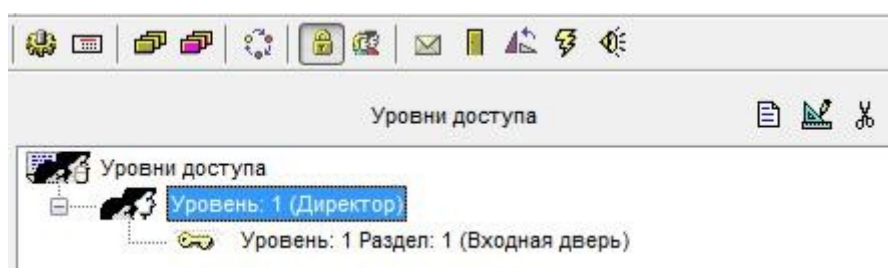


Рисунок 4.14

10. Создаём уровень доступа для бухгалтера с той же последовательностью действий.

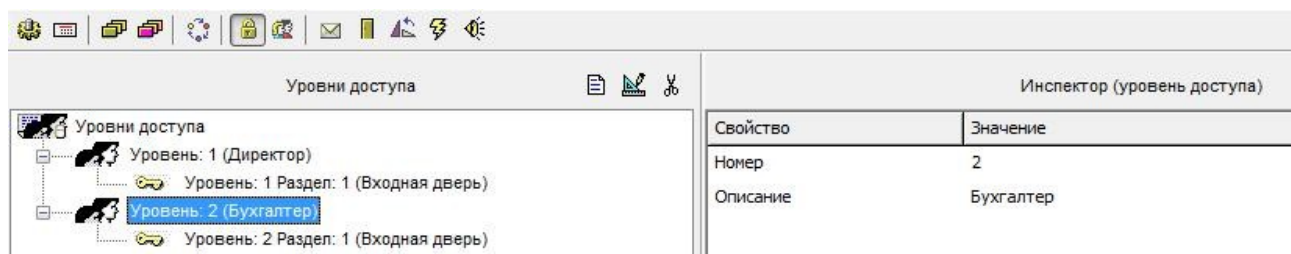


Рисунок 4.15

11. Задаём пароль. На вкладке пароли. По умолчанию отображается код для перевода пульта С2000-М в режим программирования и код для управления шлейфами

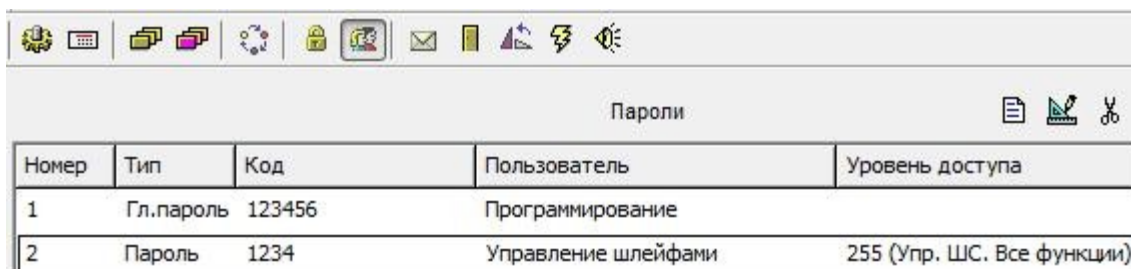


Рисунок 4.16

- 1) Для Главного пароля вносим описание в окне Инспектор (пароль): - Уровень доступа: 1(Директор)
- 2) Для Пароля:

- Уровень доступа: 2 (Бухгалтер)

12. Создать сценарий управления доступом для автоматической подачи команды на создание режима свободного прохода (двери/турникеты открыты и предъявление ключа не требуется) при сигнале Пожар:

- На вкладке сценарии управления 🔊 добавляем сценарий Управление доступом:

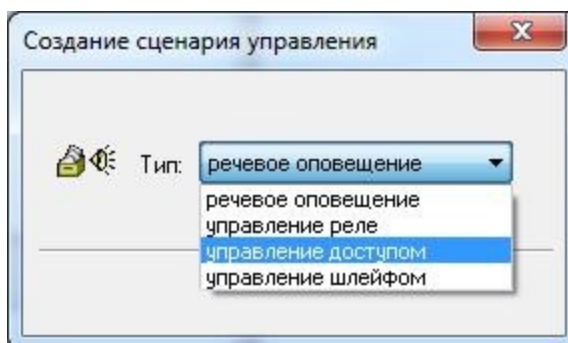


Рисунок 4.17

- Принять
- исходное состояние: нет
- добавляем шаг сценария 📄
- в описании прописываем: При пожаре
- команда считывателю: открыть доступ

13. Привязать создаваемый сценарий управления к считывателю, которому пульт будет синхронно выдавать управляющие команды в рамках создаваемого сценария. Для этого следует:

- в окне сценариев управления отметить нужный сценарий управления

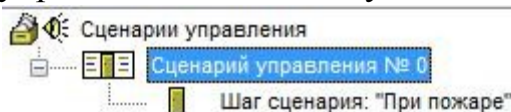


Рисунок 4.18


- в нижнем окне выбрать нужный считыватель, отвечающий за разблокировку двери при выходе)
- выбрать нужное значение параметра «Сценарий» в окне «Инспектор» (см. Рисунок 4.19).

Инспектор (реле)	
Свойство	Значение
Адрес прибора	1
Номер считывателя	1
Сценарий	не задан
	не задан
	Сценарий № 0

Рисунок 4.19



14. Задать необходимые компоненты сценария управления связанными считывателями. Для этого:

- выбрать Шаг сценария
- в окне Состояния и разделы для шага сценария выбираем  Править разрешающее условие
- из перечня состояний отмечаем: Пожар
- из окна Свободные разделы переносим 1 (Входная дверь) в Выбранные разделы

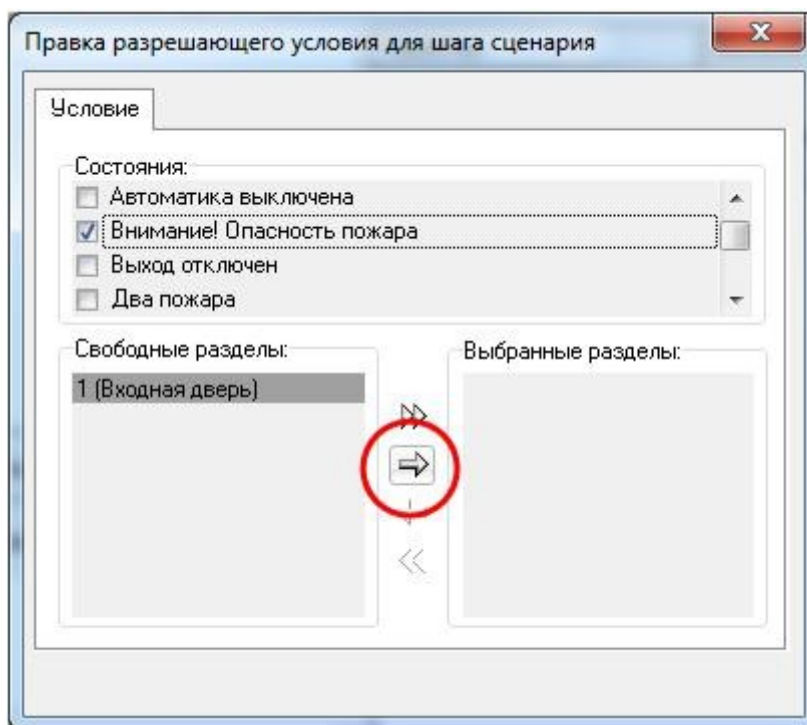



Рисунок 4.20

- в окне Инспектор автоматически появляется Команда считывателю: открыть доступ

- в окне Состояния и разделы для шага сценария выбираем  Править запрещающее условие

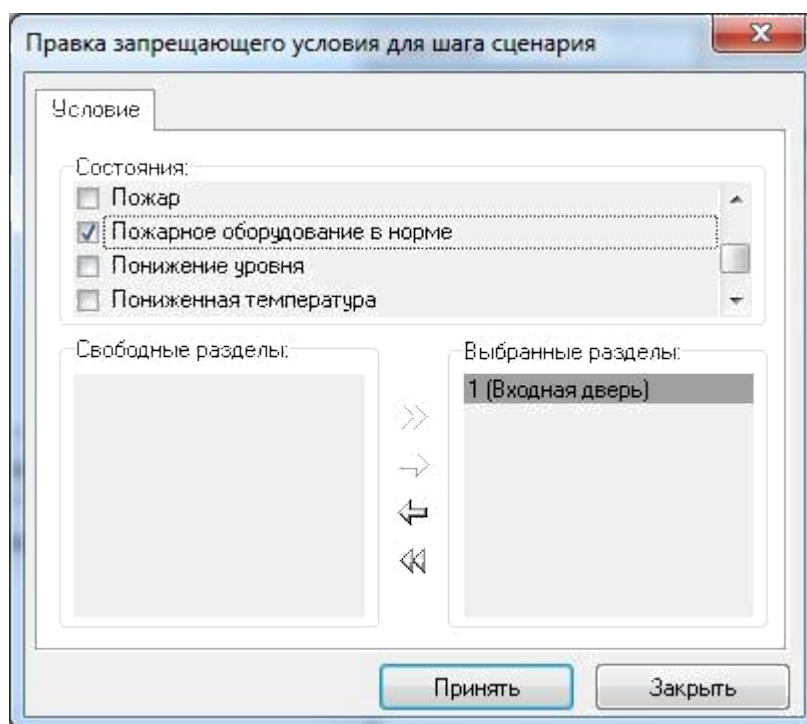


Рисунок 4.21

- результатом создания сценария будет следующий вид окна Состояния и разделы для шага сценария

Разрешающее условие	Запрещающее условие
Пожар	Пожарное оборудование в норме
1 (Входная дверь)	1 (Входная дверь)

Рисунок 4.22

### Оформление отчета:

Отчет по работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

### Отчет должен содержать:

4. Название, цели и задачи работы;
5. Скриншоты о проделанной работе;
6. Заключение и выводы.

### **Контрольные вопросы:**

1. Дайте определение Системы контроля и управления доступом
2. Дайте определение Считывателя?
3. Назовите три основные задачи, которые призваны решать современные системы контроля доступа?
4. Из каких основных устройств строится СКУД?

### **Лабораторная работа №5**

#### **Тема: Программирование proximity -карт с помощью контролера «С2000-2».**

**Цель:** научиться программировать proximity-карты с помощью контролера «С2000-2»

#### **Краткая теория**

Система контроля и управления доступом (СКУД) — это совокупность программных и технических средств, а также организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением охраняемого объекта.

Современные системы контроля доступа призваны решать три основные задачи:

- Организация контроля перемещения персонала.** Правильная организация труда. Каждому пользователю достаточно выдать один ключ (“Touch Memory” или карту «Proximity») для его идентификации системой охраны объекта. Исключение возможности праздно шатания сотрудников.
- Организация учета.** Создание системы учета рабочего времени (на основе анализа времени прихода/ухода сотрудника с территории предприятия или рабочего места). Контроль места нахождения сотрудника на объекте с точностью до зоны доступа.
- Организация охраны предприятия.** Интеграция СКД с системой охранно-пожарной сигнализации для комплексного решения задач

безопасности. Обеспечение реакции охранной составляющей системы на попытки несанкционированного доступа, взлома дверей и т.д. Возможность автоматической постановки/снятия с охраны помещений по факту прохода в зону доступа сотрудника. Предоставление свободного доступа в случае возникновения пожара.

### Термины и определения

- **Контроллер доступа** – это устройство, предназначенное для управления доступом через контролируемые точки доступа путём анализа считанных с помощью считывателей идентификаторов пользователей (проверки прав). Контроллеры доступа могут сами принимать решения предоставлять или не предоставлять доступ в случае, если идентификаторы пользователей хранятся в памяти контроллера (в таком случае говорят, что используется локальный доступ). Также идентификаторы пользователей могут быть записаны только в сетевом контроллере (в базе данных программного обеспечения). В этом случае контроллер доступа выполняет функции ретранслятора – отправляет код сетевому контроллеру и получает от него решение о предоставлении или не предоставлении доступа (в таком случае говорят о централизованном доступе). Контроллеры доступа управляют преграждающими устройствами с помощью контактов реле;
- **Идентификаторы** – уникальные признаки пользователей СКУД. Идентификатором может быть электронный ключ Touch Memory, бесконтактная Проху-карта, радио-брелок, PIN-код, биометрические данные (отпечаток пальца, ладони, рисунок радужной оболочки или сетчатки глаза, геометрические характеристики лица и т.п.). В СКУД каждому идентификатору присваиваются определённые полномочия, в соответствии с которыми контроллерами доступа разрешается или запрещается проход;
- **Считыватели** – устройства, предназначенные для считывания кода идентификатора пользователя и передачи его контроллеру доступа;
- **Точка доступа** – логический объект СКУД, фактически представляет собой физическую преграду, оборудованную контроллером доступа и считывателем. Точкой доступа может являться дверь, калитка, турникет, шлагбаум, шлюз, и т.п. Точки доступа, могут работать в двух режимах: с контролем и без контроля направления прохода. Точки доступа с контролем направления прохода могут быть как двунаправленными (оборудованными двумя считывателями), так и однонаправленными (с

одним считывателем, без возможности прохода в обратном направлении). Выход через точки доступа без контроля направления прохода чаще всего осуществляется по кнопке.

- **Зона доступа** – логический объект СКУД. Зоны доступа – это участки, на которые разбита территория охраняемого предприятия. На границах зон доступа всегда располагаются точки доступа с направлением прохода. Зоны доступа настраиваются для точек доступа в случае, если в системе используются такие функции, как расчёт рабочего времени и запрет повторного прохода (правило antipassback);
- **Уровень доступа** – индивидуальные права доступа, которые определяют правила прохода через точки и присутствия в зонах доступа, назначенные идентификатору пользователя. На основе этих прав контроллеры доступа (или сетевые контроллеры) принимают решение о предоставлении или не предоставлении доступа;
- **Окна времени** – совокупность временных интервалов, в течение которых разрешён проход. Временные интервалы могут устанавливаться для каждой точки или зоны доступа индивидуально;

#### **Типовые режимы работы СКУД:**

- Стандартный режим прохода.
- Запрет повторного прохода (правило antipassback).
- Доступ по правилу двух (или более) лиц.
- Доступ с подтверждением.
- Двойная идентификация.
- Закрытый режим доступа.
- Открытый режим доступа.

Контроллер имеет возможность работать в нескольких режимах: «две двери на вход», «одна дверь на вход/выход», «турникет», «шлагбаум», «шлюз».

**Одна дверь на вход/выход.** Данный режим предназначен для управления доступом через одну дверь, у которой имеется только одно запорное устройство и которая контролируется одним датчиком прохода (рисунок 1). Предоставление доступа в обоих направлениях требует предъявления идентификаторов пользователей. Для предоставления доступа также могут использоваться кнопки выхода (например, для открывания двери с поста охраны).

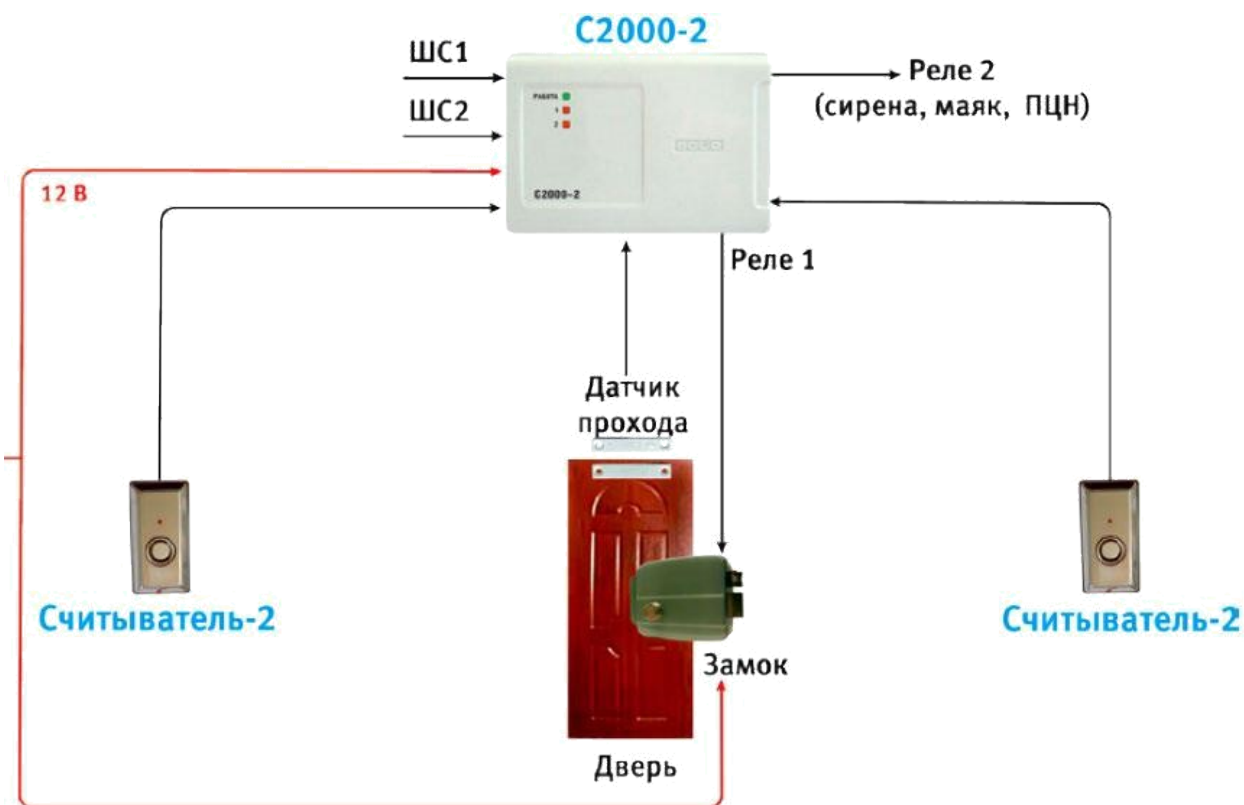


Рисунок 1 – Схема режима Одна дверь на вход/выход

Контроллер доступа "С2000-2" (в дальнейшем – контроллер) предназначен для управления доступом (рисунок 2).

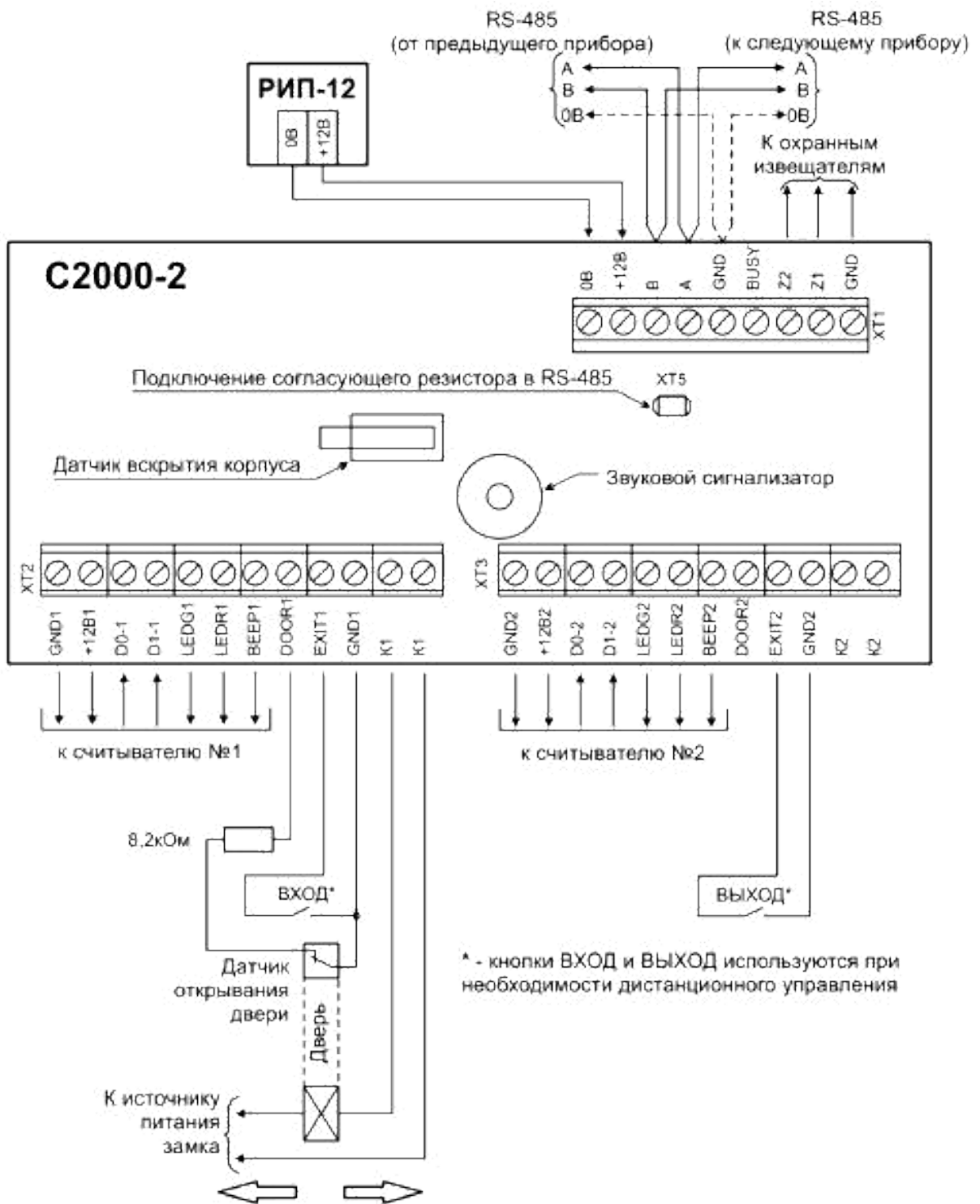


Рисунок 2 – Внешний вид контроллера доступа "С2000-2"

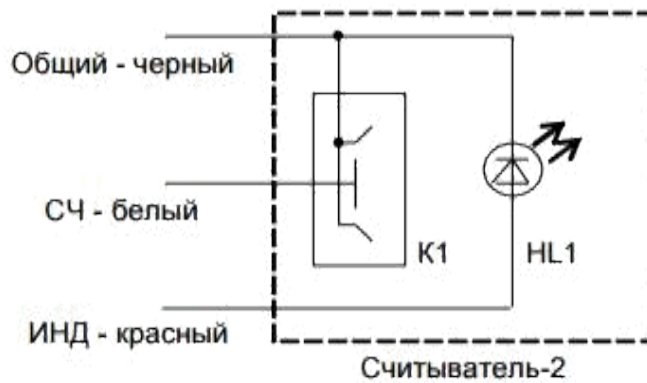
Контроль доступа осуществляется путем считывания кодов предъявляемых идентификаторов (карт Proximity, ключей Touch Memoгу и PIN-кодов), проверки прав доступа и замыкания (размыкания) контактов реле, управляющих запорными устройствами (электромеханическими и электромагнитными замками и защелками, турникетом, шлагбаумом).

Каждый идентификатор имеет индивидуальный код, который присваивается еще на заводе-изготовителе. Ключ считывается через контактор и со считывателя на контроллер передается сигнал. Контроллер индексирует свою память и в случае наличия в его памяти именно этого ключа, дает команду на открытие замка.

Локальный контроль доступа – предоставление либо запрет доступа по идентификатору (ключу), занесенному в базу данных контроллера, в зависимости от прав доступа данного ключа, текущего режима доступа и наличия нарушений режима доступа у предъявленного ключа. На рисунке 4 показана схема подключения контроллера "С2000-2" в режиме "Одна дверь на вход/выход".







HL 1 – индикатор единичный Kingbright L-934ID

K1 – контактное устройство "Touch Memory"

Рисунок 5 - Схема подключения считывателей с интерфейсом Touch Memory.

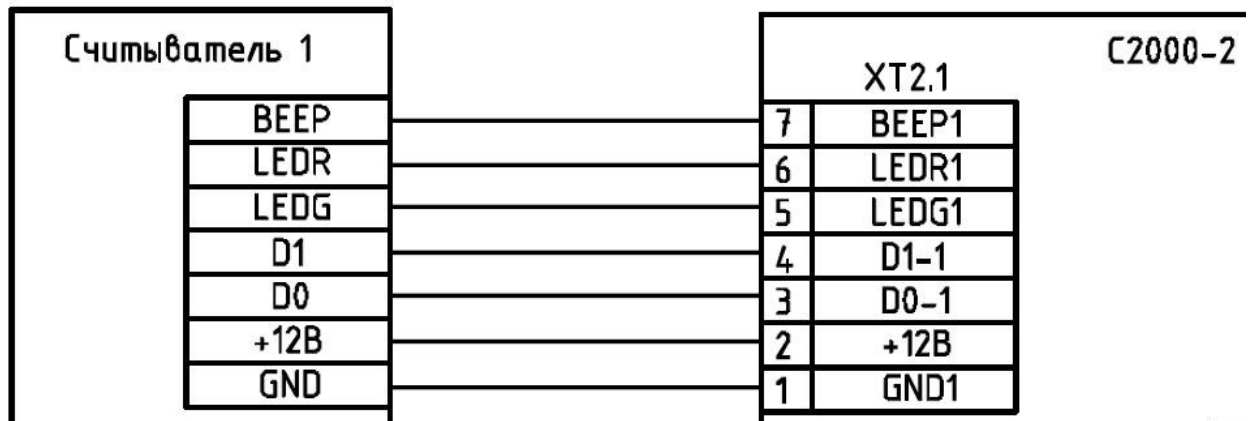


Рисунок - Схема подключения считывателей бесконтактных C2000-PROXY.

Контроллер C2000-2 может работать в автономном режиме. Однако для задания параметров работы необходим Пульт контроля и управления охранно-пожарный (ПУ) C2000 (или C2000M).

Информационное взаимодействие между пультом "C2000M" и приборами ИСО "Орион" осуществляется по проводной линии связи RS-485.

Итак, для задания параметров работы контролера C2000-2 нам необходим ПУ C2000M. Пульт объединит все приборы, которые требуется использовать в СКУД. Конфигурирование пульта C2000M осуществляется только с помощью персонального компьютера и программы "pprog.exe" версии от 2.00 и выше.

Далее потребуется программа `urprog.exe`, предназначенная для настройки конфигурационных параметров приборов, в нашем случае конфигурировать будем С2000-2.

Для связи ПУ С2000М с ПК нам потребуется преобразователь интерфейсов С2000-USB (либо USB-RS 485) для преобразования сигналов интерфейса USB в сигналы двухпроводного магистрального интерфейса RS-485 (рис. 7).

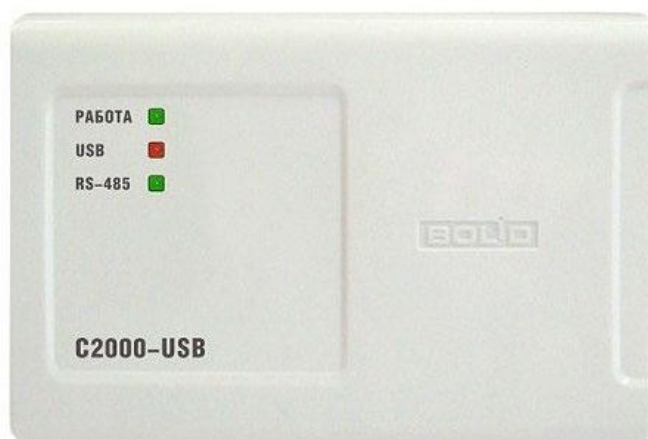
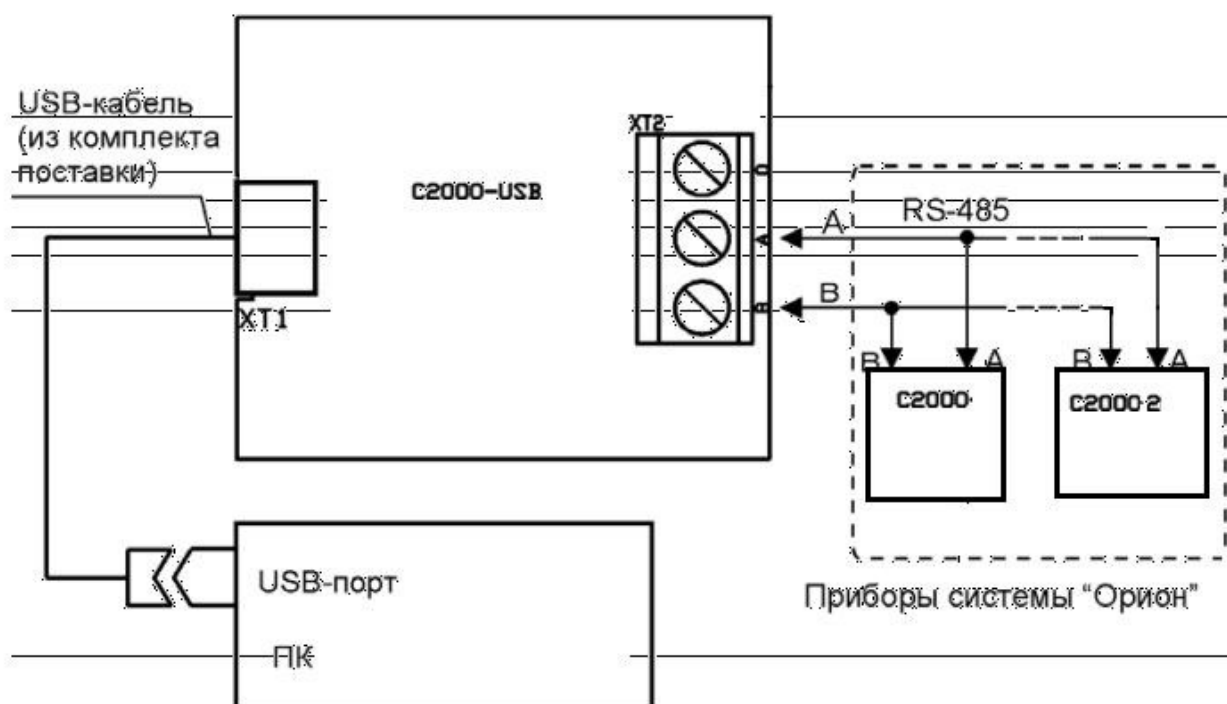


Рисунок 7 - Внешний вид преобразователя интерфейсов С2000-USB

Схема соединений интерфейса посредством С2000-USB показана на рисунке 8.



## Рисунок 8 - Схема соединений интерфейса с ПК.

При работе контроллера в составе системы "BOLID" на базе персонального компьютера коды ключей Touch Memory, Proximity-карт, PIN-коды и коды других идентификаторов заносятся в базу данных контроллера (в энергонезависимую память контроллера) с помощью программы. При работе контроллера в составе системы "BOLID" на базе пульта "С2000-2", а также при автономной работе контроллера для программирования ключей используется персональный компьютер и программа "UProg.exe". Данная программа позволяет добавлять и удалять ключи, задавать и изменять атрибуты ключей, сохранять список ключей в файл, загружать список ключей из файла в прибор и т.д.

При программировании ключей с помощью программы "UProg.exe", любой ключ можно удалить или заблокировать. А возможность вводить текстовые комментарии для ключей (фамилии владельцев) и сохранять эту информацию в файле компьютера (в контроллере она не сохраняется) – существенно облегчает процесс редактирования списка ключей.

### **Описание комплекта лабораторного оборудования «Болид».**

Комплект лабораторного оборудования «Болид» состоит из четырёх стендов. Каждый стенд оснащён оборудованием с учётом функционального назначения и выполнения различных задач. Компоновка комплекта оборудования СКУД в стендовом исполнении реализована на стенде №3. На стенде установлены отдельные блоки. Расположение блоков жёстко фиксировано. Стенд соединяется посредством разъёмов и кабелей с другими стендами для удобства проведения того или иного конкретного эксперимента. Стенд устанавливается на стене. Вид лабораторного стенда №3 показан на рисунке 9.

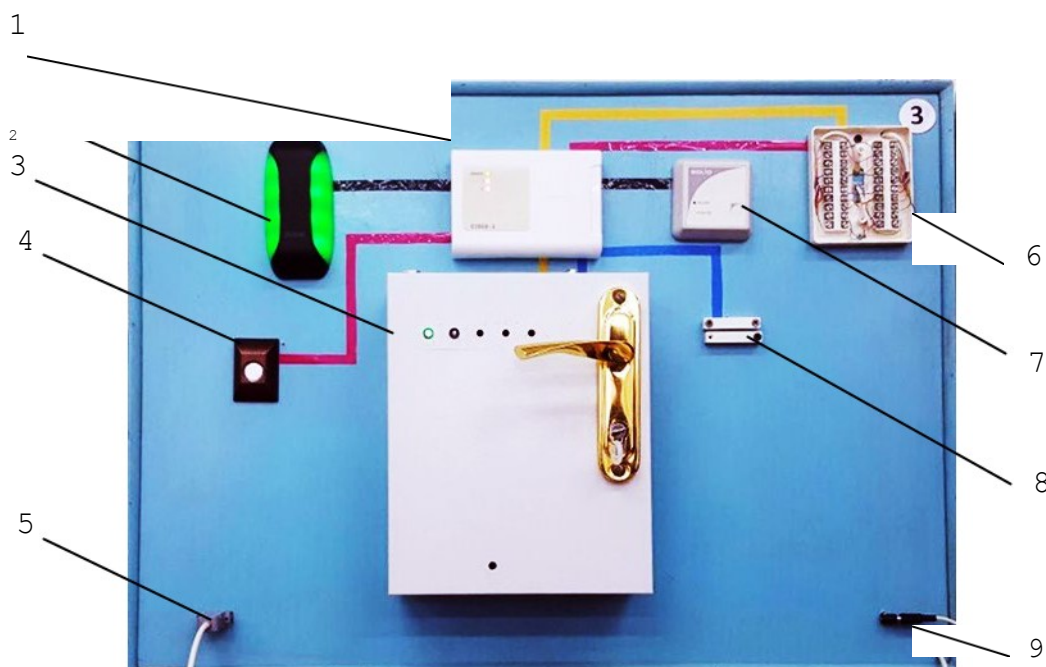


Рисунок 9. Общий вид лабораторного стенда №3.

Лабораторный стенд №3 состоит из:

- 1 – Контроллер «С2000-2»;
- 2 – Считыватель «Proxy-3A»;
- 3 – Имитатор двери со световой индикацией 12В и датчика прохода;
- 4 – Кнопка «Выход»;
- 5 - Разъёмы для подключения интерфейса RS-485, Шлейфов оповещения;
- 6 – Коробка телефонная распределительная КРТП 10x2;
- 7 – Считыватель бесконтактный «С2000-Proxy Н»;
- 8 – ШС с охранным извещателем СМК;
- 9 - Разъём для подключения напряжения 12В.

#### Порядок выполнения работы:

1. Заходим в систему от имени администратора.
2. Проверяем соединение Стенда с ПК по кабелю USB.
3. Подключаем электропитание стенда (12В).
4. Для начала работы необходимо установить время и дату на ПУ С2000. Время и дата требуются для протоколирования событий и для корректной работы временных окон в приборах, управляющих доступом («С2000-2»).

##### 4.1 Настройка времени:

С помощью клавиш пульта вводим:

- > «PROG»
- > 123456 (стандартный пароль для входа в режим конфигурирования, можно изменить в ПО PProg на вкладке пароли)
- > «ENTER»
- > Выберите пункт меню «СЕРВИС» клавишами «▲» и «▼», либо для быстрого перехода нажмите клавишу «6»
- > «ENTER»
- > Выберите пункт меню «ВРЕМЯ» клавишами «▲» и «▼», либо для быстрого перехода нажмите клавишу «1»
- > «ENTER»

На ЖКИ будет отображено текущее время в формате ЧЧ:ММ (часы и минуты).

-> Введите новое время.

После изменения времени пульт формирует два сообщения: «Изменение времени» и «Отметка времени». Сообщение «Изменение времени» информирует, когда пользователь изменил время. Сообщение «Отметка времени» показывает, какое значение времени было установлено пользователем.

#### 4.2 Настройка даты:

- > Выберите пункт меню «СЕРВИС» клавишами «▲» и «▼», либо для быстрого перехода нажмите клавишу «6»
- > «ENTER»
- > Выберите пункт меню «ДАТА» клавишами «▲» и «▼», либо для быстрого перехода нажмите клавишу «2»
- > «ENTER»

На ЖКИ будет отображена текущая дата в формате ДД.ММ.ГГ (день, месяц и год).

-> Введите новую дату.

#### 5. Включаем режим программирования С2000. Для этого:

- > нажимаем на клавиатуре кнопку «PROG»
- > 123456 (стандартный пароль для входа в режим конфигурирования)
- > «ENTER»
- > 5 НАСТРОЙКА клавишами «▲» и «▼», либо для быстрого перехода нажмите клавишу «5» -> 6 РЕЖИМ ПРОГРАММИРОВАНИЯ клавишами «▲» и «▼», либо для быстрого перехода нажмите клавишу «6»

#### 6. Запускаем Pprog.exe -> Создать конфигурацию


7. На вкладке Приборы  в окне поиска выбираем 8 порт (или тот, который отображается в диспетчере устройств номер)
8. -> нажимаем «Начать поиск» (лупа). Дожидаемся завершения поиска.



Рисунок 5.1

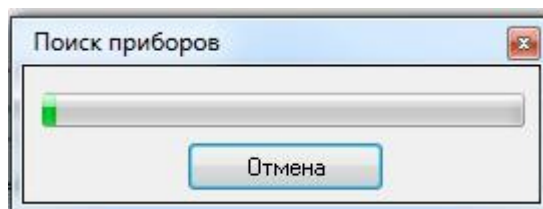


Рисунок 5.2

В окне поиска появились приборы:

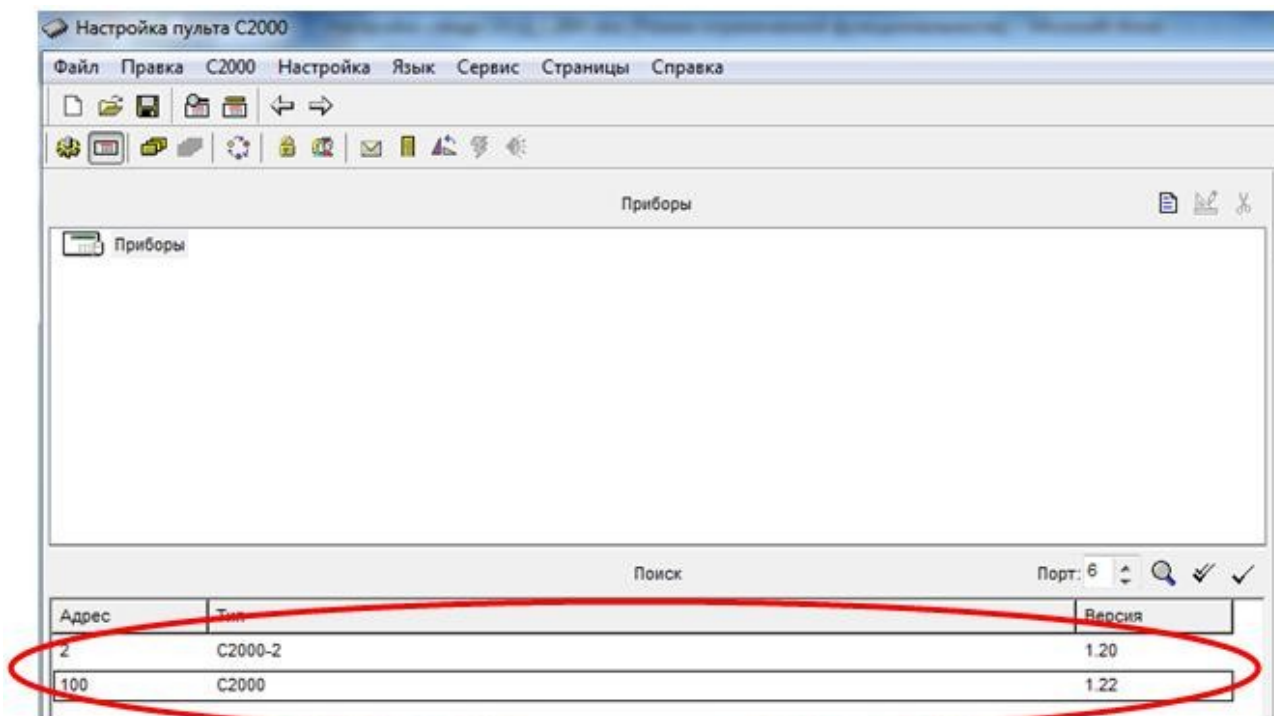


Рисунок 5.3

Нажав ЛКМ на C2000-2 в окне Поиск, переносим прибор C2000-2 в окно приборы

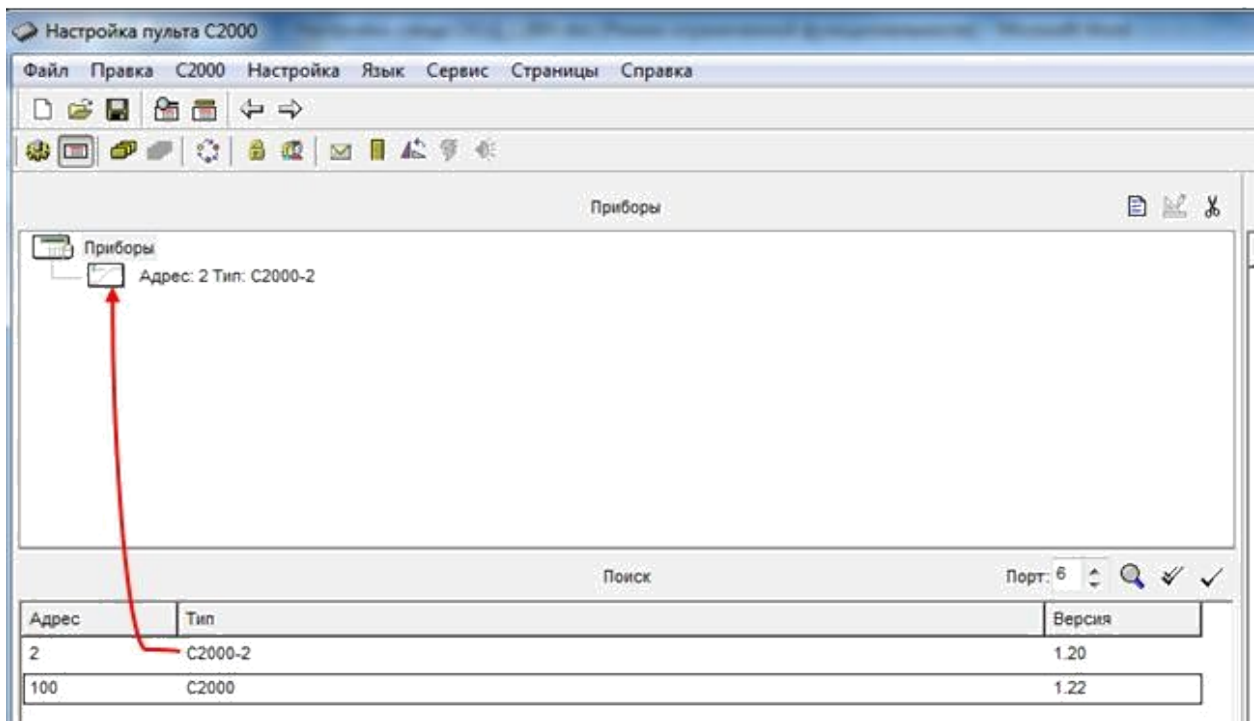


Рисунок 5.4

Записываем конфигурацию

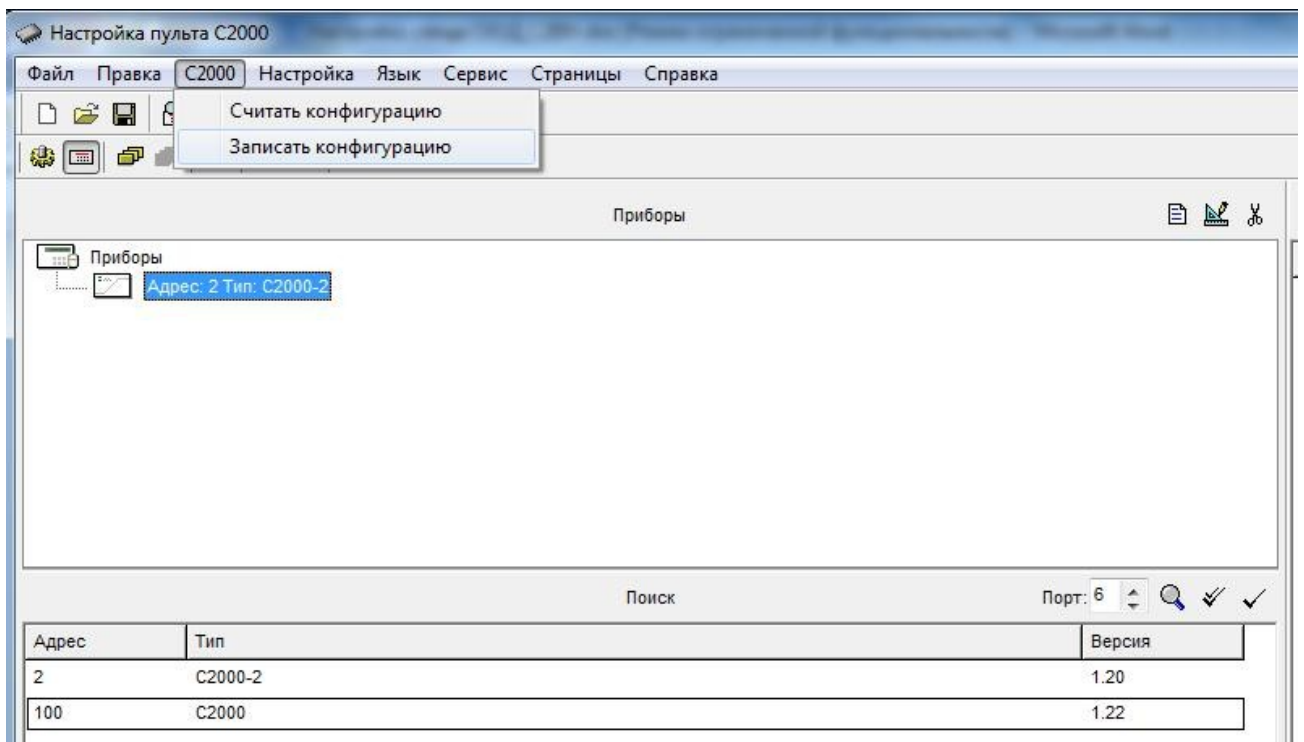


Рисунок 5.5

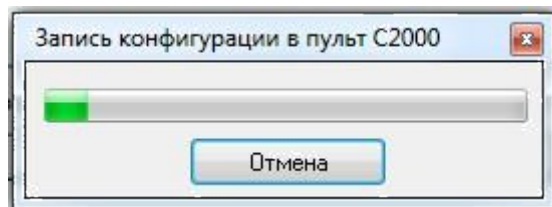


Рисунок 5.6

Подсвечивается жёлтым



Рисунок 5.7

Закрываем, сохраняем

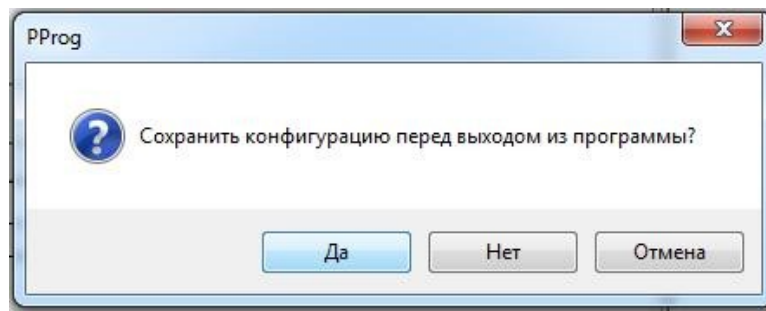


Рисунок 5.8

9. Запустить программу Uprog.exe (рис.5.8).

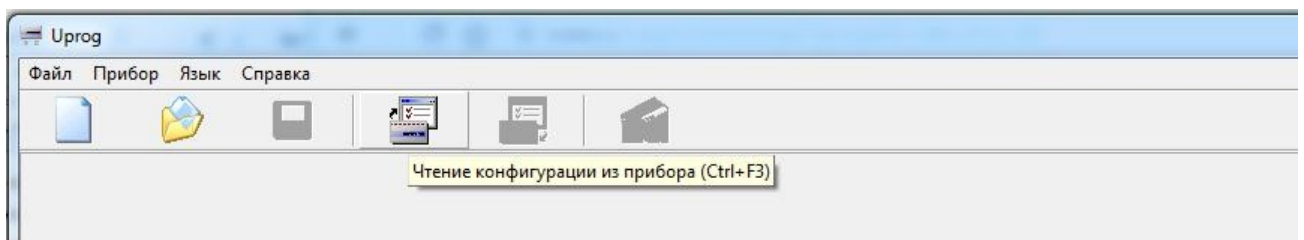


Рисунок 5.9



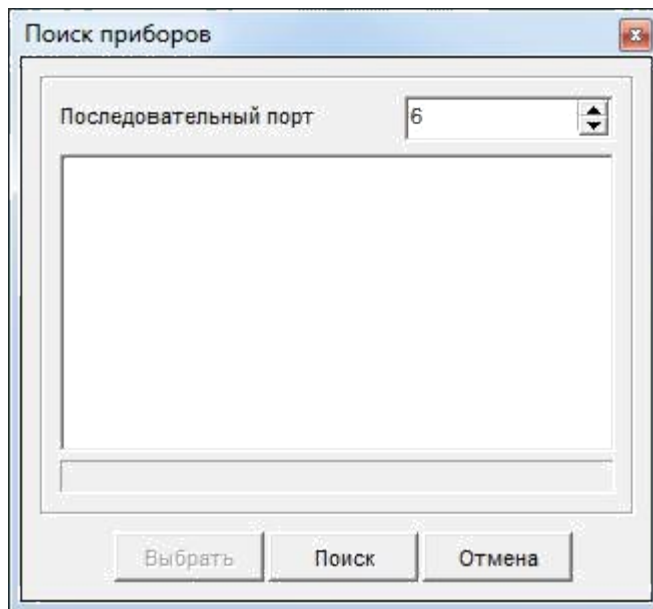


Рисунок 5.10

Далее выбираем C2000-2:

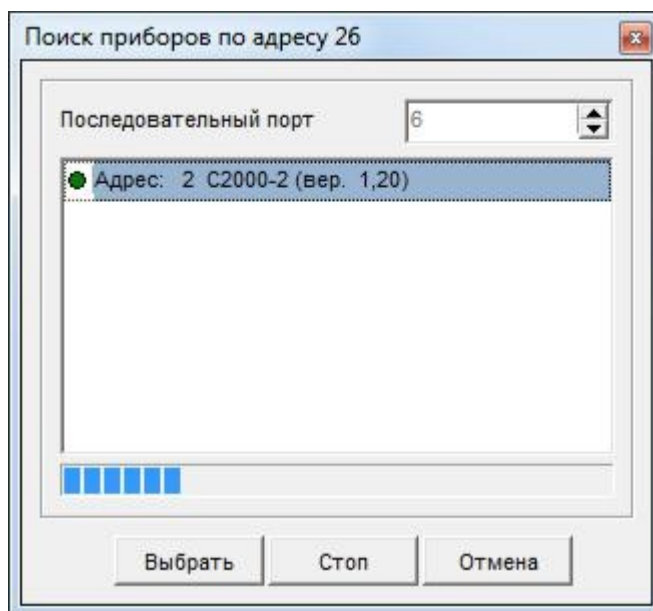


Рисунок 5.11

Произойдёт чтение конфигурационных приборов:



Рисунок 5.12

Открывается Диалоговое окно настройки параметров C2000-2. Прodelываем необходимые установки:

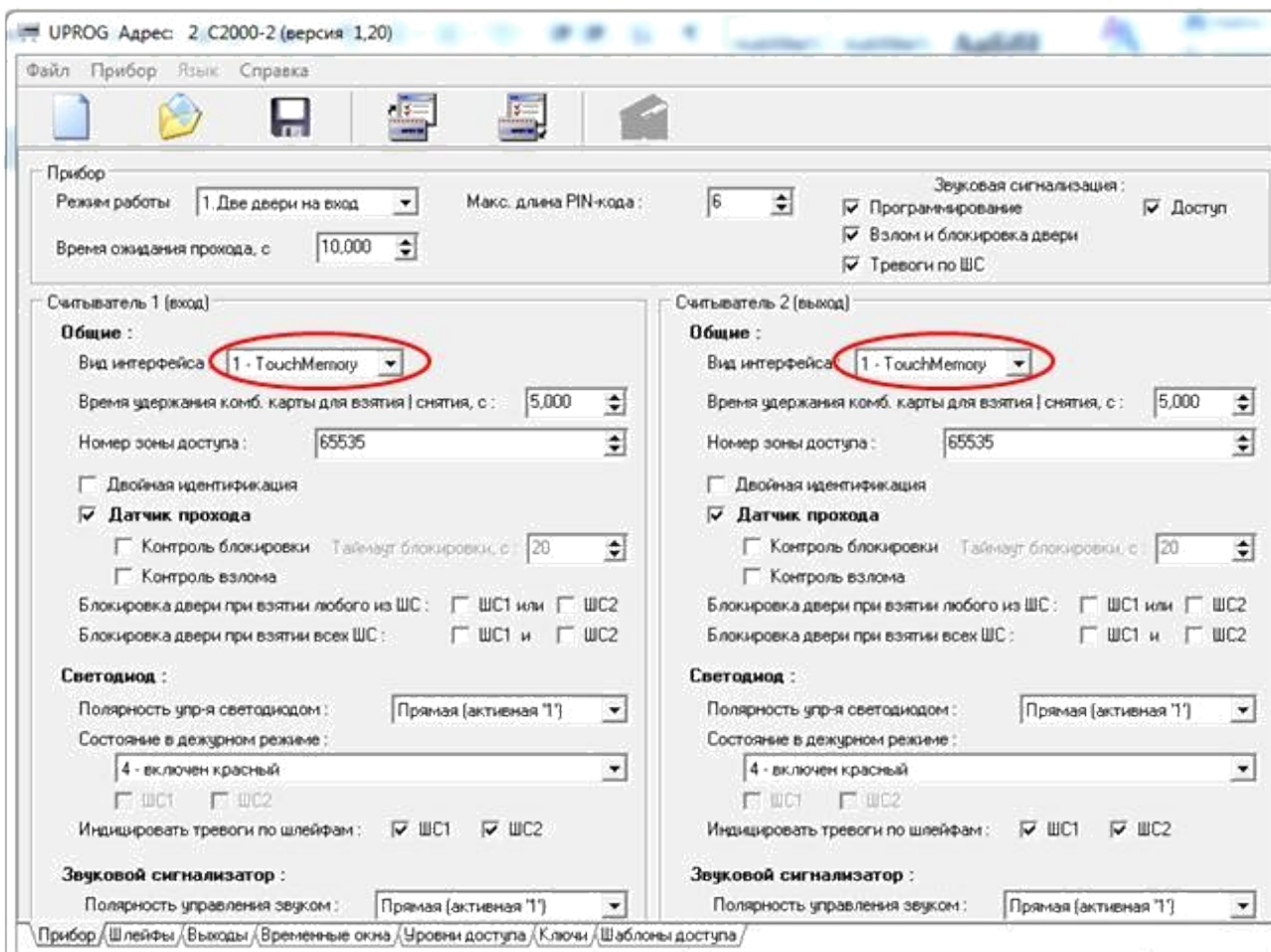


Рисунок 5.13

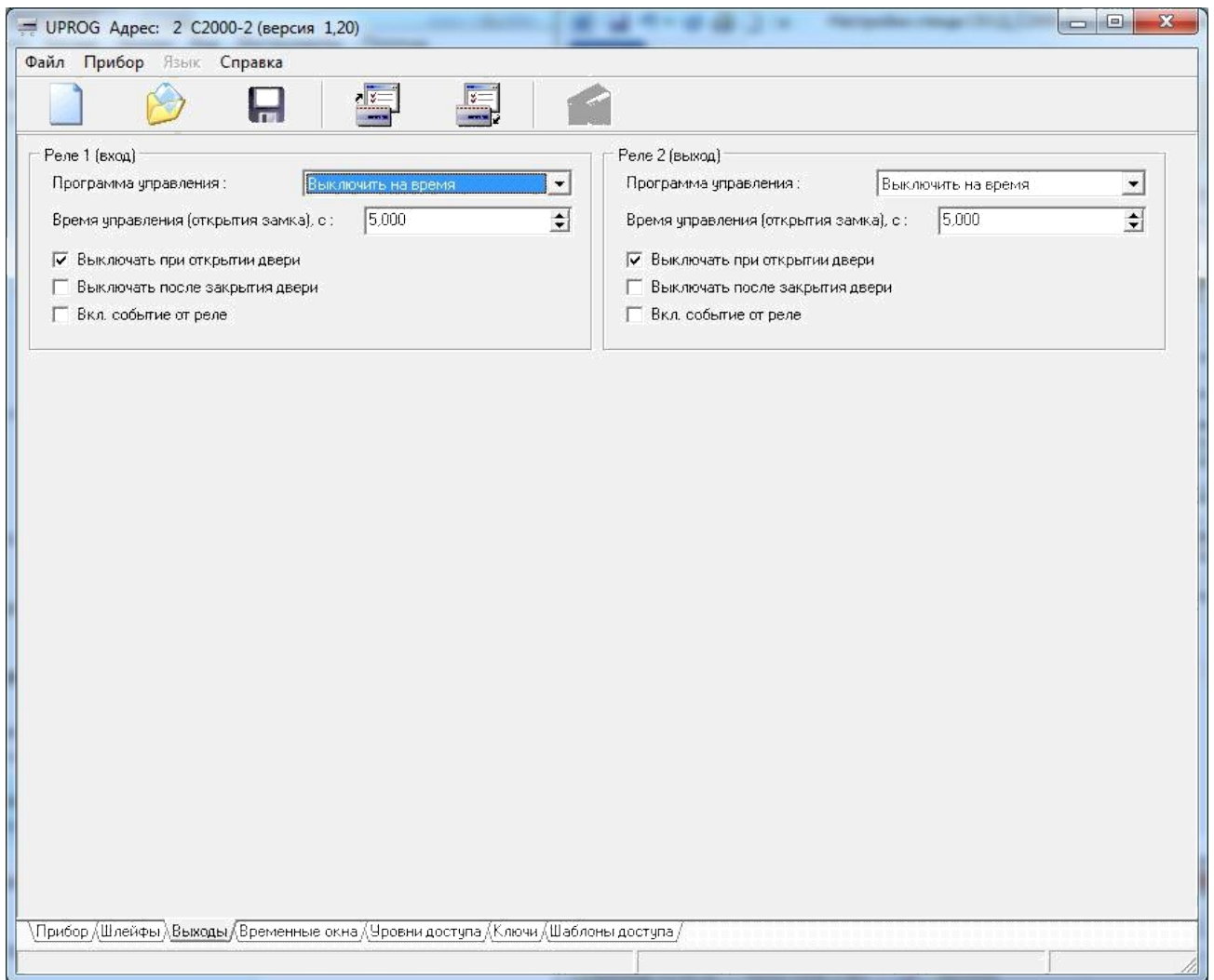


Рисунок 5.14

Переходим на вкладку «Ключи»

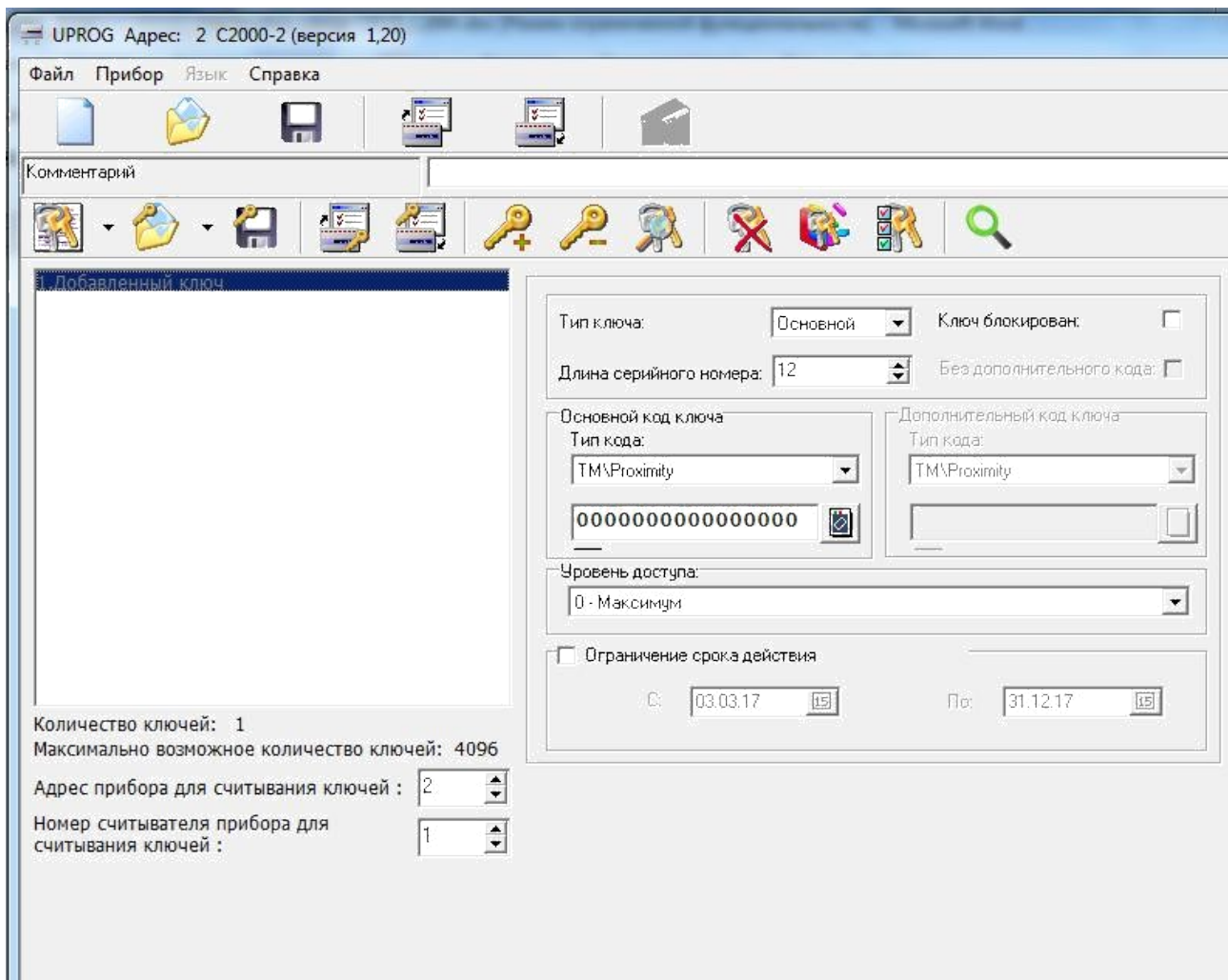




Рисунок 5.15

Если в приборе уже прописаны ключи, не используемые в системе, то стираем старые ключи с помощью кнопки «Удаление всех записанных ключей» .

После, приступаем к добавлению новых ключей в считыватели “Proxu\_3A” и “С2000–Proxu Н”:

- 1) нажимаем на кнопку «Добавить ключ в прибор»  ;
- 2) указываем тип ключа. Тип «Основной» предназначен для доступа или/и взятия/снятия ШС на охрану;
- 3) выбираем номер считывателя прибора, если у нас имеется считыватель на вход и на выход;
- 4) нажимаем на кнопку «Считать код»;

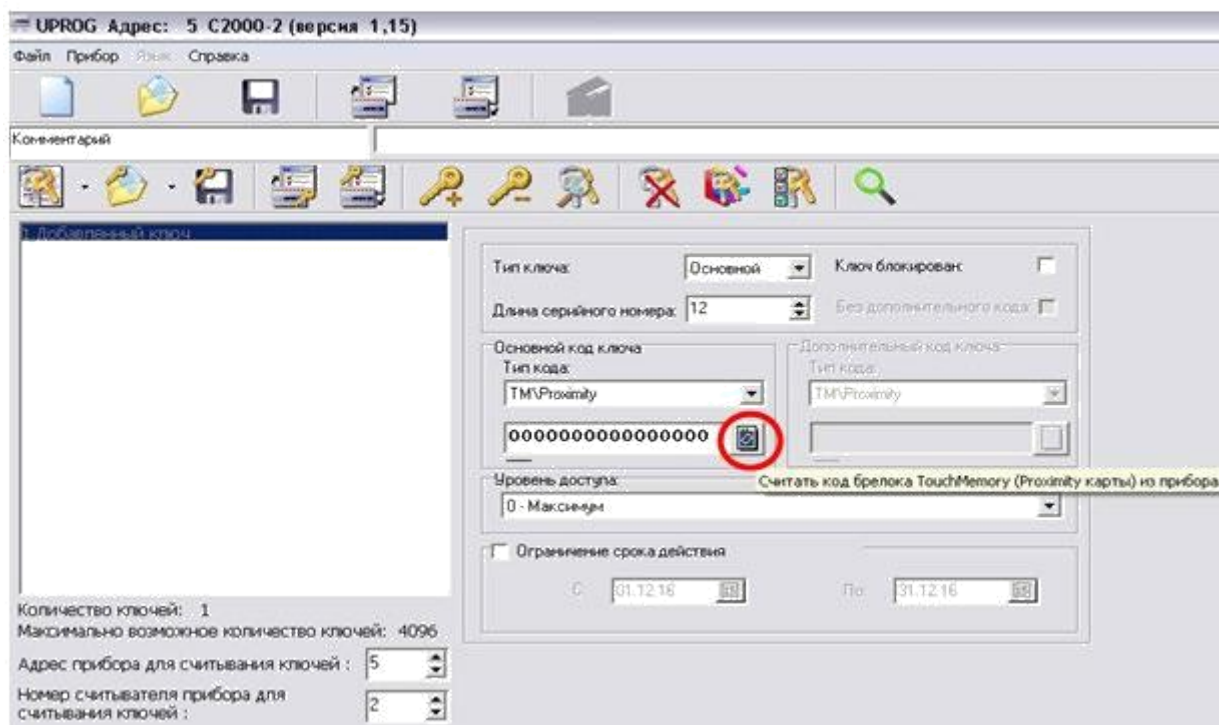


Рисунок 5.16 - Добавление ключа в считыватель

1) подносим карту к считывателю.

После появится окно «Считывание кода ключа»

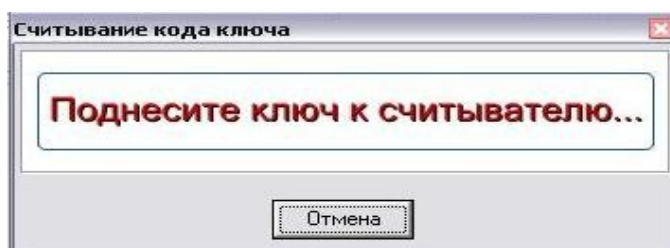


Рисунок 5.17

При пропадании активного окна «Считывание кода ключа» операция считывания выполнена, ключ добавится в прибор.

2) добавляем ключ во второй считыватель.

Аналогично добавляются ключи других пользователей.

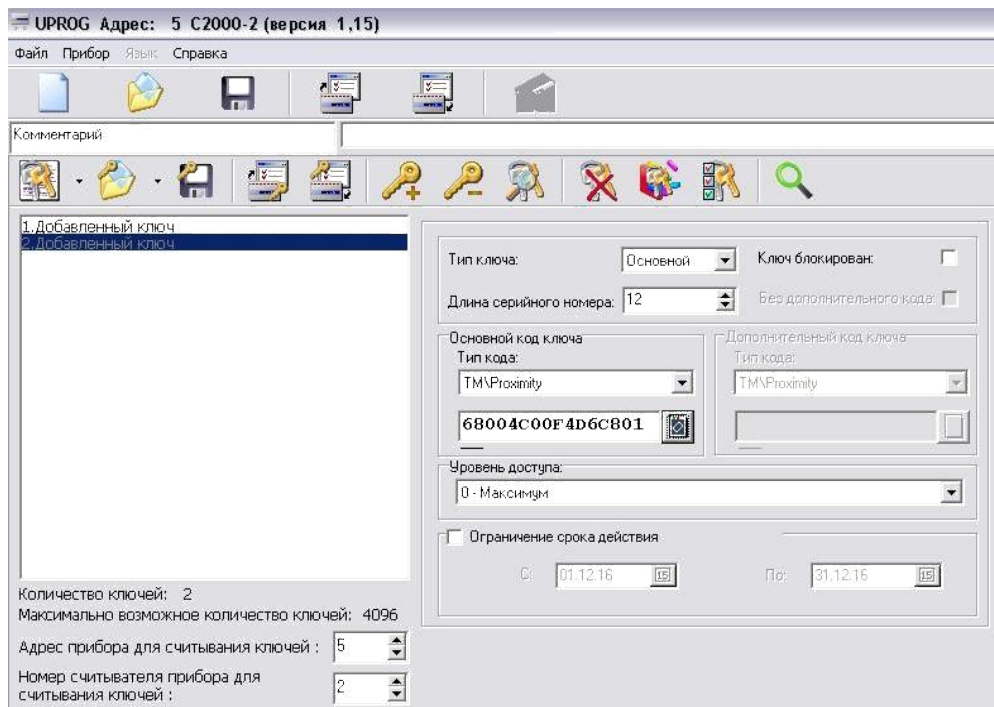


Рисунок 5.18

**Задание:**

1. Запрограммировать 3-и ключа с помощью программы "UProg.exe". Типы ключей – «Основной».
2. Запрограммировать один ключ с помощью программы "UProg.exe". Типы ключа – «МАСТЕР».
3. Запрограммировать 3-и ключа «Основной» с помощью ключа «МАСТЕР».

**Оформление отчета:**

Отчет по работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

**Отчет должен содержать:**

1. Название, цели и задачи работы;
2. Скриншоты о проделанной работе;
3. Заключение и выводы.

**Контрольные вопросы:**

1. Дайте определение идентификатора.
2. Перечислите основные виды считывателей с протоколами обмена данными, с которыми работает контролер «С2000-2»?
3. Назовите место хранения электронных ключей пользователей системы контроля доступа?
4. Может ли «С2000-2» работать автономно?

**Лабораторная работа №6**

**Тема: Настройка тактики работы системы оповещения при помощи программ «Pprog» и «UProg»**

**Цель:** научиться настраивать параметры и тактику работы интегрированной системы «Орион» для системы оповещения.

## Теория

Система охранно-тревожной сигнализации обеспечивает выполнение следующих функций: выявление (автоматически и персоналом) тревожных ситуаций и формирование сигналов тревоги. Устройства сигнализации и оповещения (сирены, лампы и т.п.), служат для информирования сотрудников службы охраны о проникновении, и для деморализации нарушителя. Система оповещения является составной частью системы охранной сигнализации и запускается автоматически при срабатывании охранной сигнализации. Оповещатели - устройства для оповещения людей о тревоге на объекте с помощью звуковых или световых сигналов.

Оповещатели предназначены для подачи световых и звуковых сигналов тревоги, привлечения внимания персонала охраны, психологического воздействия на нарушителя, информирования персонала объекта. В зависимости от характера выдаваемых сигналов они подразделяются на:

- Звуковые (сирены);
- Световые (лампы);
- или Свето-звуковые (комбинированные).

Звуковые оповещатели используются, в основном, в системах автономной сигнализации. Время звучания устройства программируется на приёмно-контрольном приборе.

Световые оповещатели также используются для отображения текущего состояния системы. Можно выделить три основных направления применения светового оповещения:

- отображение общего состояния объектовой сигнализации;
- автоматическое подтверждение принятия под охрану ПЦО;
- индикация режимов работы отдельных зон и шлейфов.

Внешние оповещатели (световой и звуковой) должны быть установлены в местах, удобных для визуального и слухового контроля.

Управление звуковыми и световыми оповещателями и их электропитание в ИСО «Орион» осуществляется от приемно-контрольных



приборов охранной сигнализации (или контрольно-пусковых блоков). Для этих целей в этих приборах предусмотрены выходы, через которые оповещатели получают напряжение питания постоянного тока для своей работы. Кроме этого, в соответствии с требованиями ГОСТ Р 53325-2009 линии связи с оповещателями контролируются на обрыв и замыкание. Схемы подключения оповещателей приведены в документации на конкретные приборы.

Примеры оповещателей для наружной установки: БИЯ-С2, Гром-12К исп.2, Гром-12К исп.3, Маяк-12-К.

**Система оповещения и управление эвакуацией при пожаре (СОУЭ)** предназначена для своевременного оповещения людей о пожаре, а также информирование о путях безопасной и максимально оперативной эвакуации с целью предотвращения ущерба их жизни и здоровью. Оповещение людей о пожаре осуществляется передачей звуковых и/или световых сигналов в помещения, где люди могут подвергаться воздействию опасных факторов пожара, а также в помещения, где могут остаться люди при блокировании эвакуационных путей пожаром, трансляцией речевой информации о необходимости эвакуироваться, о путях эвакуации и действиях, направленных на обеспечение безопасности. Управление эвакуацией осуществляется посредством передачи по СОУЭ специально разработанных текстов, направленных на предотвращение паники и других явлений, усложняющих процесс эвакуации, трансляции текстов, содержащих информацию о необходимом направлении движения, включения световых указателей направления движения и дистанционного открывания дверей дополнительных эвакуационных выходов.

Типы СОУЭ. В зависимости от функциональных характеристик (согласно СП 3.13130.2009), СОУЭ делятся на пять типов:

- 1-й тип характеризуется наличием звукового способа оповещения (звонки, тонированный сигнал и др.);

- 2-й тип характеризуется наличием звукового способа оповещения и световых указателей «Выход». Оповещение должно производиться во всех помещениях одновременно;

- 3-й тип характеризуется речевым способом оповещения (запись и передача специальных текстов) и наличием световых указателей «Выход». Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по специально разработанной очередности;

- 4-й тип характеризуется речевым способом оповещения, наличием световых указателей направления движения и «Выход». Должна обеспечиваться связь зоны оповещения с диспетчерской. Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по специально разработанной очередности;

- 5-й тип характеризуется речевым способом оповещения, наличием световых указателей движения и «Выход». Световые указатели направления движения должны быть с отдельным включением для каждой зоны. Должна обеспечиваться связь зоны оповещения с диспетчерской. Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по специально разработанной очередности. Обеспечивается полная автоматизация управления системой оповещения и возможность реализации множества вариантов организации эвакуации из каждой зоны оповещения.

Организация СОУЭ в ИСО «Орион». Для организации системы оповещения и управления эвакуацией в ИСО «Орион» можно применить следующие устройства:

1. Исполнительные выходы приёмно-контрольных приборов с контролем целостности линии. Такие выходы имеют устройства: «Сигнал-20М», «Сигнал-20П», «Сигнал-10», «С2000-4». К выходам данных устройств возможно подключать световые и звуковые оповещатели;

2. Контрольно-пусковые блоки «С2000-КПБ» с контролем целостности линии. К выходам данного блока также можно подключать световые и звуковые оповещатели. «С2000-КПБ» могут использоваться в случае, если исполнительных выходов прибора физически не хватает для подключения всех используемых в системе оповещателей, указателей и т.п.;

3. Прибор речевого оповещения «Рупор». Предназначен для трансляции предварительно записанной речевой информации. Имеет два параллельных канала оповещения по 10 Вт, рассчитанных на подключение недорогих низкоомных акустических модулей. В память прибора можно записать до 255 различных сообщений общей продолжительностью до 340 секунд. Может запускаться централизованно командой по интерфейсу RS-485 или локально. Запуск речевого оповещения локально производится при нарушении одного из четырёх шлейфов прибора. К каждому из шлейфов возможно привязать своё речевое сообщение. Кнопкой с лицевой панели прибора «Рупор» также можно запустить оповещение локально. Прибор поддерживает настройку таких параметров, как задержка оповещения, пауза между речевыми сообщениями, преамбулы речевого сообщения, время оповещения, приоритеты оповещения для сообщений.

#### **Описание комплекта лабораторного оборудования «Болид».**

Комплект лабораторного оборудования «Болид» состоит из четырёх стендов. Каждый стенд оснащён оборудованием с учётом функционального назначения и выполнения различных задач. Компоновка комплекта оборудования системы оповещения в стендовом исполнении реализована в лабораторном стенде №4. На стенде установлены отдельные блоки. Расположение блоков жёстко фиксировано. Стенд соединяется посредством разъёмов и кабелей с другими стендами для удобства проведения того или иного конкретного эксперимента. Стенд устанавливается на стене. Вид лабораторного стенда №4 показан на рисунке 1.

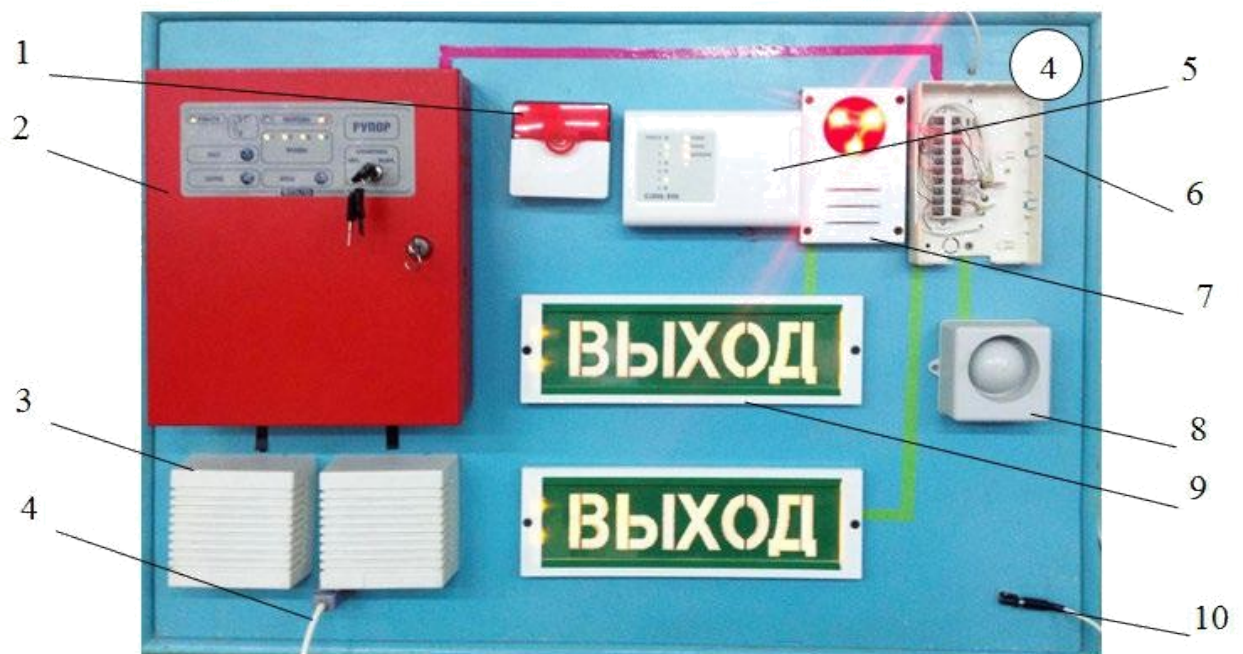


Рисунок 1. Общий вид лабораторного стенда №4

Лабораторный стенд №4 состоит из:


- 1 – Оповещатель комбинированный светозвуковой ОПОП 124-7;
- 2 – Прибор речевого оповещения «Рупор»;
- 3 – Громкоговорители настенные «ROXTON»;
- 4 – Разъём для подключения RS-485, Шлейфов оповещения;
- 5 – Блок контрольно-пусковой С2000-КПБ;
- 6 – Коробка телефонная распределительная КРТП 10х2;
- 7 - Комбинированный оповещатель «Маяк-12-К»;
- 8 – Сирена «Свирель»;
- 9 - Световое табло «ВЫХОД»;
- 10– Разъём для подключения напряжения 12В.

## 2. Порядок выполнения работы

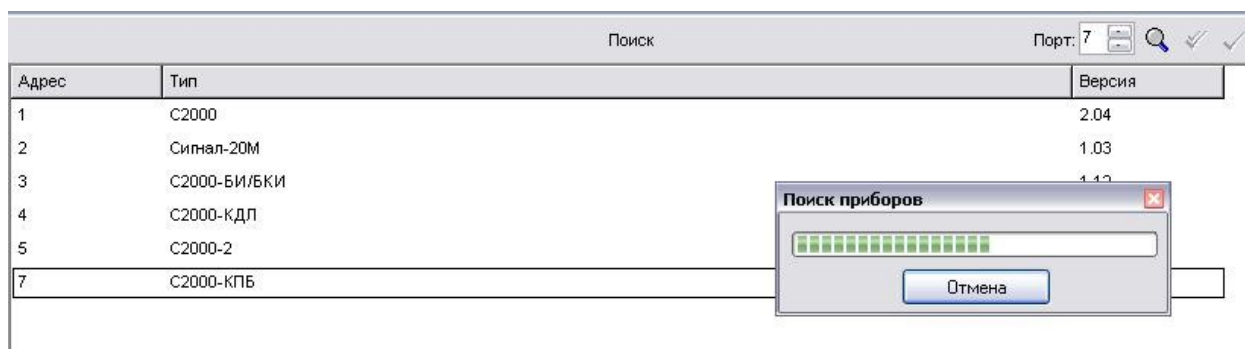
### 2.1 Прошивка пульта С2000 М

Сначала проверяем соединения между стендами, подключаем питание на всех стендах и включаем режим программирования С2000 М. Для этого нажимаем на клавиатуре кнопку «PRG», вводим стандартный пароль для

входа в режим конфигурирования (заводской – 123456, можно изменить в PProg на вкладке пароли), выбираем пункт 5 НАСТРОЙКА, в нем 56 РЕЖИМ ПРОГРАММИРОВАНИЯ (можно выбрать цифрами с клавиатуры введя 5-6).


Чтобы прошивать прибор открываем PProg -> на вкладке Приборы  в окне поиска выбираем 7 порт (предварительно проверить в диспетчере устройств номер порта) -> нажимаем «Начать поиск» (лупа). Дожидаемся завершения поиска.

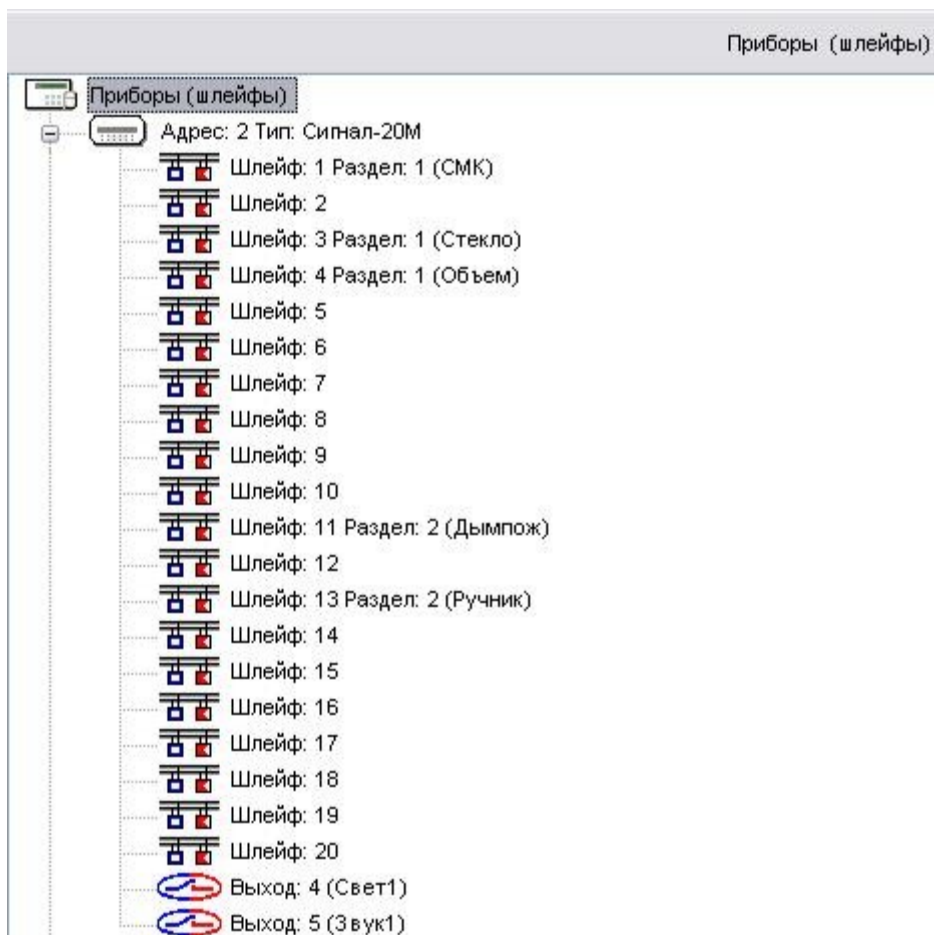
ЗАМЕТКА: Для изменения адреса соответствующего прибора выходим из режима программирования, вновь входим в режим конфигурирования -> 3 АДРЕСА -> 31 АДРЕСА ПРИБОРОВ -> вводим старый адрес и нажимаем ENT -> вводим новый адрес для прибора и нажимаем ENT.

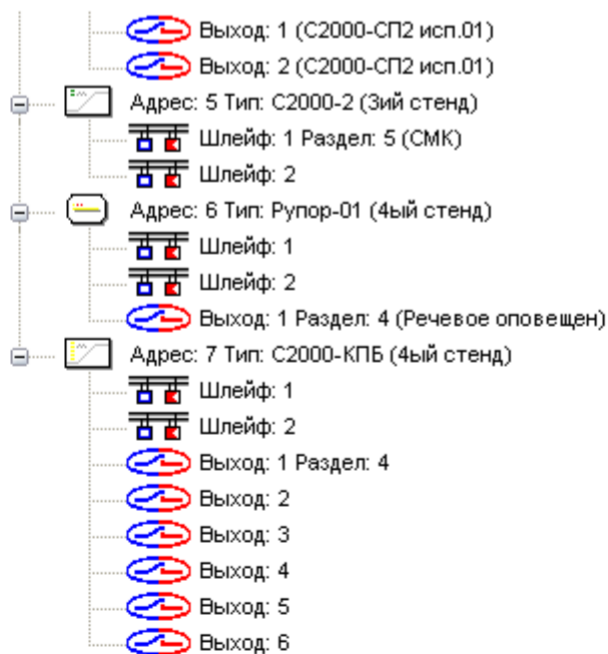
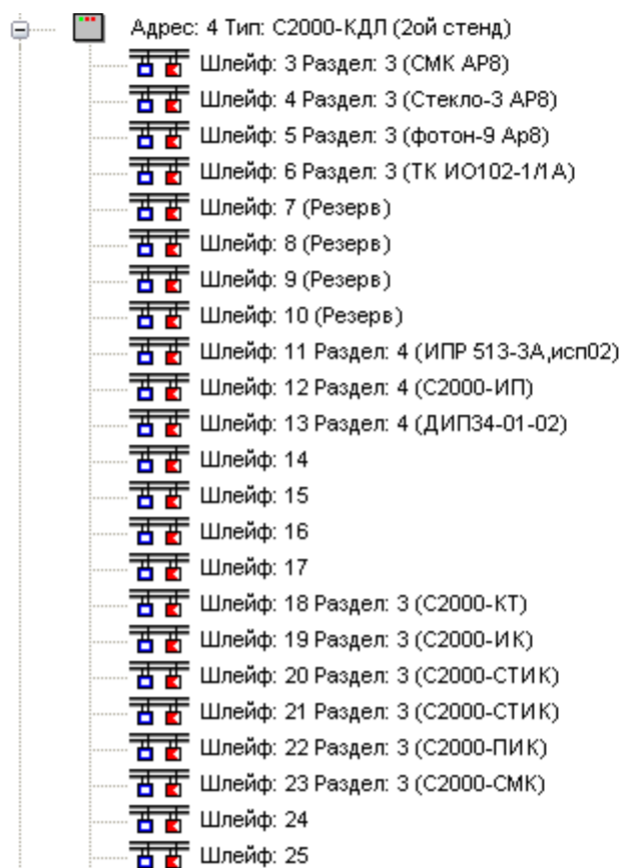


Чтобы считать уже имеющуюся конфигурацию, в пункте меню выбираем C2000 -> Считать конфигурацию. Приступаем к конфигурированию. Первое что сделаем - привяжем все приборы в системе пульту C2000 М перетаскиванием из окна «Поиск» в окно «Приборы».

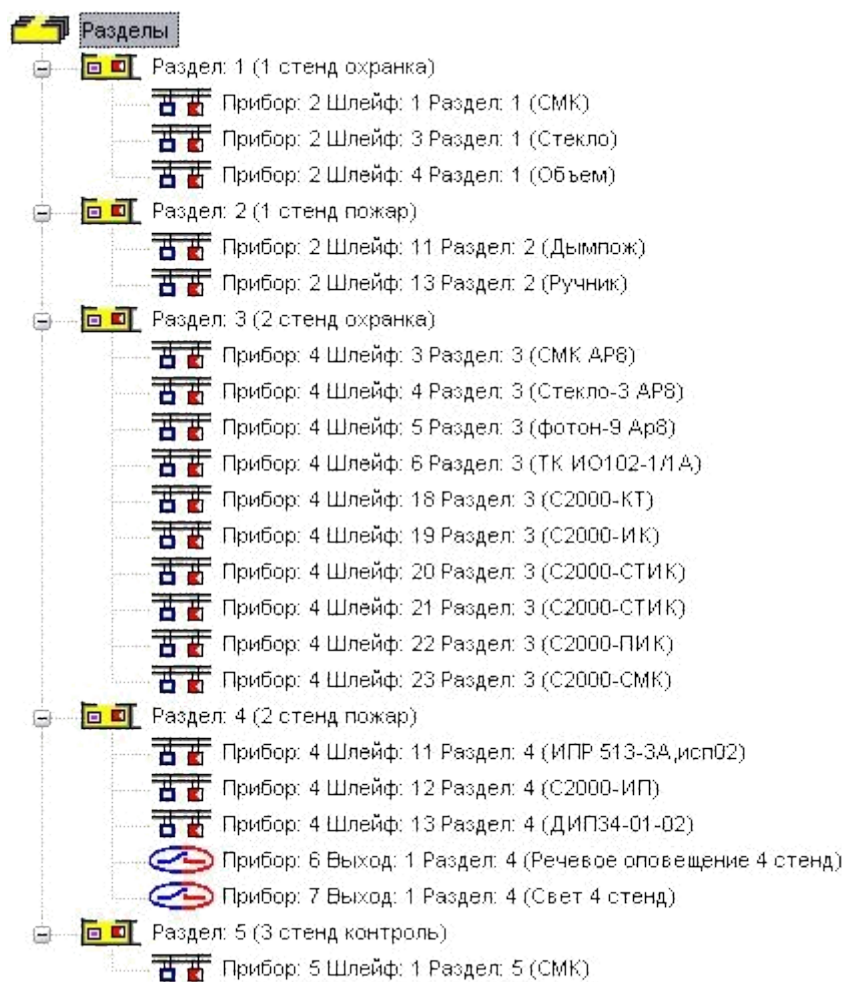



Создаем разделы. Переходим во вкладку «Разделы», нажав , в окне «Приборы (шлейфы)» для каждого из приборов настраиваем шлейфы (обязательно так же как подключено на приборе, это можно узнать визуально, вскрыв прибор и разобравшись в устройстве по инструкции).






Создаем разделы соответственно стендам и привязываем к ним устройства по следующему принципу:

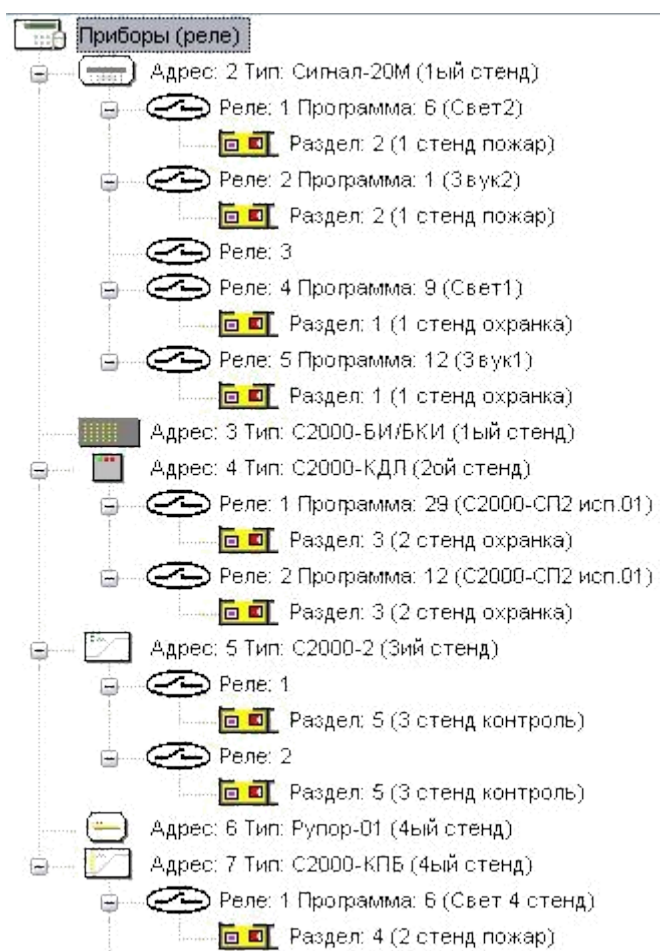




На соседней с ней вкладке «Группы разделов»  создаем новые группы и привязываем к ним перетаскиванием из окна «Разделы» разделы, как показано ниже:

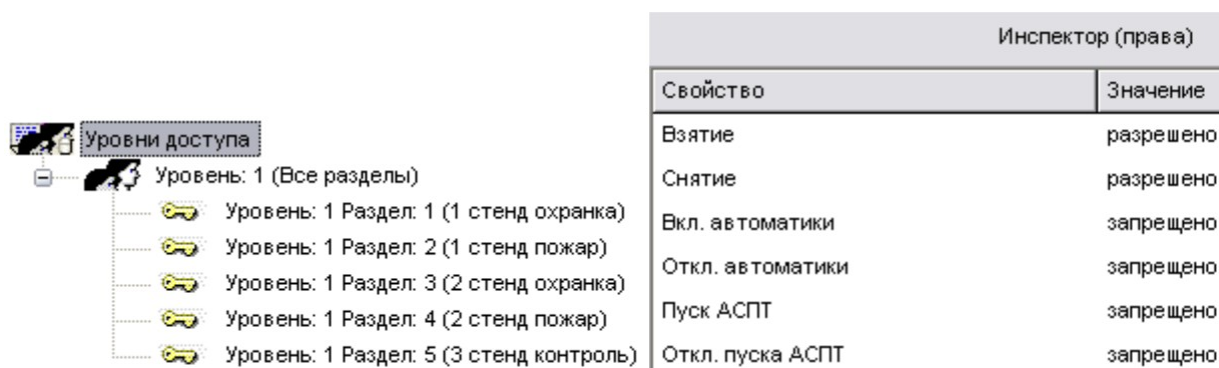





На соседней вкладке «Реле»  в окне «Приборы (реле)» описываем реле, их программы управления и привязываем разделы к реле перетаскиванием их из окна «Разделы», как показано на картинке:




На вкладке «Уровни доступа»  в окне «Уровни доступа» создаем новый уровень доступа (нажав ) , перетаскиванием из окна «Разделы» привязываем к нему все разделы (на картинке ниже слева), в окне «Инспектор (права)» для каждого из радела в окне «Уровни доступа» присваиваем значения свойствам как на картинке ниже справа.




Инспектор (права)	
Свойство	Значение
Взятие	разрешено
Снятие	разрешено
Вкл. автоматики	запрещено
Откл. автоматики	запрещено
Пуск АСПТ	запрещено
Откл. пуска АСПТ	запрещено


На вкладке «Пароли»  настраиваем пароли для доступа к режиму конфигурирования (программирования), режиму управления шлейфами и


создаем новый пароль (нажав ) для снятия всех шлейфов и присваиваем ему ранее созданный уровень доступа.

Пароли					Инспектор (пароль)	
Номер	Тип	Код	Пользователь	Уровень доступа	Свойство	Значение
1	Гл.пароль	123456	Программирование		Номер	3
2	Пароль	1234	Управление шлейф	255 (Упр. ШС. Все функции)	Код	111111
3	Пароль	111111	СНИМАТЕЛЬ	1 (Все разделы)	Пользователь	СНИМАТЕЛЬ
					Уровень доступа	1 (Все разделы)

На вкладке «Входные шлейфы»  шлейф от С2000-2 с СМК перетаскиваем в окно «Входные шлейфы» и меняем его свойства в окне «Инспектор (входная зона)» как показано на рисунках ниже.


Входные шлейфы

 Входные шлейфы
 










 **Прибор: 5 Шлейф: 1**




Инспектор (входная зона)	
Свойство	Значение
Адрес	5
Шлейф	1
Задержка тревоги	1

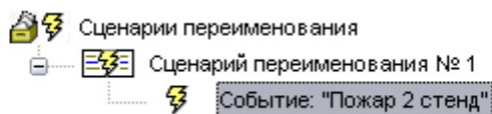
На вкладке «Привязка управления»  привязываем управление 4-ым разделом Рупору и КДЛУ путем перетаскивания раздела из окна «Разделы» в окно «Привязка управления» на соответствующий прибор.

Привязка управления

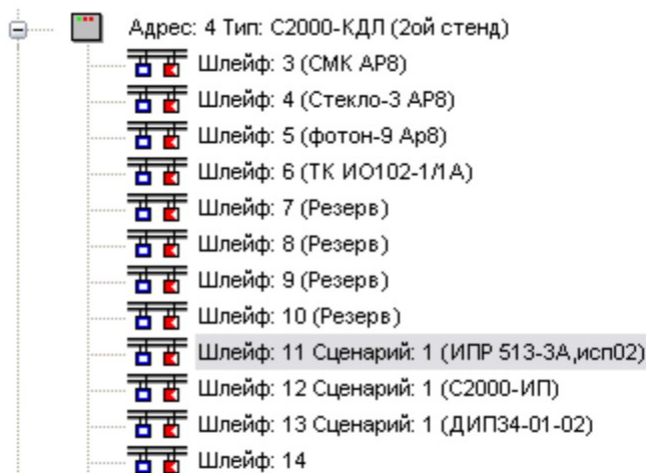
-  Пульт С2000
-  Адрес: 2 Тип: Сигнал-20М (1ый стенд)
-  Адрес: 3 Тип: С2000-БИ/БКИ (1ый стенд)
-  Адрес: 4 Тип: С2000-КДЛ (2ой стенд)
-  Адрес: 5 Тип: С2000-2 (3ий стенд)
-  Адрес: 6 Тип: Рупор-01 (4ый стенд)
-  Раздел: 4 (2 стенд пожар)
-  Адрес: 7 Тип: С2000-КПБ (4ый стенд)
-  Раздел: 4 (2 стенд пожар)




Если мы хотим чтобы на пульте отображалась надписи, которые будут понятны не только нам, но и охране, то на вкладке «Переименование

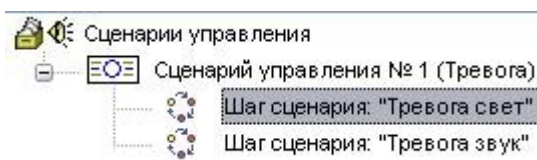
событий»  добавляем новый сценарий () и добавляем событие (). Далее в окне «Инспектор (Событие)» по желанию настраиваем событие и затем в окне «Приборы (шлейфы)» к нужным шлейфам привязываем это событие.



Инспектор (Событие)	
Свойство	Значение
Номер	0
Описание	Пожар 2 стэнд
Базовое соб.	Внимание! Опасность пожара
Группа	Пожары
Формат	Раздел, прибор, шлейф
Звук	сигнал "Пожар"
Тревожность	10




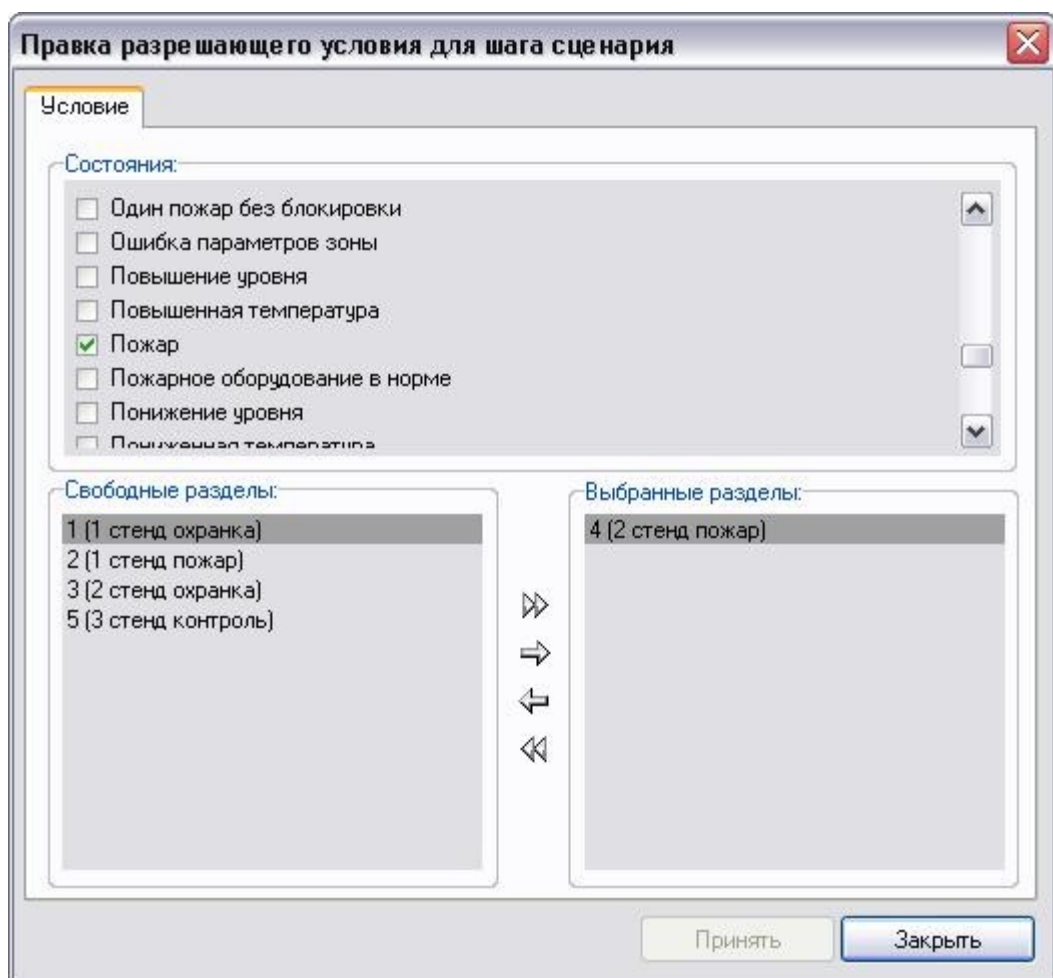
На вкладке «Сценарии управления»  добавляем сценарий () , в него добавляем два шага сценария () и настраиваем их в окне «Инспектор (шаг сценария управления)».



Инспектор (шаг сценария управления)	
Свойство	Значение
Номер	0
Описание	Тревога свет
Программа упр.	6 (мигать из состояния включено)
Маска мигания	34. _**_**_*****
Задержка вкл.	0
Время упр.	30

Свойство	Значение
Номер	1
Описание	Тревога звук
Программа упр.	1 (включить)
Маска мигания	1. *****
Задержка вкл.	0
Время упр.	30

В окне «Состояния и разделы для шага сценария» правим разрешающее условие ()




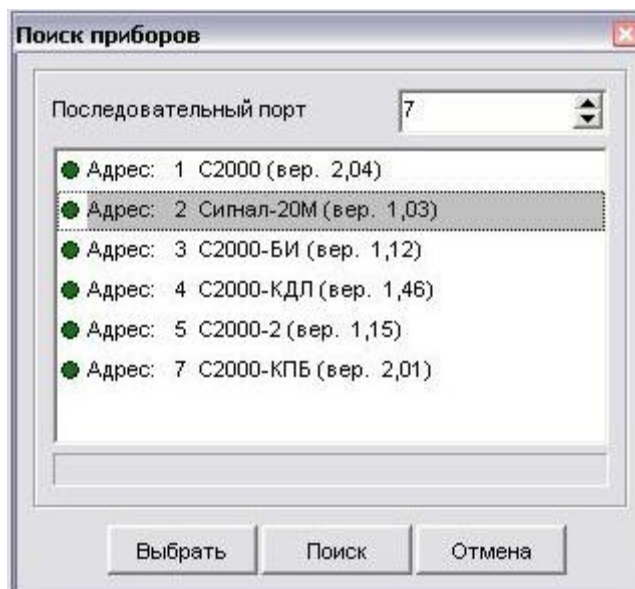
Состояния и разделы для шага сценария	
Разрешающее условие	Запрещающее условие
Пожар Тревога взлома	
4 (2 стенд пожар)	

В пункте меню выбираем С2000 -> Записать конфигурацию. Сохраняем конфигурацию через меню Файл -> Сохранить как..., и прошивка пульта завершена.

## 2. 2 Прошивка Сигнал-20М

Открываем UProg и нажимаем кнопку «Чтение конфигурации из

прибора» . Выбираем Порт 7 (предварительно проверить в диспетчере устройств номер порта), нажимаем поиск и ждем окончания поиска. Далее выбираем нужное нам устройство (в нашем случае это Сигнал-20М).



На 1-ой вкладке (Приборы) снимаем все галочки, пароль не трогаем.



На 2-ой вкладке «Шлейфы» отмечаем, что 1 шлейф – СМК, 3 – Стекло, 4 – Объемник (для всех трех тип ШС – 4 - Охранный шлейф; привязываем управление 4 и 5 реле); 11 – 2 дымовых пожарных, 13 – пожарная сигнальная кнопка (тип ШС – 1 - Дымовой шлейф; привязываем управление 1 и 2 реле). Тип шлейфа выставляется на пересечении «Тип ШС» и номера шлейфа; реле привязывается на пересечении «Управление реле <номер реле>» и номер шлейфа.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Тип ШС	4	4	4	4	4	4	4	4	4	4	1	1	4	4	4	4	4	4	4	4
Задержка перехода в тревогу/пожар, с	5	5	5	5	5	5	5	5	5	5	1 - Дымовой шлейф 2 - Комбинированный шлейф 3 - Тепловой шлейф 4 - Охранный шлейф 5 - Охранный с контролем блокировки 6 - Технологический 7 - Охранный входной 11 - Тревожный 12 - Программируемый технологический									
Задержка взятия, с	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Задержка анализа ШС после сброса, с	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0
Задержка управления реле 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Задержка управления реле 2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Задержка управления реле 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Задержка управления реле 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Задержка управления реле 5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Без права снятия с охраны																				
Автоперевзятие из невзятия	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Автоперевзятие из тревоги																				
Контроль снятого ШС																				
Блокировка перезапроса пож. ШС																				
Интегрирование 300 мс	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Блокировка 10% отклонений охр. ШС																				
Управление реле 1 (ПЦН1)											+	+								
Управление реле 2 (ПЦН2)											+	+								
Управление реле 3 (ПЦН3)																				
Управление реле 4 (Лампа)	+		+	+																
Управление реле 5 (Сирена)	+		+	+																

Реле 1 – 4-ый стенд верхняя табличка выход.

Реле 2 – 4-ый стенд верхняя сирена.

Реле 4 – 1-ый стенд лампа.

Реле 5 – 1-ый стенд сирена.

На вкладке «Выходы» задаем программы управления реле:

- Реле 1 – «6 - Мигать из состояния включено». В штатном состоянии табличка «Выход» горит, при сработке дымовых извещателей или извещателя ручного на 1ом стенде табличка моргает.

- Реле 2 – «1 - Включит (замкнуть)». В штатном состоянии сирена выключена, при сработке дымовых извещателей или кнопки на 1ом стенде сирена издает непрерывный сигнал.
- Реле 4 – «9 - Лампа». Охранные шлейфы не взяты – не горит, в штатном состоянии (когда шлейф взят) лампа горит, при сработке охранной сигнализации на 1ом стенде лампа моргает.
- Реле 5 – «12 - Лампа». В штатном состоянии (когда охранный шлейф или взят, или не взят) сирена выключена, при сработке охранной сигнализации на 1ом стенде – издает звук.

По желанию ставим время управления.

<b>Реле 1</b>	
Программа управления :	6 - Мигать из состояния включено
Время управления, с :	8190,375
События о включении/выключении	<input type="checkbox"/>
<b>Реле 2</b>	
Программа управления :	1 - Включить (замкнуть)
Время управления, с :	8191,875
События о включении/выключении	<input type="checkbox"/>
<b>Реле 3</b>	
Программа управления :	10 - ПЦН
Время управления, с :	8191,875
События о включении/выключении	<input type="checkbox"/>
<b>Реле 4 :</b>	
Программа управления :	9 - Лампа
Время управления, с :	8191,875
Режим контроля :	Контроль на обрыв и КЗ
События о включении/выключении	<input type="checkbox"/>
<b>Реле 5 :</b>	
Программа управления :	12 - Сирена
Время управления, с :	120,000
Режим контроля :	Контроль на обрыв и КЗ
События о включении/выключении	<input type="checkbox"/>

Завершаем прошивку, нажав кнопку «Запись конфигурации в прибор»




. Сохраняем конфигурацию на ПК.



## 2.3 Прошивка С2000-БИ

Открываем UProg и нажимаем кнопку «Чтение конфигурации из

прибора» . Выбираем Порт 7 (предварительно проверить в диспетчере устройств номер порта), нажимаем поиск и ждем окончания поиска. Далее выбираем нужное нам устройство (в нашем случае С2000-БИ).

В PProg открываем заранее сохраненную конфигурацию для пульта С2000М и открываем вкладку раздела (или по памяти). Соответственно разделу заполняем тип индикатора и время звучания сигнализации на пересечении номера индикатора и его свойства.

Тип индикатора	0 - Охранный	
	0 - Охранный	
	1 - Пожарный	
Индикатор №1	2 - Технологический	
	3 - Охранный 2	
Индикатор №2	2	1
Индикатор №3	3	0
Индикатор №4	4	1
Индикатор №5	5	0
Индикатор №6	6	0
Индикатор №7	7	0

Тип индикатора	0 - Охранный	
	Номер раздела	Тип индикатора
Индикатор №1	1	0
Индикатор №2	2	1
Индикатор №3	3	0
Индикатор №4	4	1
Индикатор №5	5	0
Индикатор №6	6	0
Индикатор №7	7	0

Время звучания сигнализации


Завершаем прошивку, нажав кнопку «Запись конфигурации в прибор»




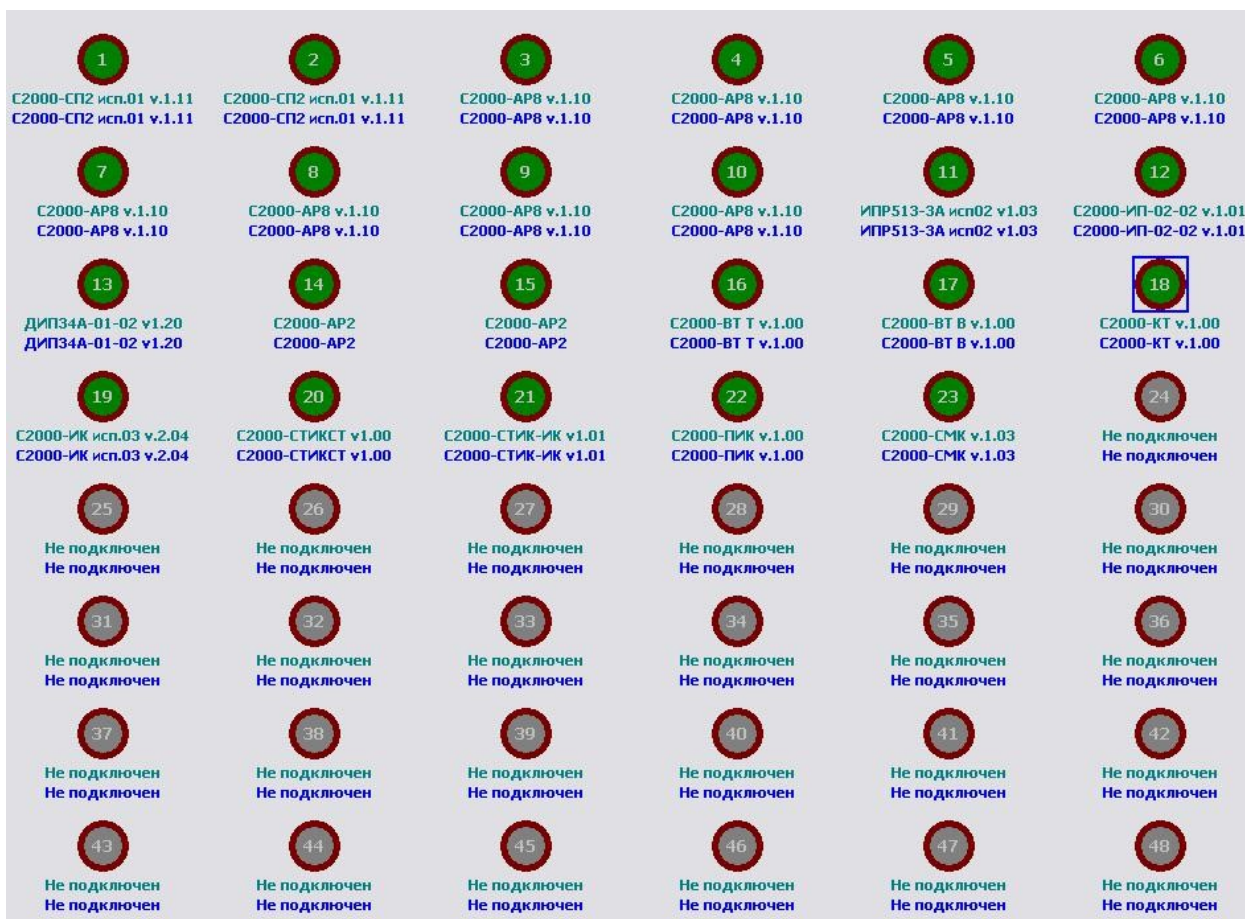
. Сохраняем конфигурацию на ПК.

## 2.4 Прошивка С2000-КДЛ и ее подсистемы

Открываем UProg и нажимаем кнопку «Чтение конфигурации из

прибора» . Выбираем Порт 7 (предварительно проверить в диспетчере устройств номер порта), нажимаем поиск и ждем окончания поиска. Далее выбираем нужное нам устройство (в нашем случае С2000-КДЛ).

На 1-ой вкладке «Тип устройств» можно проверить работоспособность, наличие и название прибора. После нажатия  система автоматически определит тип и адрес прибора (некоторые приборы имеют несколько адресов, например, С2000-ВТ имеет два адреса – один для температуры, один для влажности). На этой же вкладке можно через правую кнопку сменить тип прибора, адрес, проверить тип, состояние АЦП и напряжение на приборе.



1 С2000-СП2 исп.01 v.1.11 С2000-СП2 исп.01 v.1.11	2 С2000-СП2 исп.01 v.1.11 С2000-СП2 исп.01 v.1.11	3 С2000-АР8 v.1.10 С2000-АР8 v.1.10	4 С2000-АР8 v.1.10 С2000-АР8 v.1.10	5 С2000-АР8 v.1.10 С2000-АР8 v.1.10	6 С2000-АР8 v.1.10 С2000-АР8 v.1.10
7 С2000-АР8 v.1.10 С2000-АР8 v.1.10	8 С2000-АР8 v.1.10 С2000-АР8 v.1.10	9 С2000-АР8 v.1.10 С2000-АР8 v.1.10	10 С2000-АР8 v.1.10 С2000-АР8 v.1.10	11 ИПР513-3А исп02 v1.03 ИПР513-3А исп02 v1.03	12 С2000-ИП-02-02 v.1.01 С2000-ИП-02-02 v.1.01
13 ДИП34А-01-02 v1.20 ДИП34А-01-02 v1.20	14 С2000-АР2 С2000-АР2	15 С2000-АР2 С2000-АР2	16 С2000-ВТ Т v.1.00 С2000-ВТ Т v.1.00	17 С2000-ВТ В v.1.00 С2000-ВТ В v.1.00	18 С2000-КТ v.1.00 С2000-КТ v.1.00
19 С2000-ИК исп.03 v.2.04 С2000-ИК исп.03 v.2.04	20 С2000-СТИКСТ v1.00 С2000-СТИКСТ v1.00	21 С2000-СТИК-ИК v1.01 С2000-СТИК-ИК v1.01	22 С2000-ПИК v.1.00 С2000-ПИК v.1.00	23 С2000-СМК v.1.03 С2000-СМК v.1.03	24 Не подключен Не подключен
25 Не подключен Не подключен	26 Не подключен Не подключен	27 Не подключен Не подключен	28 Не подключен Не подключен	29 Не подключен Не подключен	30 Не подключен Не подключен
31 Не подключен Не подключен	32 Не подключен Не подключен	33 Не подключен Не подключен	34 Не подключен Не подключен	35 Не подключен Не подключен	36 Не подключен Не подключен
37 Не подключен Не подключен	38 Не подключен Не подключен	39 Не подключен Не подключен	40 Не подключен Не подключен	41 Не подключен Не подключен	42 Не подключен Не подключен
43 Не подключен Не подключен	44 Не подключен Не подключен	45 Не подключен Не подключен	46 Не подключен Не подключен	47 Не подключен Не подключен	48 Не подключен Не подключен

На вкладке «Зоны» изменить свойства устройства. Тут нас интересует Тип ШС (выставляем для каждого устройства соответствующий), Групповое

снятие/взятие (для удобства помечаем только для задействованных адресов),  
остальные свойства по желанию.

	3	4	5	6	7	8	9	10
Тип ШС	4	4	4	4 - Охранный	3	3	3	3
Автоматическое перезвятие				4 - Охранный шлейф				
Автоперезвятие из тревоги				5 - Охранный с контролем вскрытия корпуса извещателя				
Контроль в снятом состоянии				6 - Технологический				
Без права снятия				7 - Входной				
Групповое снятие/взятие	+	+	+	8 - Дымовой адресно-аналоговый с изменяемыми порогами				
Задержка взятия, с	0	0	0	9 - Тепловой адресно-аналоговый с изменяемыми порогами				
Время восстановления	0	0	0	10 - Тепловой термостатический				
Время задержки перехода в тревогу	0	0	0	11 - Тревожный				
Дневной порог пожара	100	100	100	13 - Счетный				
Дневной порог внимание	80	80	80	15 - Влагоизмерительный				
Ночной порог пожара	90	90	90					
Ночной порог внимание	70	70	70					
Порог запыленности	40	40	40					
Температура 'Пожар'	54	54	54					
Температура 'Внимание'	50	50	50					
Порог понижения температуры	20	20	20					
Порог повышения температуры	22	22	22					
Управление индикацией АУ	1	1	1					
Экономичный режим	+							
Счетный порог	1000	1000	1000					
Время интегрирования счетчика, мс	1	1	1					
Порог повышения влажности	70	70	70					

11	12	13	14	15	16	17	18	19	20	21	22	23
3	9	8	3	3	10	15	4	5	5	5	5	5
+	+	+	+	+	+	+	+	+	+	+	+	+
0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0
100	100	100	100	100	100	100	100	100	100	100	100	100
80	80	80	80	80	80	80	80	80	80	80	80	80
90	90	90	90	90	90	90	90	90	90	90	90	90
70	70	70	70	70	70	70	70	70	70	70	70	70
40	40	40	40	40	40	40	40	40	40	40	40	40
54	56	54	54	54	54	54	54	54	54	54	54	54
50	29	50	50	50	50	50	50	50	50	50	50	50
20	20	20	20	20	15	20	20	20	20	20	20	20
22	22	22	22	22	33	22	22	22	22	22	22	22
1	1	1	1	1	1	1	1	1	1	1	1	1
					+	+						
1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
1	1	1	1	1	1	1	1	1	1	1	1	1
70	70	70	70	70	70	80	70	70	70	70	70	70

На вкладке «Выходы» к устройству можно привязать управление реле (нижняя часть окна) и задать сами программы управления и другие свойства (верхняя часть окна). Для привязки устройства к реле выбираем реле в

верхней части и в нижней части плюсами отмечаем устройства. Для 1-го реле (свет) задаем программу управления 29 Включить при взятии; для 2-го реле (звук) – 12 Сирена. Остальные свойства настраиваем по желанию.

	1	2
Номер программы управления	29	12
Время управления реле	10	5
Задержка управлением	0	0
Алгоритм работы по 'ИЛИ'/И'	и	и
Порог повышения температуры	29	29
Порог понижения температуры	20	20
Порог повышения влажности	70	78
Порог понижения влажности	50	50
Сообщать об изменении состояния исполнительных выходов	Да	Да

Привязка зон к реле 1 - [С2000-СП2 исп.01 v.1.11] :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		+	+	+	+												+	+	+	+	+	+

Остальные вкладки не трогаем. Завершаем прошивку, нажав кнопку

«Запись конфигурации в прибор» . Сохраняем конфигурацию на ПК.

### Оформление отчета:

Отчет по работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

### Отчет должен содержать:

1. Название, цели и задачи работы;

2. Скриншоты о проделанной работе;
3. Заключение и выводы.

**Контрольные вопросы:**

1. Какие задачи решает Система оповещения?
2. Дайте определение оповещателя?
3. Перечислите исполнительные устройства системы охраны?
4. Из каких основных устройств состоит Система оповещения?

**Лабораторная работа №7**

**Тема: Определение угла обзора видеокамеры**

**Цель:** научиться определять горизонтальный угол обзора видеокамеры.

**Теория**

Одним из важных параметров, которые необходимо брать во внимание перед расстановкой камер видеонаблюдения, является угол обзора объектива. От этой величины напрямую зависит то, какая площадь наблюдаемого участка попадет в поле зрения камеры. Например, для получения общего обзора участка или тесного помещения необходимо выбирать камеры с широким углом обзора, а при необходимости сосредоточения на каком-либо определенном объекте – с узким.

Расстояние от фокуса до линзы (системы линз) называется **фокусным расстоянием (ФР)**.

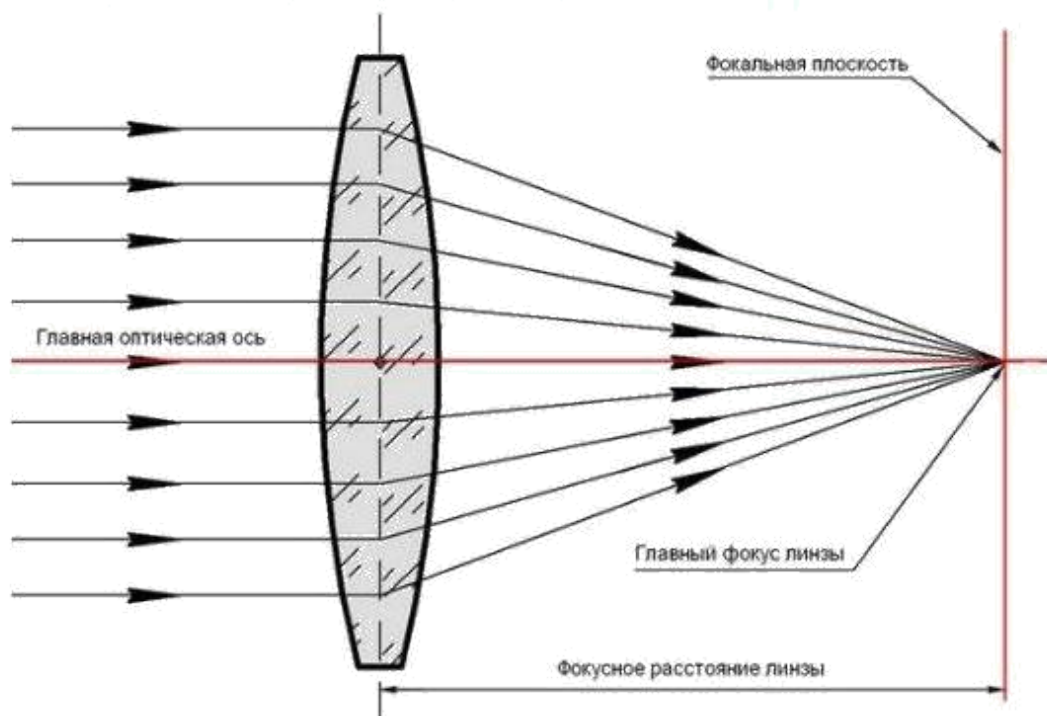


Рисунок 7.1 – Основные параметры, составляющие свойства линзы

Понятия «фокусное расстояние» и «угол обзора» очень тесно связаны между собой. Существует определенная линейка объективов, построенная именно на основе углов обзора и фокусных расстояний. Этот диапазон выглядит приблизительно так: от 2,8 до – до 50 мм.

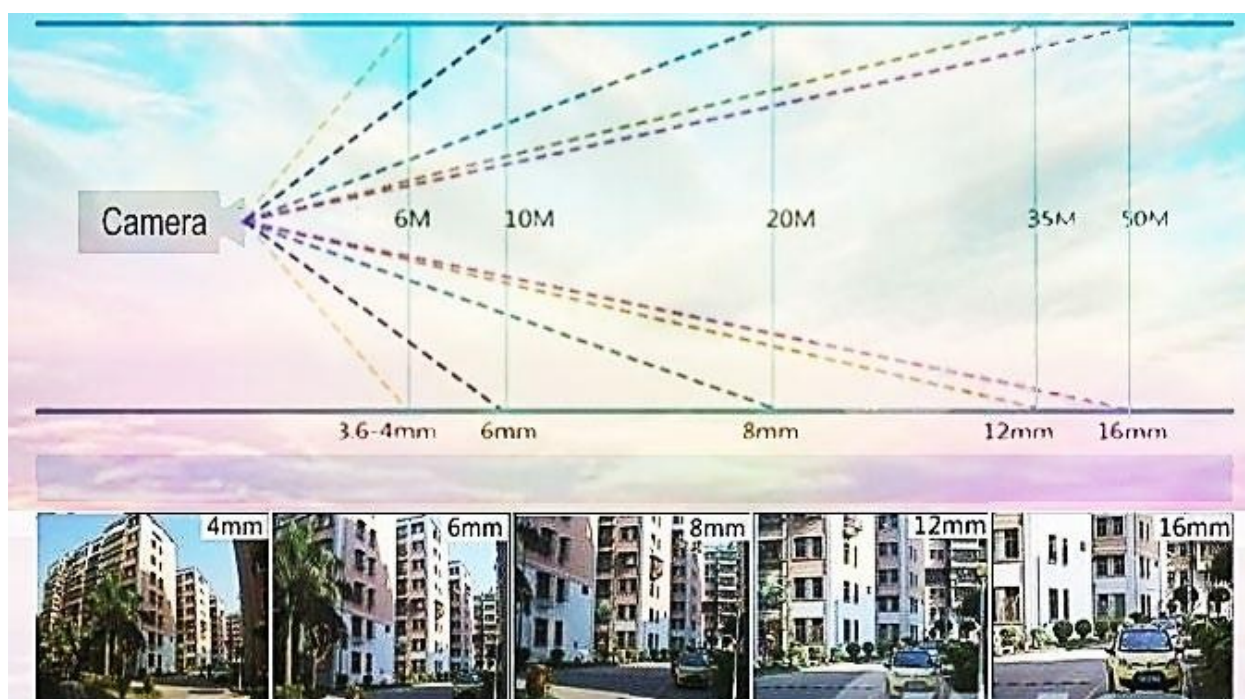


Рисунок 7.2 – Зависимость углов обзора и фокусных расстояний

Чем меньше фокусное расстояние объектива, тем больше (шире) угол обзора. На практике это означает следующее — если вы хотите видеть на мониторе, например, лицо человека, то вам понадобится максимальный угол обзора, а это означает, что нужно выбрать минимально возможное фокусное расстояние на объективе. Для наблюдения за периметром объекта потребуются видеокамеры с максимальным ФР.

Угол обзора объектива зависит от двух определяющих его параметров: фокусное расстояние, которое имеет объектив; размер чувствительного элемента (матрицы). Следует запомнить, что чем большим ФР обладает объектив, тем меньшим будет угол его обзора, поэтому длиннофокусные объективы обладают возможностью наблюдения за относительно удаленными от камеры объектами, а широкоугольные позволяют охватить большую площадь территории или помещения. Зависимость угла обзора камеры видеонаблюдения от физического размера матрицы также имеет место быть. Так, чем больше размер матрицы, тем большим будет угол обзора, например: Матрица, диагональ которой составляет  $\frac{1}{4}$  будет иметь угол обзора  $64^\circ$  при фокусном расстоянии 2,8; при этом матрица с диагональю  $\frac{1}{2}$  будет иметь угол обзора  $96^\circ$ . Данные расчеты справедливы для обозначения горизонтального угла обзора, для поиска вертикального угла необходимо брать в расчет соотношение вертикальных и горизонтальных сторон матрицы.

### **Порядок выполнения работы**

1. Расположить измеряемый объект перед видеокамерой, так, чтобы его горизонтальный размер занимал всю ширину на экране монитора, согласно схемы 7.3.

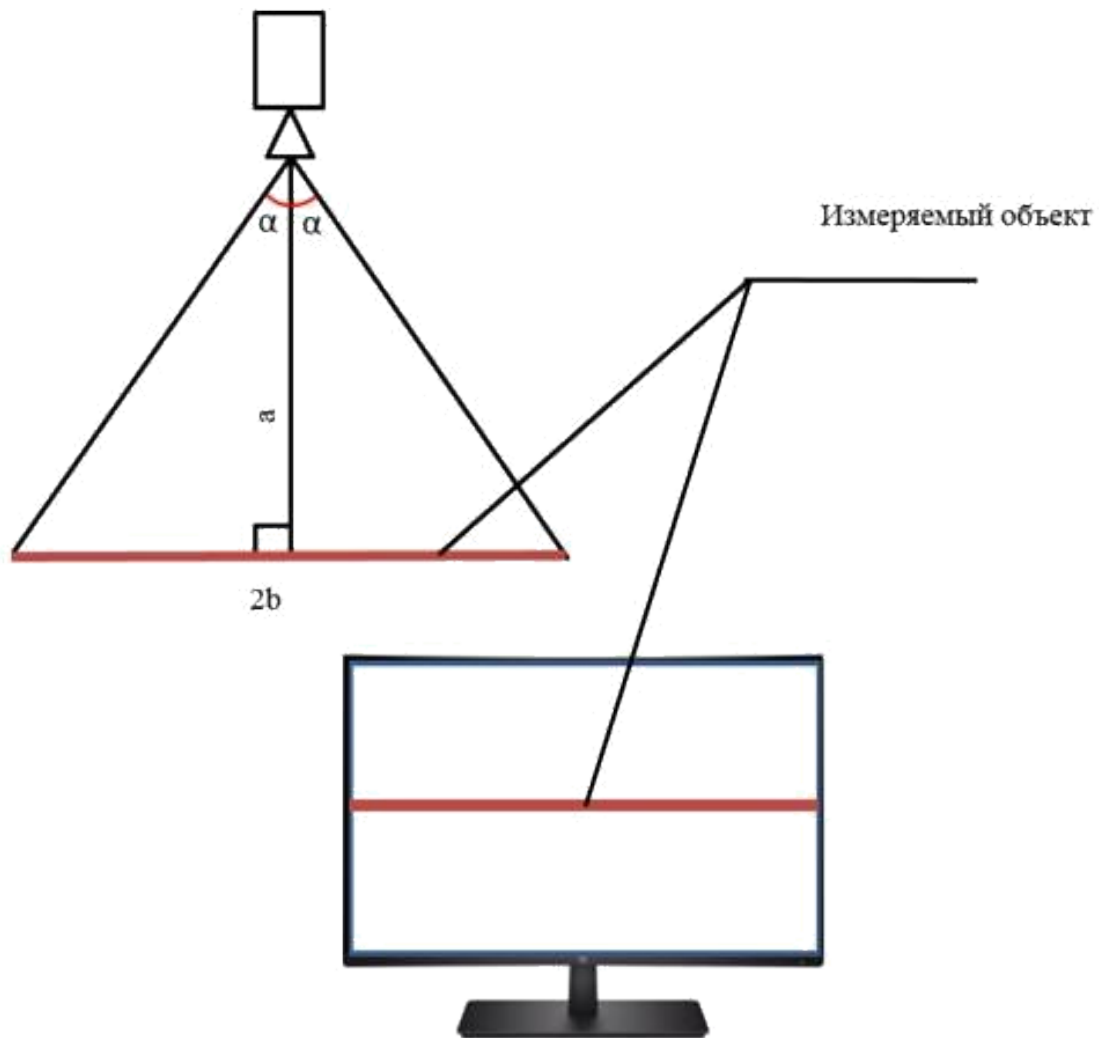


Рисунок 7.3 – 1. Схема расположения измеряемого объект перед видеокамерой

2. Измерить расстояние ( $a$ ) до объекта.
3. Измерить горизонтальный размер объекта ( $2b$ ).
4. Рассчитать угол  $\alpha$ , используя тригонометрическое выражение:

$$\operatorname{tg} = \frac{b}{a} \quad (7.1)$$

5. Определить горизонтальный угол обзора видеокамеры.

### Задание

- 1) Используя формулу (7.1) определить горизонтальный угол обзора видеокамеры.
- 2) Ответить на вопросы.

### Оформление отчета:



Отчет по работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в отпечатанном виде на листах формата А4.

**Отчет должен содержать:**

1. Название, цели и задачи работы;
2. Скриншоты о проделанной работе;
3. Заключение и выводы.

**Контрольные вопросы:**

1. Что представляет собой фокусное расстояние объектива видеокамеры?
2. От каких параметров зависит угол обзора?
3. Какой угол обзора выбрать для видеонаблюдения за большой территорией без необходимости выделения конкретного объекта?
4. Каким должен быть размер наблюдаемой зоны для уверенного распознавания объекта на расстоянии 12 метров?

**ЛИТЕРАТУРА**

1. Владо Дамьяновски ССТV. Библия видеонаблюдения. Цифровые и сетевые технологии/Пер, с англ. - М.: ООО «Ай-Эс-Эс Пресс», 2006, — 480 с: ил.
2. Р 78.36.002-2010. Рекомендации: Выбор и применение систем охранных телевизионных. - М.: ФГУ НИЦ «Охрана» МВД России, 2010, - 183 с.

**Лабораторная работа №8**

**Тема: «Исследование светового индикатора состояния извещателя охранного в составе охранного шлейфа сигнализации ПКПОП**

**Сигнал20М»**

**Цель работы:** определить количество возможных световых индикаторов состояния извещателя охранного при последовательном подключении в шлейфе сигнализации.

Световой индикатор состояния извещателя охранного (СИОСИО) это устройство, показывающее состояние герметизированного контакта путём световой индикации. Известен герметизированный контакт, содержащий контактные пластины, расположенные в запаянной стеклянной колбе, наполненной инертным газом, насаженную на колбу Рис. 1.



Однако визуальный контроль состояния данного герметизированного контакта невозможен в виду его конструктивных особенностей – малых размеров и слабой прозрачности колбы. Поэтому совместно с работой герметизированного контакта в составе извещателей охранных магнитно-контактных (ИОМК) в качестве визуального контроля состояния ИОМК используем СИОСИО. Внешний вид СИОСИО представлен на рис. 2, который включает в себя красный светодиод 1, коробку соединительную 2 и зелёный светодиод 3. Совместно с магнитно-контактным датчиком он применяется в шлейфах сигнализации в качестве индикатора положения окон или дверей.

В положении закрытого окна (или двери) включается зелёный светодиод, тем самым указывая на то, что магнитно-контактный извещатель замкнут, следовательно, появляется возможность постановки защищаемого помещения под охрану. При открытом положении (не до конца закрытом/ при неисправности магнитно-контактного извещателя) окна (двери) светится красный светодиод, сигнализируя о том, что требуется, сперва, устранить

данное нарушение и только после этого появится возможность постановки охранной системы на сигнализацию.



Рисунок 2 - Световой индикатор отображения состояния извещателя охранного магнитно-контактного в двух режимах работы

Рассмотрим работу СМК совместно с СИОСИО в шлейфе сигнализации прибора «Сигнал 20М» в составе системы BOLID и определим количество возможных световых индикаторов при последовательном подключении. Будем считать, что реализованы условия, приближенные к реальным, при которых шлейф имеет максимально возможную длину 4 км, соответствующую сопротивлению равному 1 кОм. При последовательном подключении СИОСИО наблюдаем следующие показания СМК при замкнутом и разомкнутом состоянии, которые вносим в таблицу 1.

Для тестирования устройств СИОСИО использовалась схема последовательного соединения, показанная на рисунке 2.

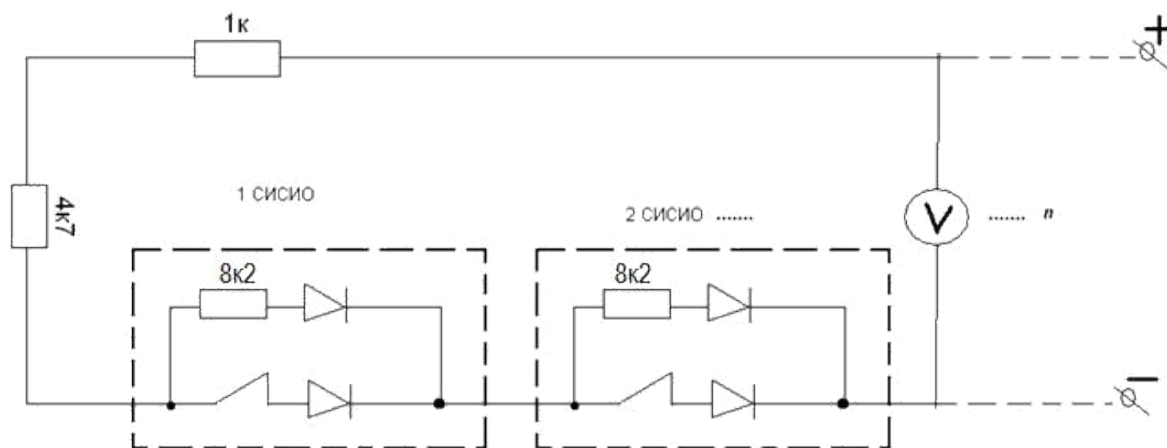


Рисунок 1 – Схема последовательного соединения СИОСИО

Для настройки работы системы BOLID через пульт Орион С2000М

нам необходимо провести следующие действия:

- Нажимаем кнопку Ent (в нашем случае без пароля)
- Затем 5 и 2 (на этом этапе пульт запрашивает у нас АДРЕС вводим 2 и нажимаем Ent)
- И последнее у нас просят указать номер ШС (в нашем случае вводим 5 и нажимаем Ent)

Начальное значение напряжения в шлейфе сигнализации составляет  $U_{xx}=27В$ . Вывод о работоспособности делался на основании успешного взятия шлейфа под охрану и получения сигнала тревоги при размыкании СМК.

Таблица 1 – Результаты измерений

Количество замкнутых СМК	Количество устройств, шт	Сопротивление ШС, кОм	Напряжение, В	Индикация светодиодов	Вывод о работоспособности
0	1				
1	1				
0	2				
1	2				
2	2				
0	3				

1	3				
2	3				
3	3				
0	4				
1	4				
2	4				
3	4				
4	4				
0	5				
1	5				
2	5				
3	5				
4	5				
5	5				
0	6				
1	6				
2	6				
3	6				
4	6				
5	6				
6	6				
0	7				
1	7				
2	7				
3	7				
4	7				
5	7				
6	7				
7	7				

Заметим, что максимальным значением сопротивления является \_\_\_\_ кОм, а минимальным \_\_\_\_ кОм. На рисунке 4 представлена графическая иллюстрация состояний работы устройств в зависимости от их количества с учётом граничных параметров.

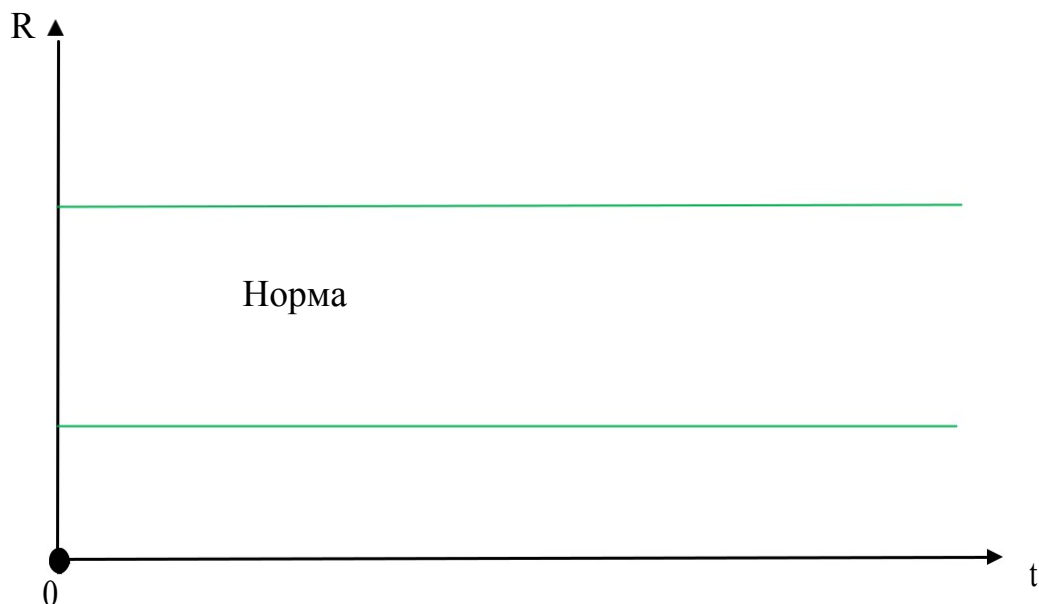


Рисунок 4 – Иллюстрация состояний работы устройств с количеством световых индикаторов

**Сделайте вывод:** в ходе эксперимента было установлено, что максимальное количество последовательно подключенных световых индикаторов равно \_\_\_\_\_ шт. Рекомендуется использовать не более \_\_\_\_\_ устройств в одном шлейфе. Данное предложение подходит для решения защиты входных зон и отдельных помещений.

**Отчет должен содержать:**

1. Название, цели и задачи работы;
2. Скриншоты о проделанной работе;
3. Заключение и выводы.

**Контрольные вопросы:**

1. Перечислите задачи, решаемые системой охраны.
2. Какова максимальная нагрузка (мА) в охранном шлейфе сигнализации Сигнал 20М?
3. Что является шлейфом сигнализации?
4. Возможно ли увеличить количество последовательно подключенных световых индикаторов?

## Лабораторная работа №9

**Тема: Настройка передачи тревожных извещений на базе контроллера охранно-пожарного «Приток-А-КОП-02»**

**Цель:** научиться настраивать передачу тревожных извещений с помощью контроллера охранно-пожарного «Приток-А-КОП-02»

### Теория

Контроллер «Приток-А-КОП-02» предназначен для работы с автоматизированным рабочим местом пультом централизованного наблюдения (АРМ ПЦН) через сеть Интернет или VLAN (например, по технологии GPON) и (или) оператора сотовой связи (например, по технологии GSM/GPRS). Каналы связи с сервером подключений - двунаправленные, с шифрованием и защитой от подмены контроллера. Контроллер, совместно с MPLU-02, предназначен для организации централизованной охраны объектов по TCP/IP совместимым каналам связи с возможностью подключения 8 шлейфов сигнализации (4 шлейфа обслуживаются контроллером, 4 шлейфа - MPLU-02) и индикации состояния шлейфов на передней панели контроллера. Связь контроллера и MPLU-02 осуществляется по линии связи RS-485. Взятие под охрану и снятие с охраны осуществляется посредством применения персональных кодов идентификации - ключей Touch Memoгу. Контроллер оборудован GSM-антенной. Более подробную информацию о контроллере можно получить в руководстве по эксплуатации. На рисунке приведён внешний вид лабораторного стенда.



**Контроллер охранно-пожарный  
- Приток-А-КОП-02 -**

ОХРАННОЕ БЮРО  
**СОКРАТ**



АРМ ПЦН    АРМ Ядро    Серверы подключений (1) (2)

Сеть GSM    Сеть TCP/IP (Internet) (GPRS)

Ethernet

шина расширения RS-485

модули клавиатуры, релейного расширителя, адресных датчиков, ППК01 011-8-1-05

шлейфы сигнализации 1 2 3 4

Приток МРШ-02(4шл)

**Модуль расширения шлейфов  
Приток-МРШ-02(4шл)**

- Связь с Притоком-А-КОП-02
- Шина расширения RS-485
- 4 шлейфа сигнализации
- Габаритные размеры - 80x55x25
- Диапазон питающего напряжения - 10В - 14В



Схема подключения платочного контроллера

ШС

Дымоуловитель

Теплоуловитель

R<sup>1</sup> = 1 кОм для кнопок с выходной цепью "сухой контакт"

R<sup>2</sup> = 0 для кнопок с которыми напряжение на сработавшем больше 5В

R<sup>1</sup> = 4,7 кОм, R<sup>2</sup> = 5,6 кОм

**Приток-А-КОП-02**

- Связь с ПЦН - Ethernet, GSM
- Режим связи по GSM - GPRS, SMS
- 4 шлейфа сигнализации
- 4 выхода для подключения световых и звуковых оповещателей
- Шина расширения RS-485
- Встроенная клавиатура
- Габаритные размеры
- Диапазон питающего напряжения - 10В - 14В



Стенд №31

Вых1 Вых2 Вых3 Вых4 Вых5 Питание

Общая Земля

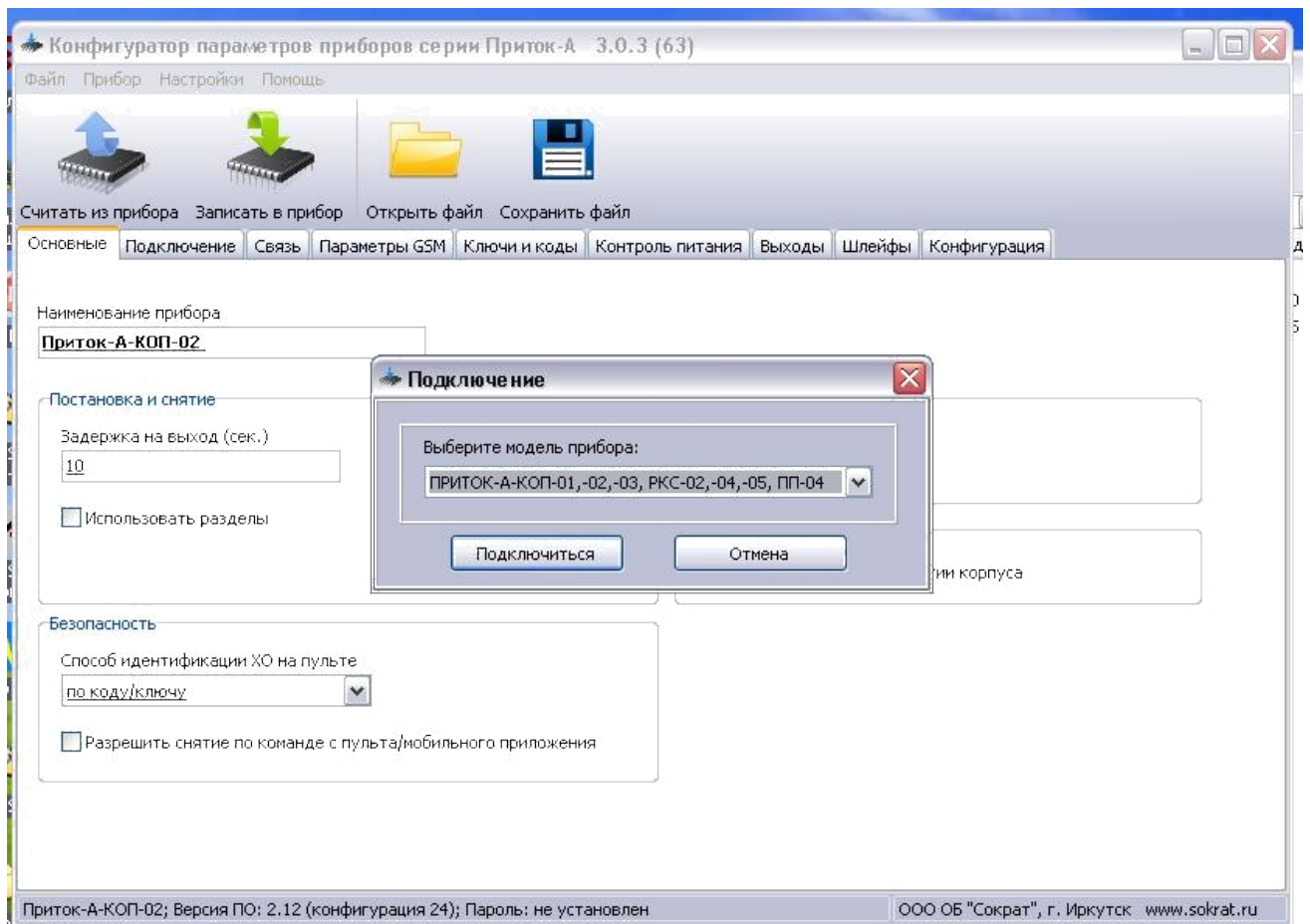
### Порядок работы:

1. Подключаем к свитчу интернет и от стенда LAN, соединяем свитч и компьютер между собой.

Для настройки Контроллера охранно-пожарного-Приток-А-КОП-02 необходимо загрузить требуемое ПО – «UniProg 3.0.3», «Приток-А 3.7» с сайта [www.sokrat.ru](http://www.sokrat.ru): → Загрузка ПО → Утилиты → Скачать конфигуратор параметров UniProg. После установки драйверов необходимо запустить программу «Конфигуратор параметров приборов серии Приток-А». Для программирования Притока нужно подключить mini-USB к ПК.

Вся настройка производится в программе UniProg 3.0.3. Запускаем программу под именем администратора. В программе нажимаем кнопку «Считать из прибора», в появившемся окне выбрать из списка «ПРИТОК-А-КОП-02, РКС-02, КОП-01, РКС-04» и нажать «Подключиться к прибору».

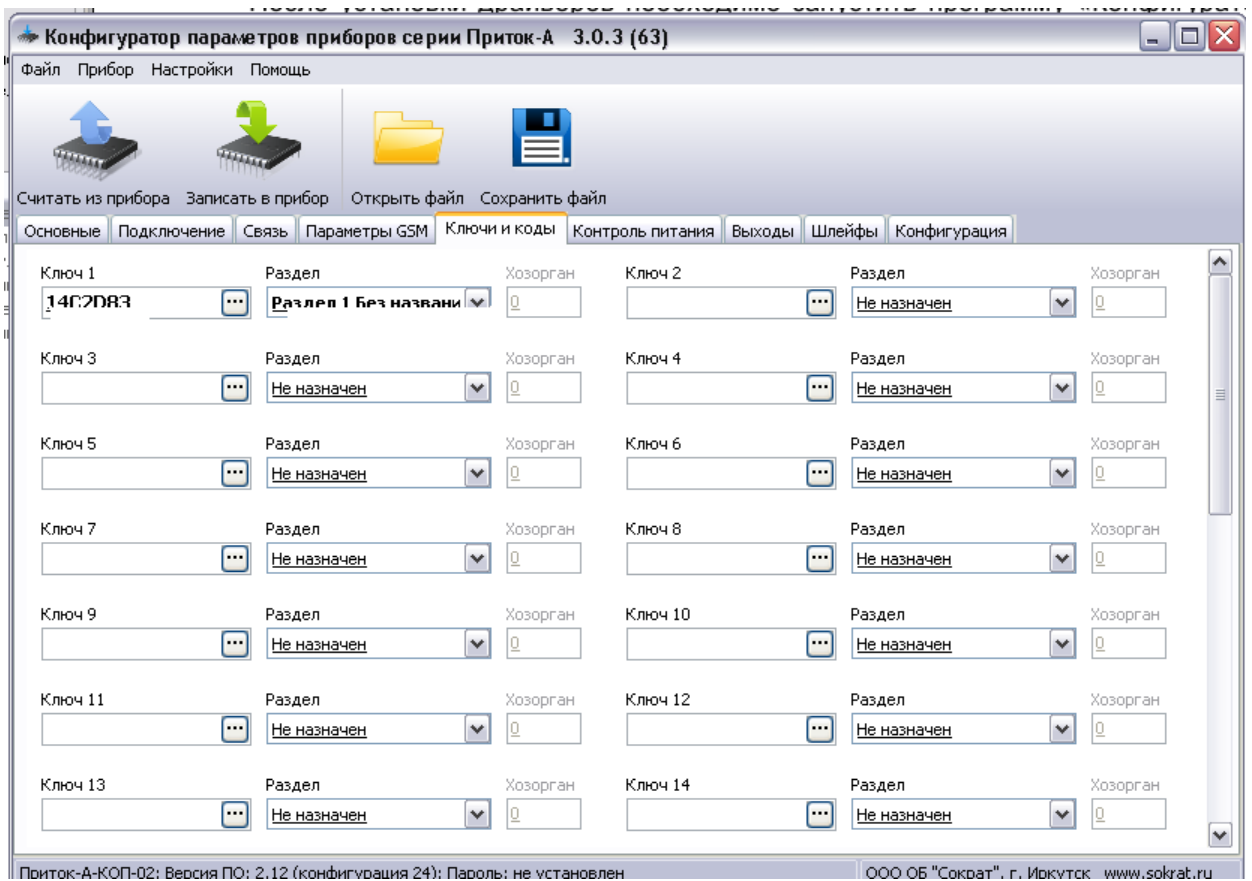




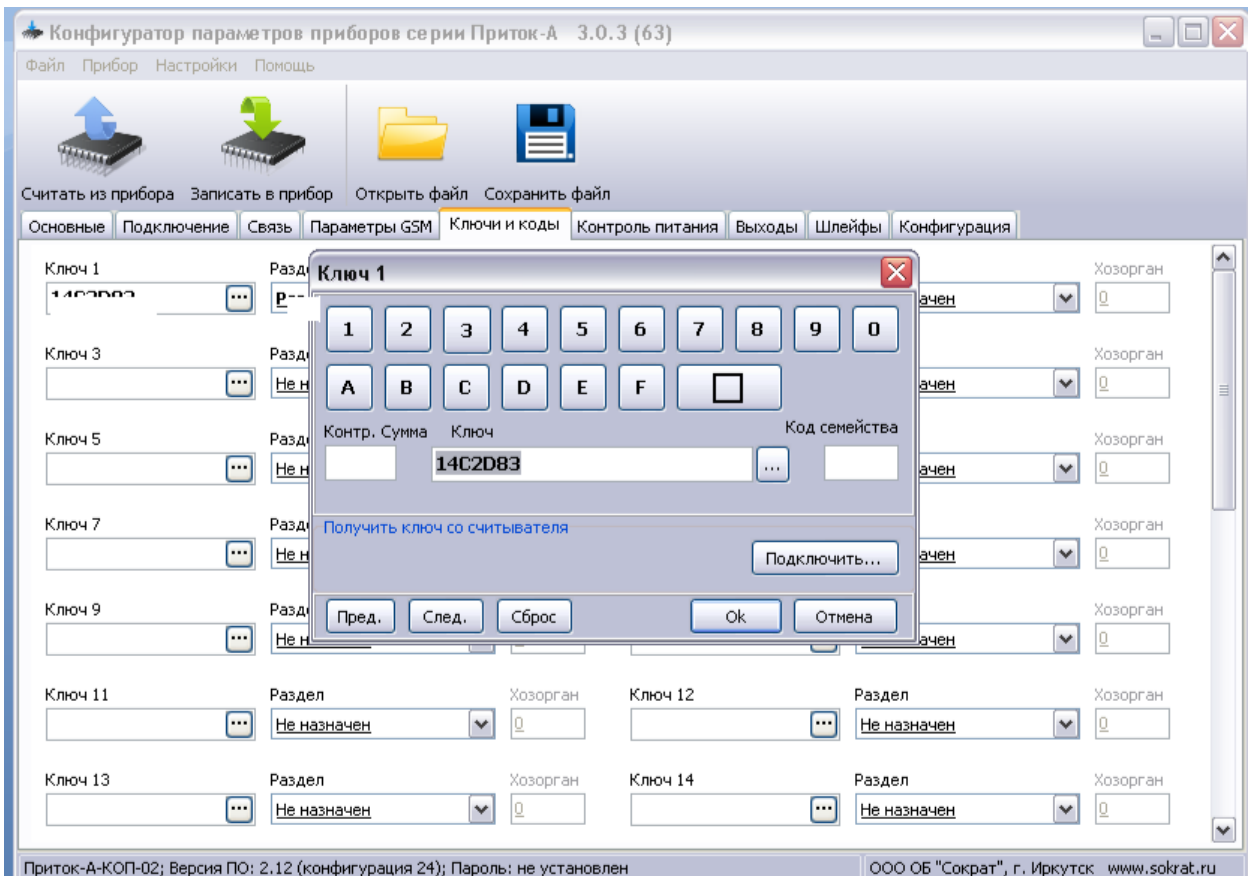
По умолчанию программа настроена на чтение настроек и после подключения заполнит поля ввода текущими настройками контроллера.

Во вкладке «Основные» окно «Наименование прибора» вводим наименование – Приток-А-КОП-02.

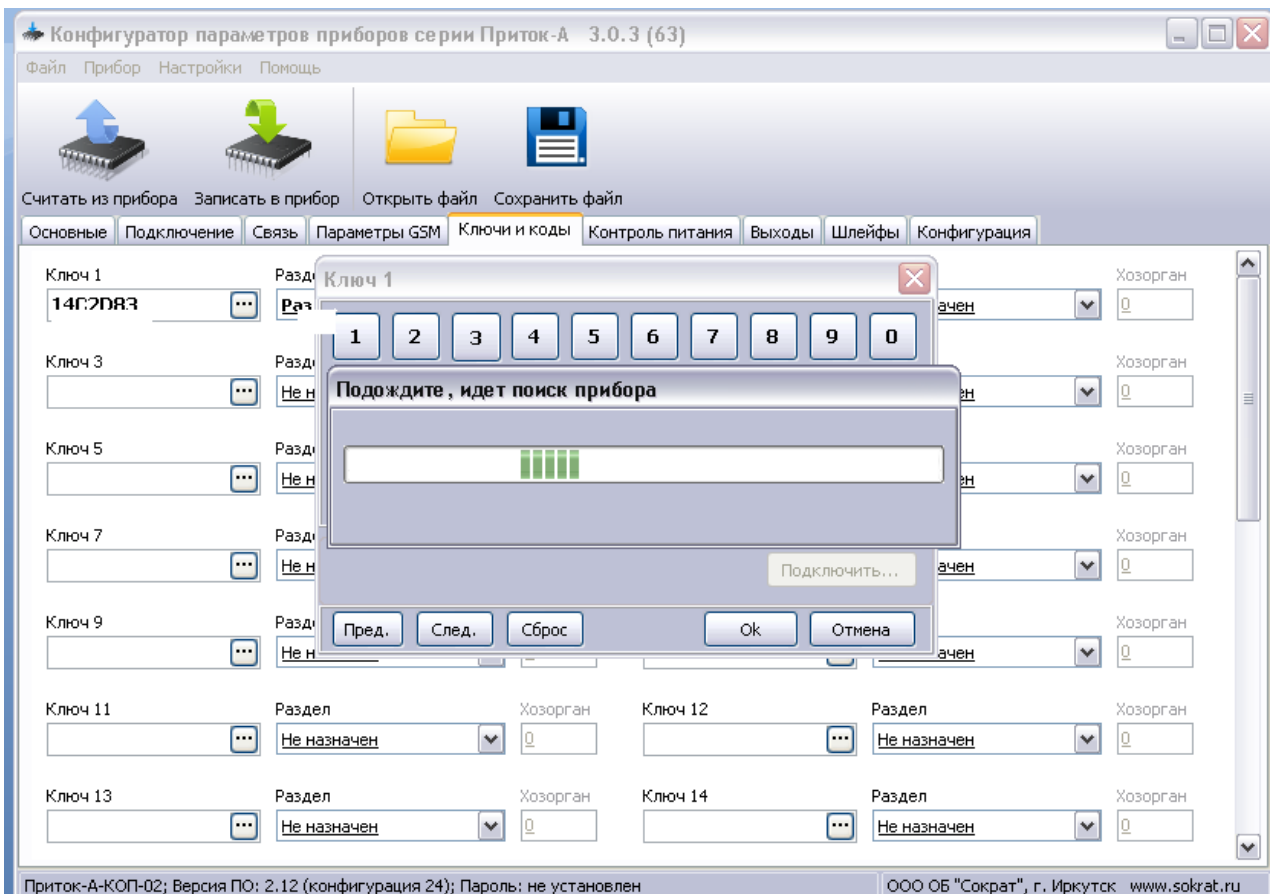
Переходим во вкладку «Ключи и коды» в окне «Ключ 1» кликаем на значок троееточия.



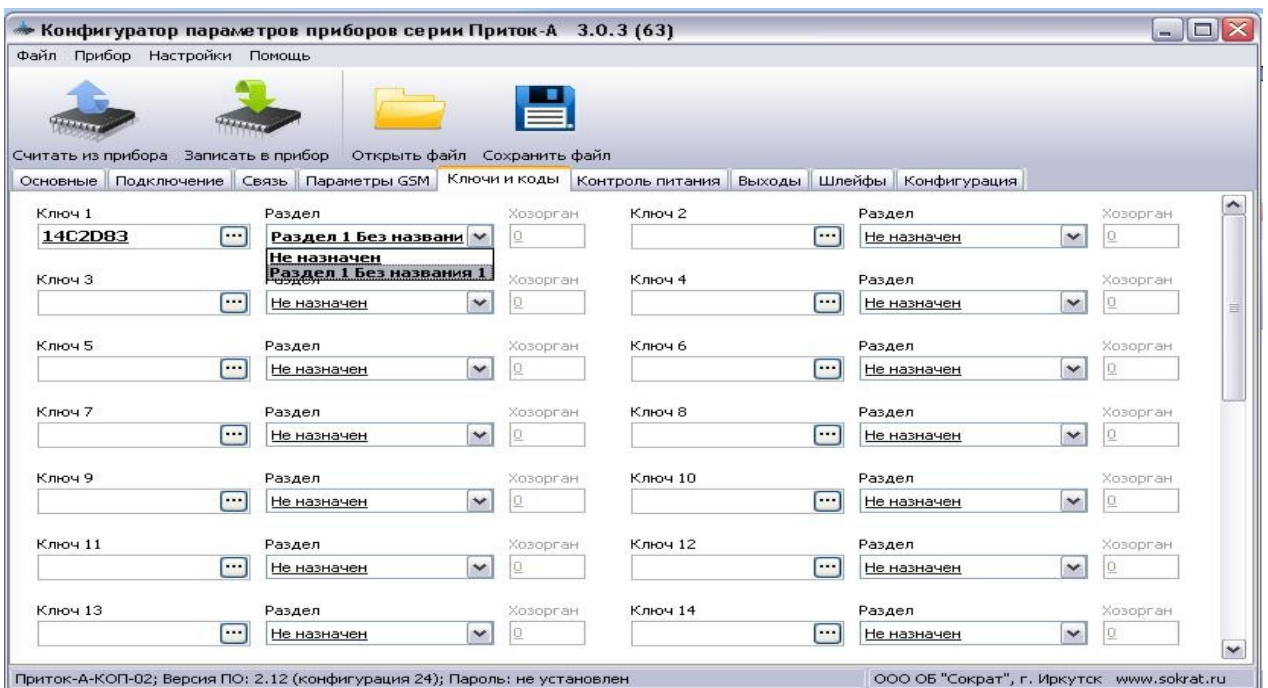
Появляется окно «Ключ 1», кликаем на кнопку «Подключить...»



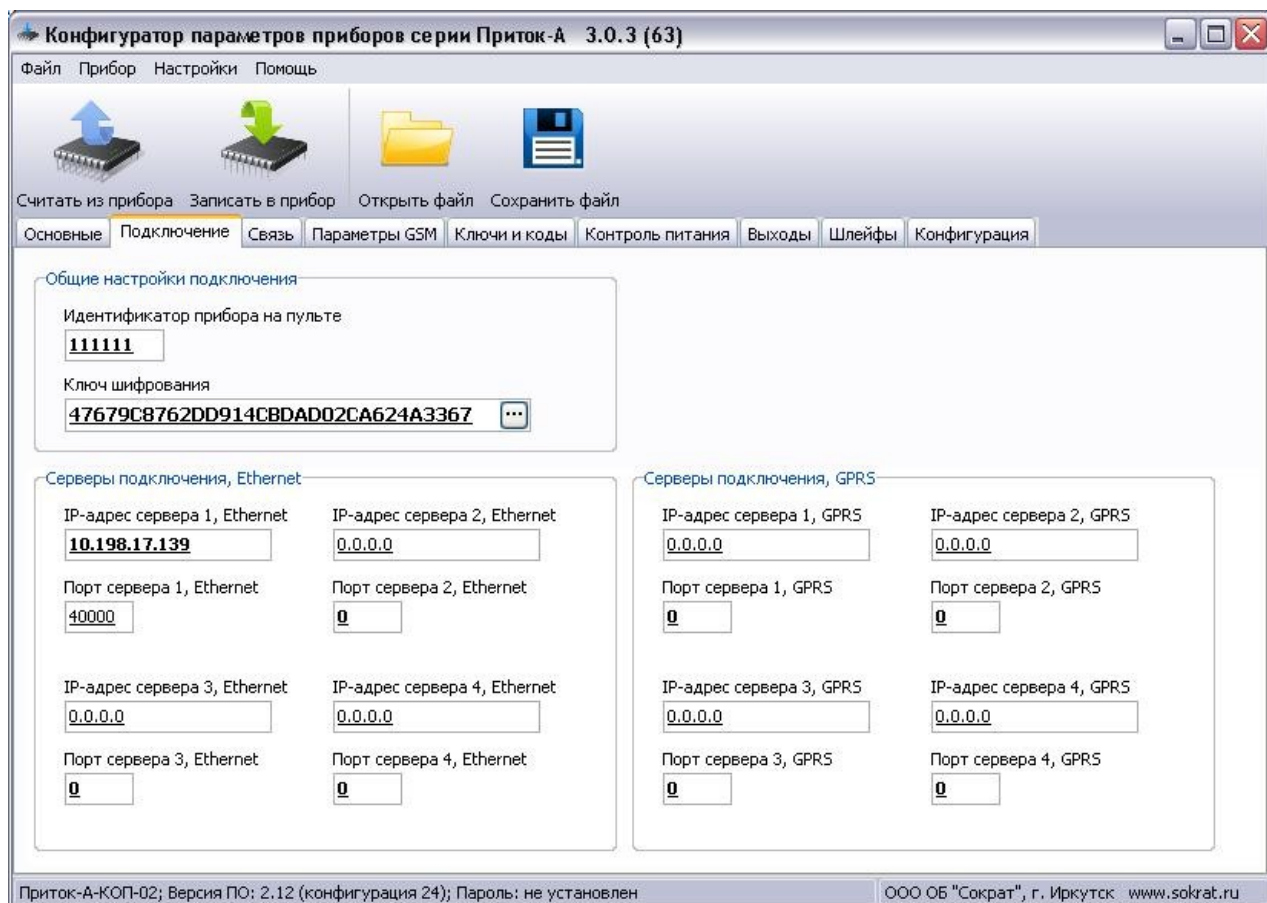
При поиске прибора прикладываем iButton, нажимаем ОК.



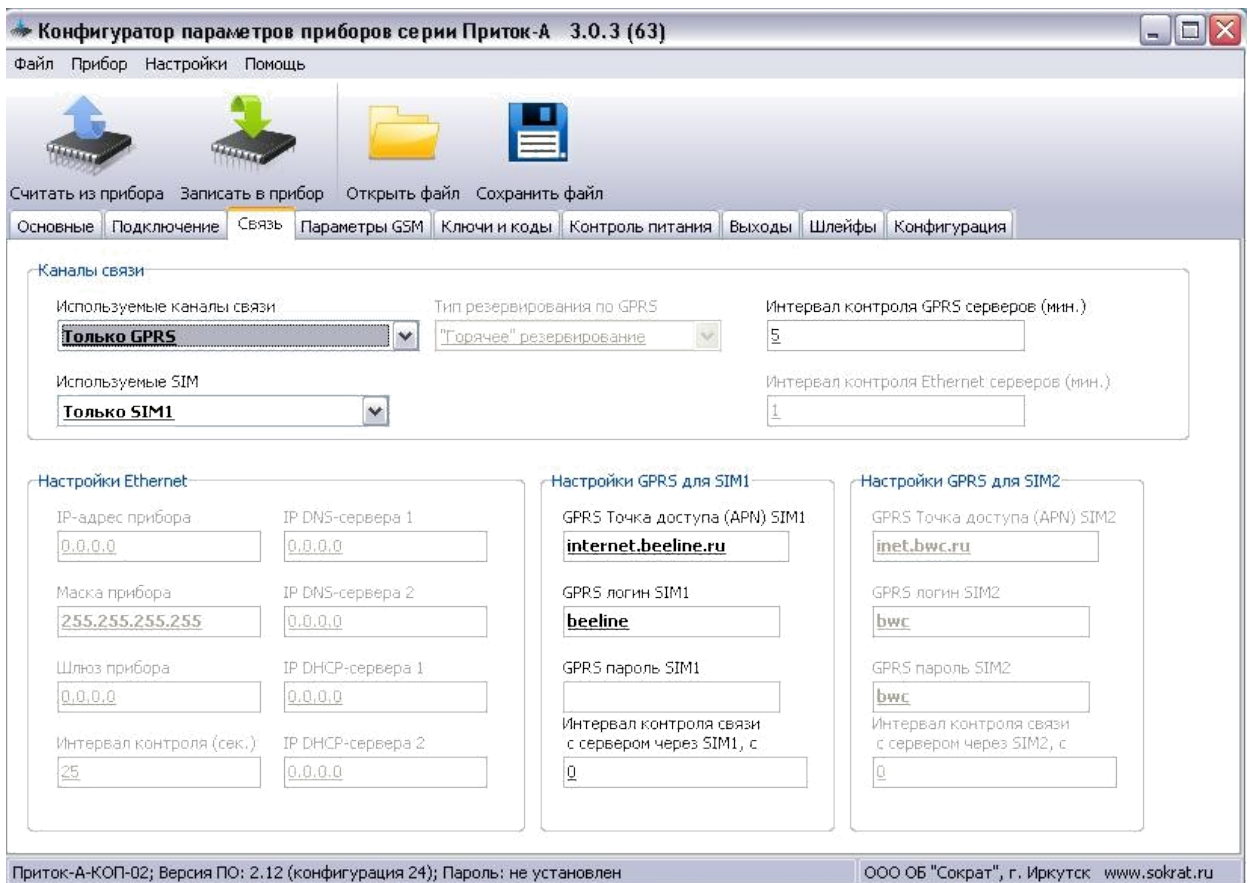
Далее в окне «Раздел» кликаем на стрелку вниз и выбираем из списка пункт «Раздел 1 Без названия».



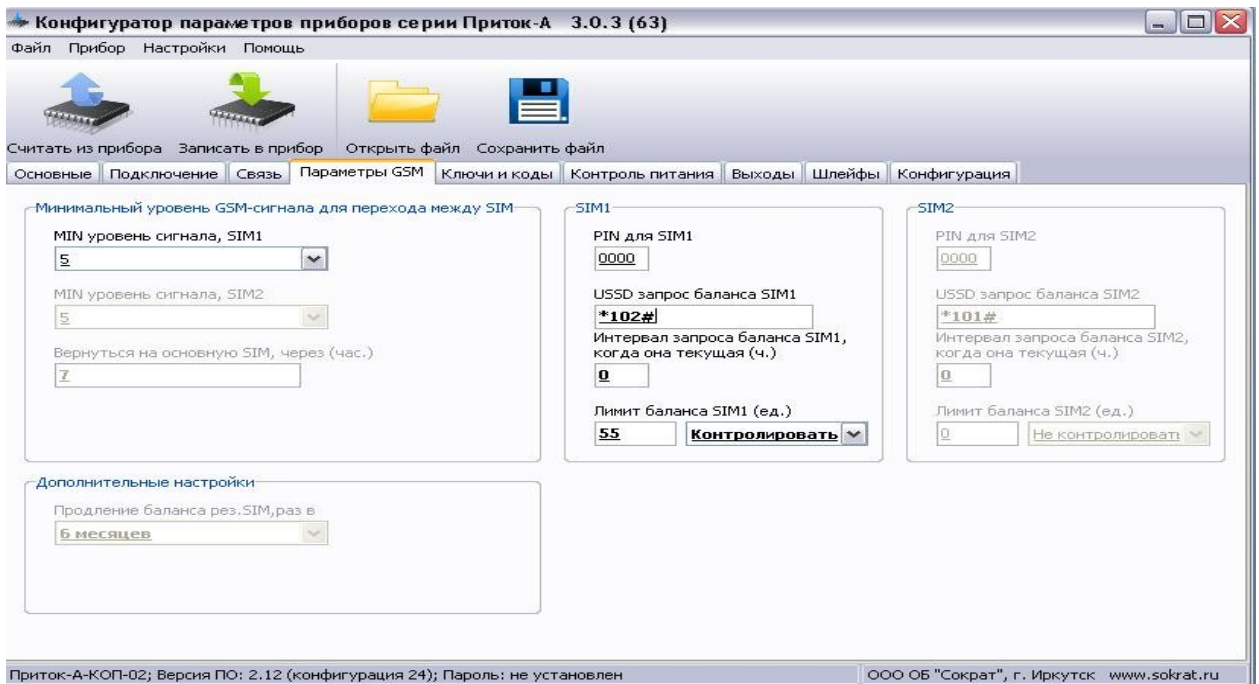
Переходим во вкладку «Подключение». Заполняем поле «IP-адрес сервера 1, Ethernet», тем IP, который можно узнать с помощью командной строки (win+Rcmd→, при этом нужно зайти в командную строку) и набрать ipconfig /all. Набираем идентификатор прибора на пульте, как показано ниже и вставляем сгенерированный ранее ключ шифрования.



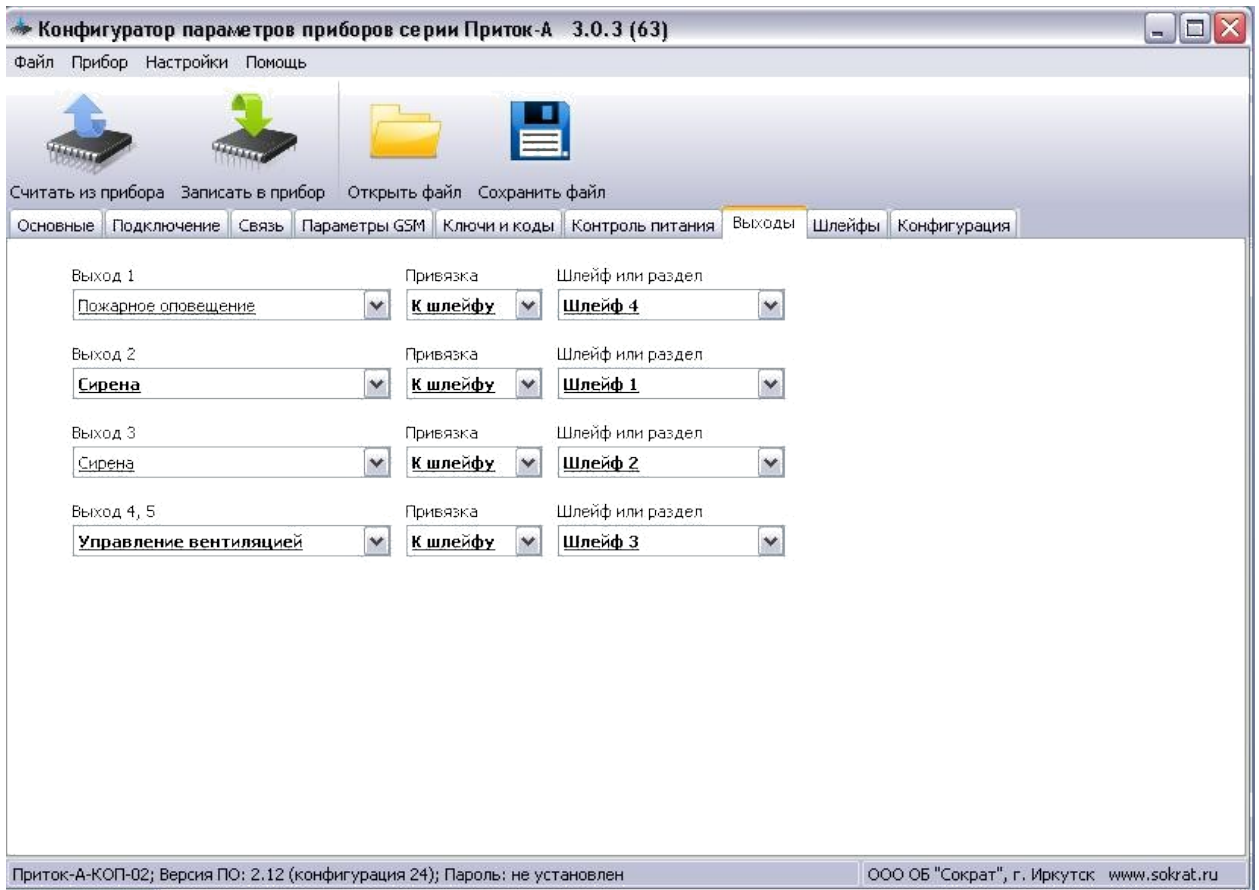
Переходим во вкладку «Связь» в окне «Используемые каналы связи» выбираем пункт «Только GPRS», а в окне «Используемые SIM» пункт «Только SIM1».



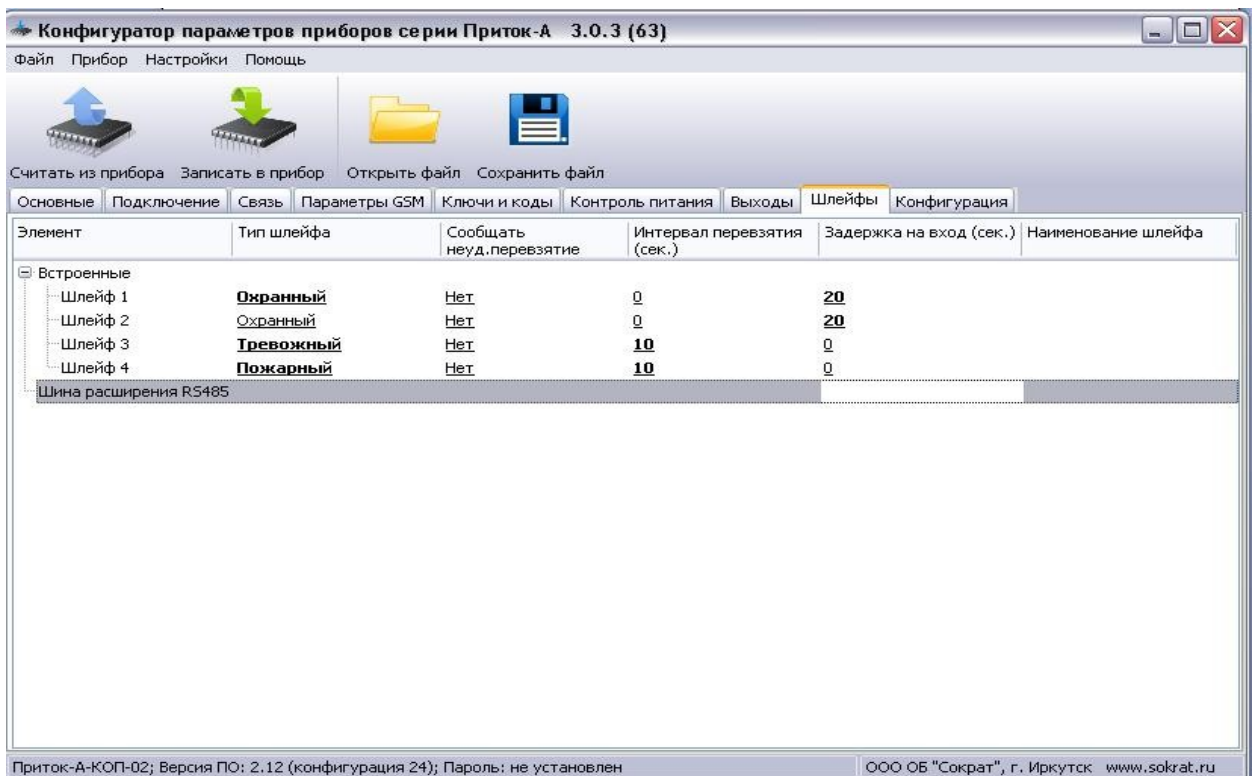
Переходим во вкладку «Параметры GSM» в окне «SIM1» выставляем USSD запрос баланса в зависимости от выбранного оператора и контроль баланса на SIM-карте.



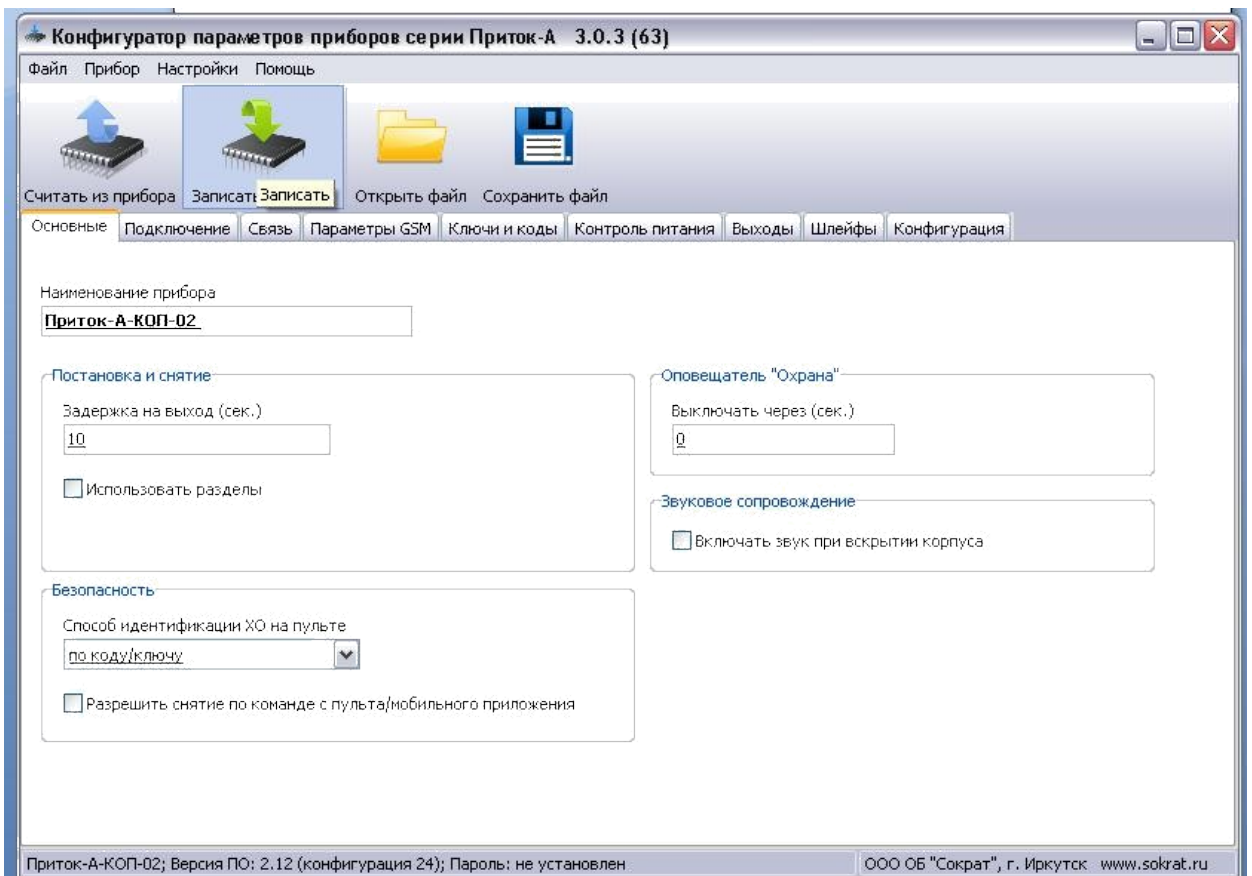
Во вкладке «Выходы» заполняем поля следующим образом:



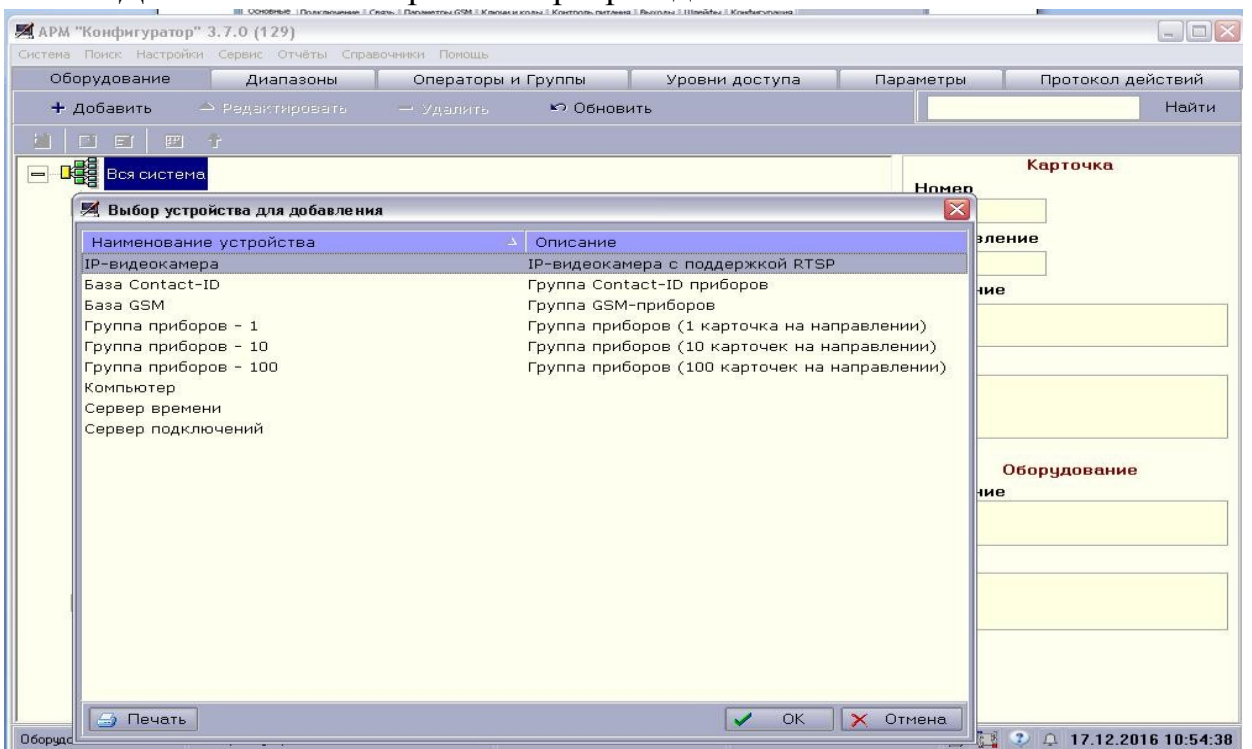
Во вкладке «Шлейфы» заполняем поля следующим образом:



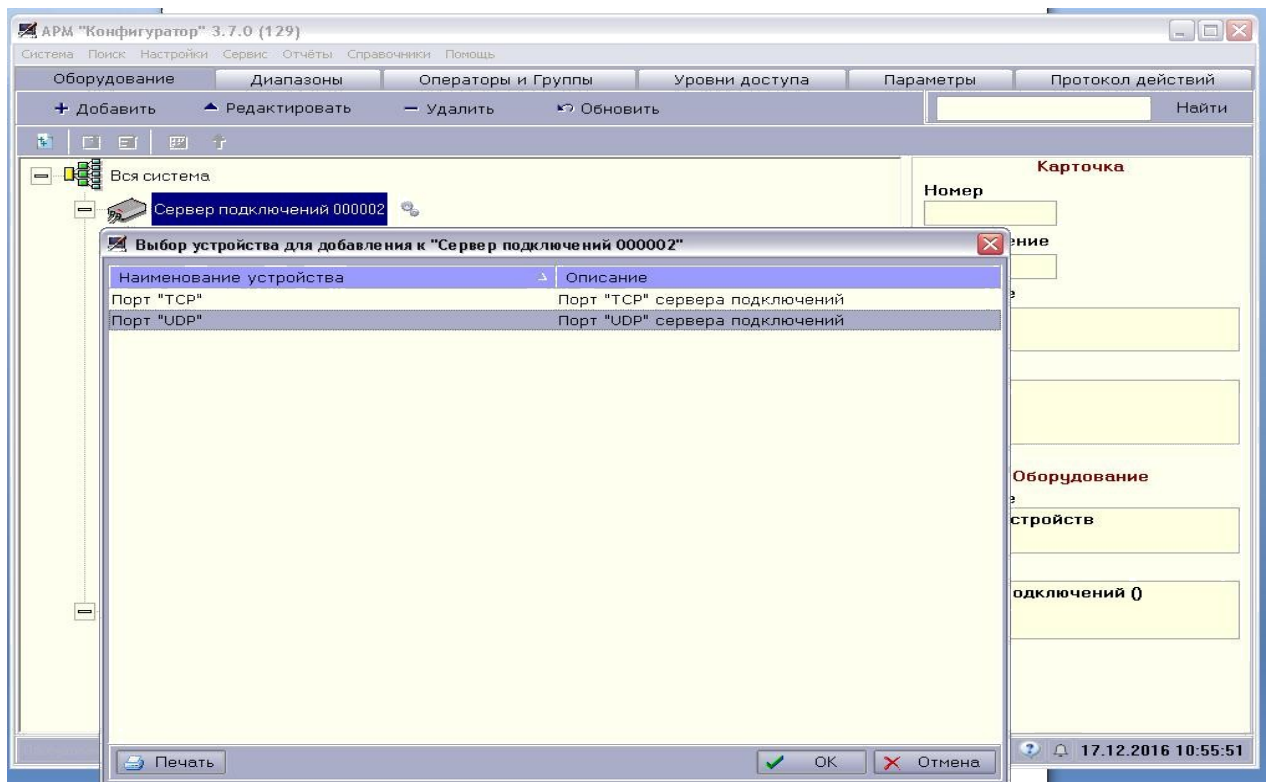
Нажимаем кнопку «Записать в прибор»



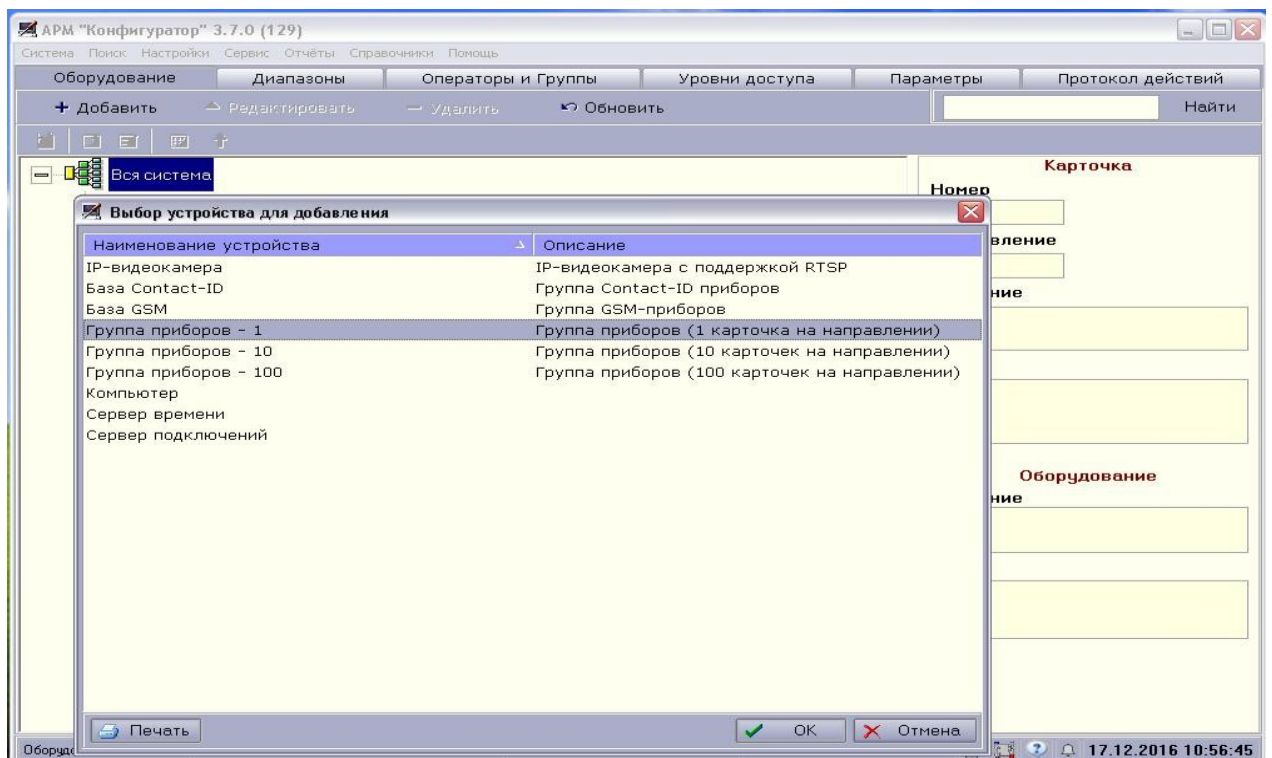
2. Запускаем программу «АРМ-Конфигуратор». Нажимаем «Вся система» «Добавить» и выбираем «Сервер подключений»



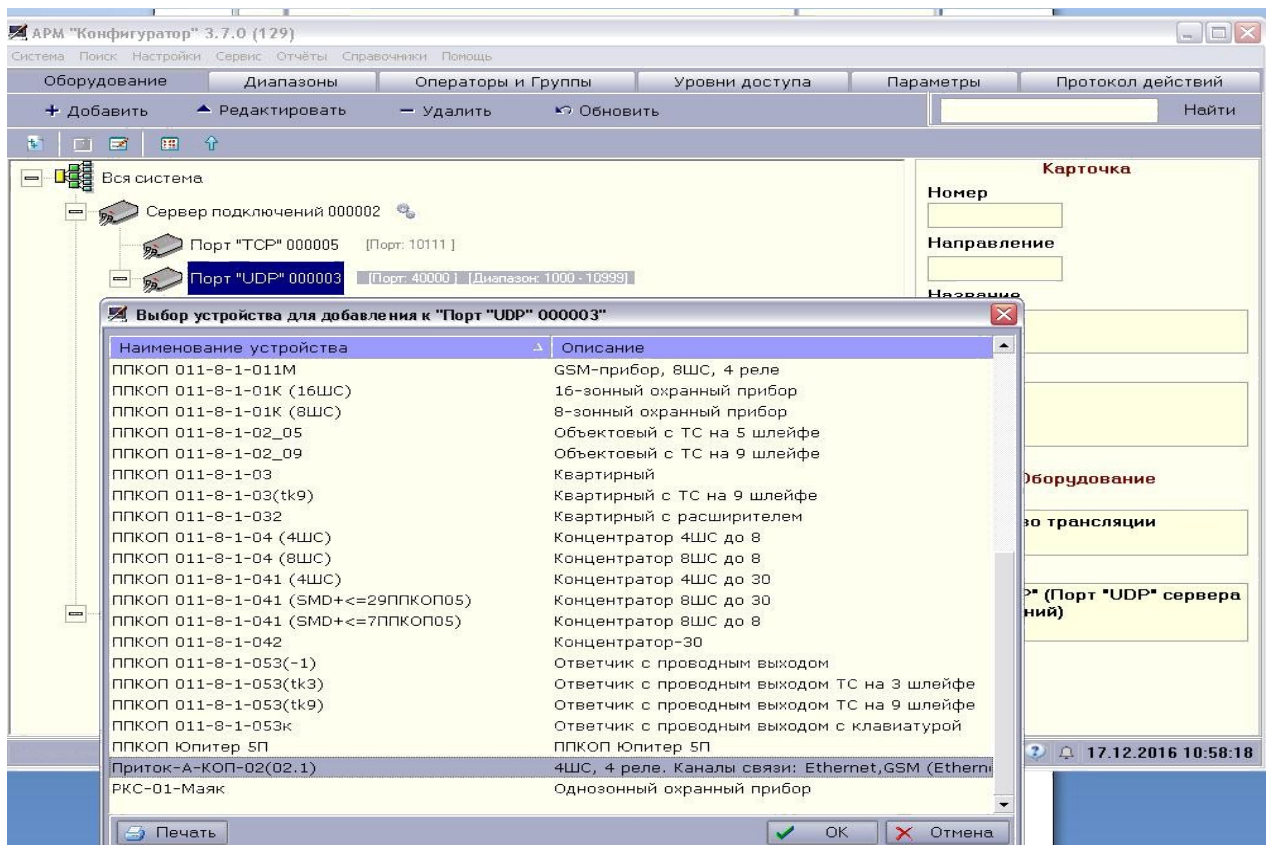
В «Сервер подключений» добавляем Порт UDP



Далее снова в «Связь системы» выбираем «Группа приборов-1». К группе приборов добавляем «Приток А-КОП-02 (02.1)»

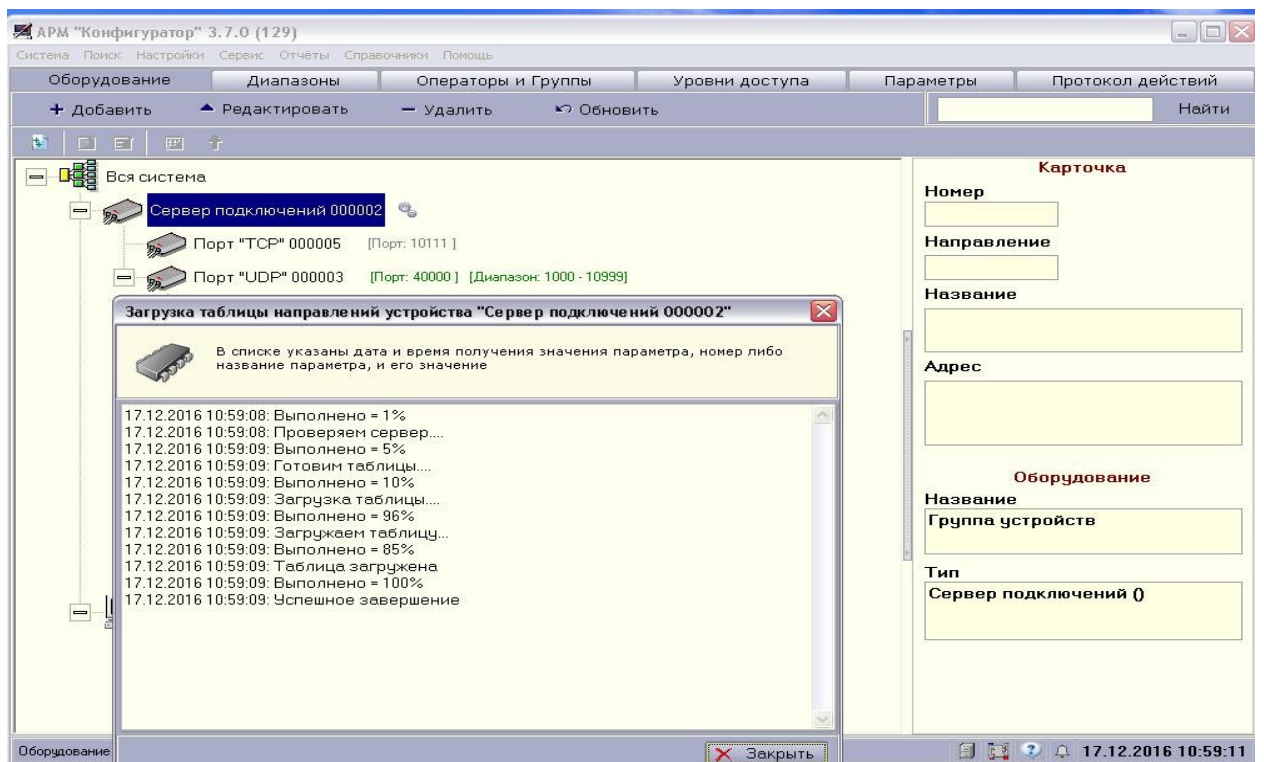




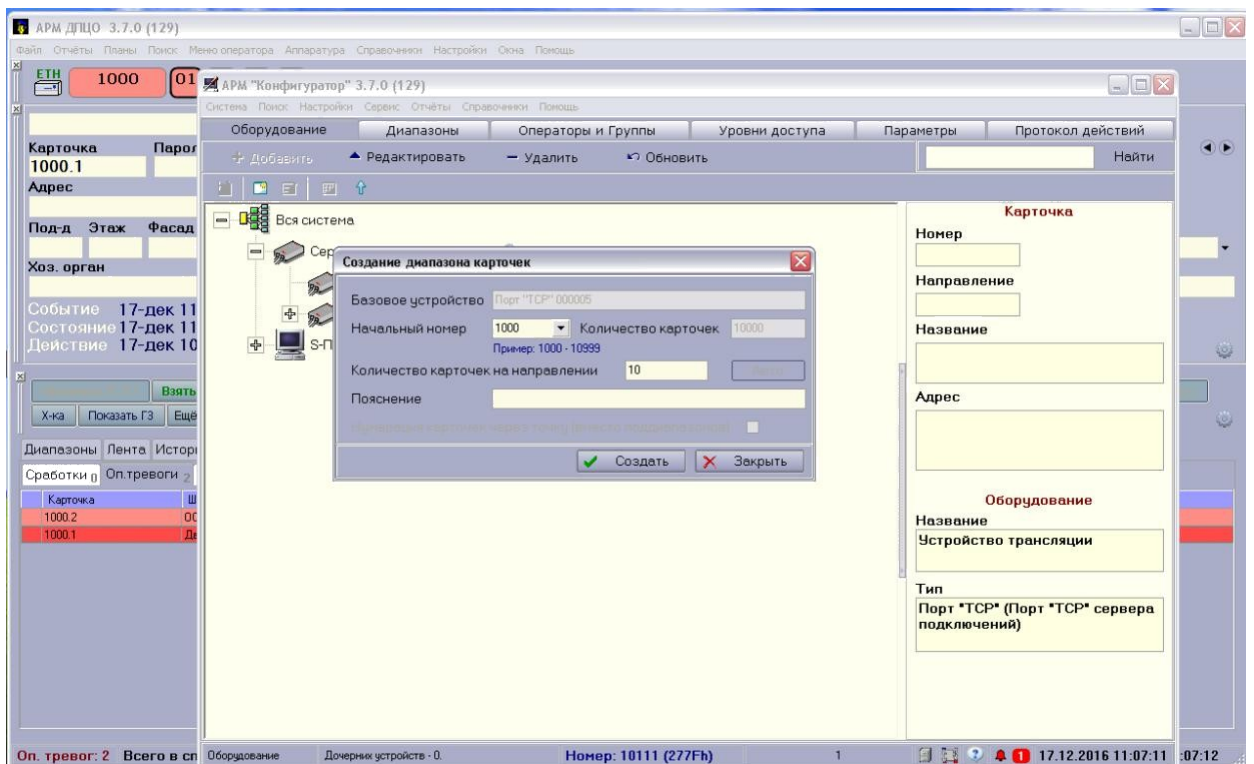


Правой кнопкой кликаем на пункт «Сервер подключений».

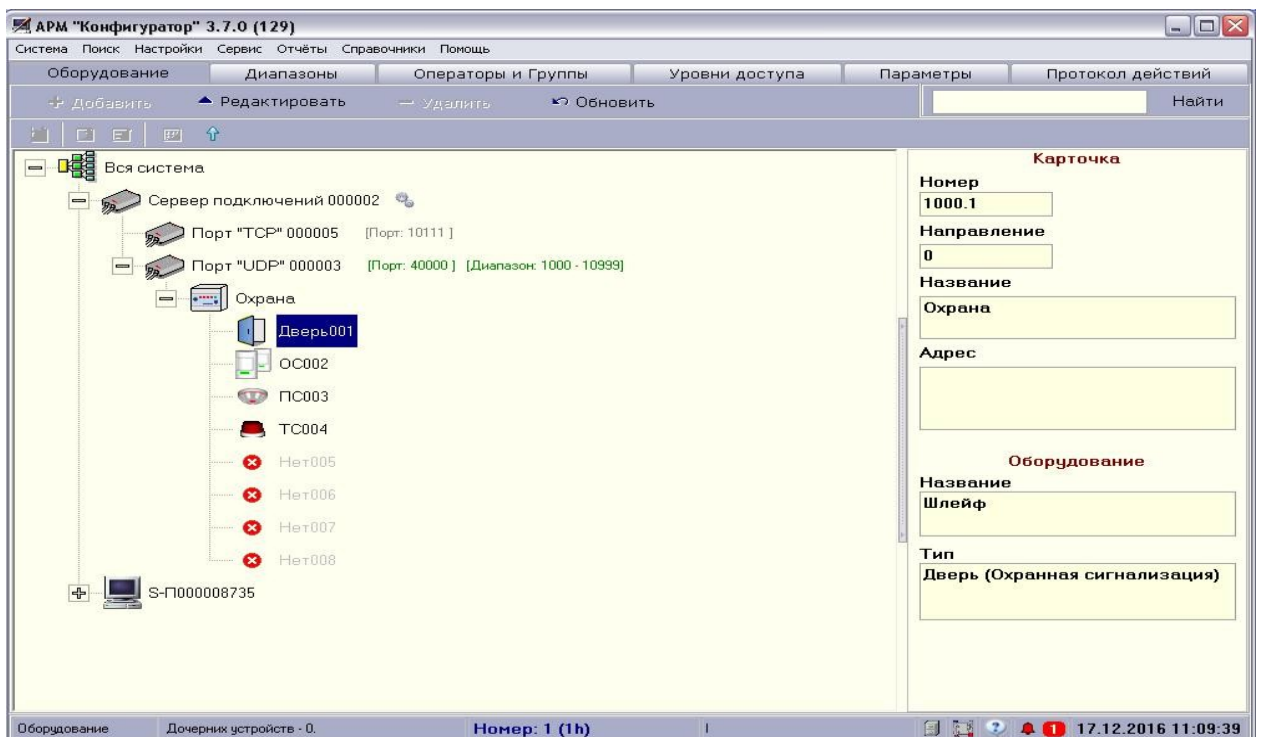
Нажимаем «Загрузить таблицу направлений». Связь установлена

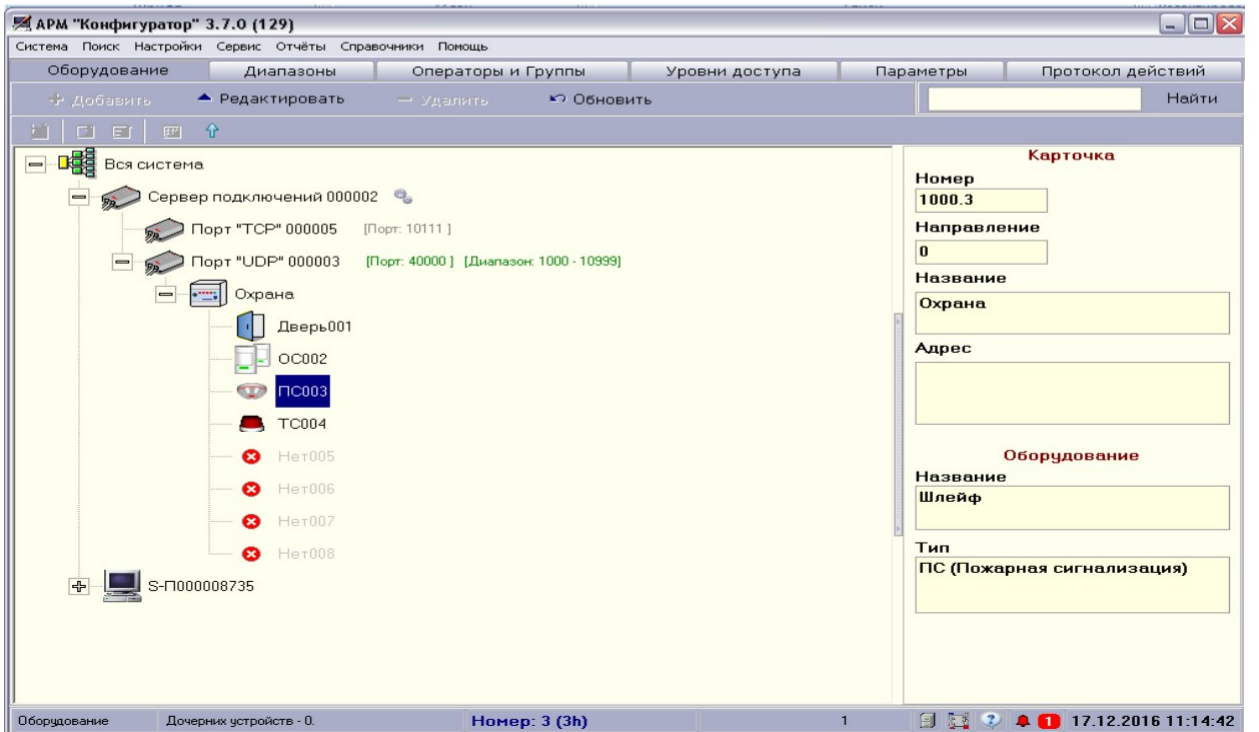
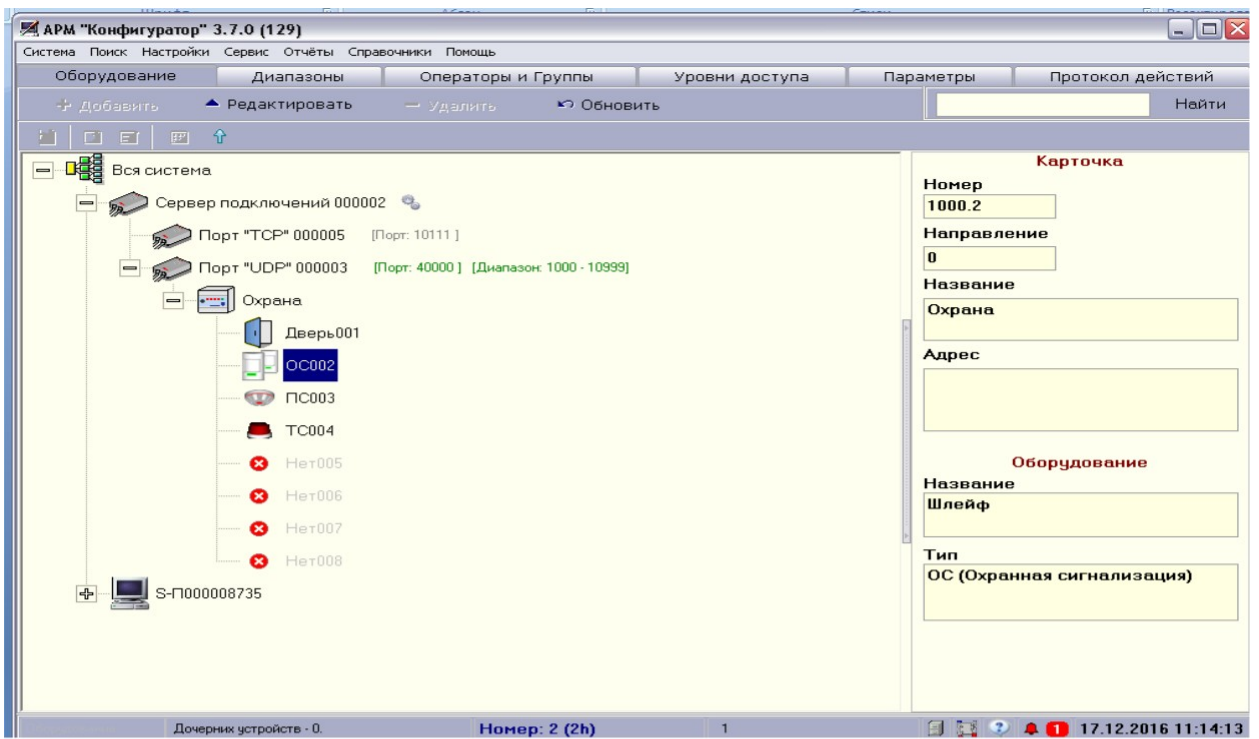


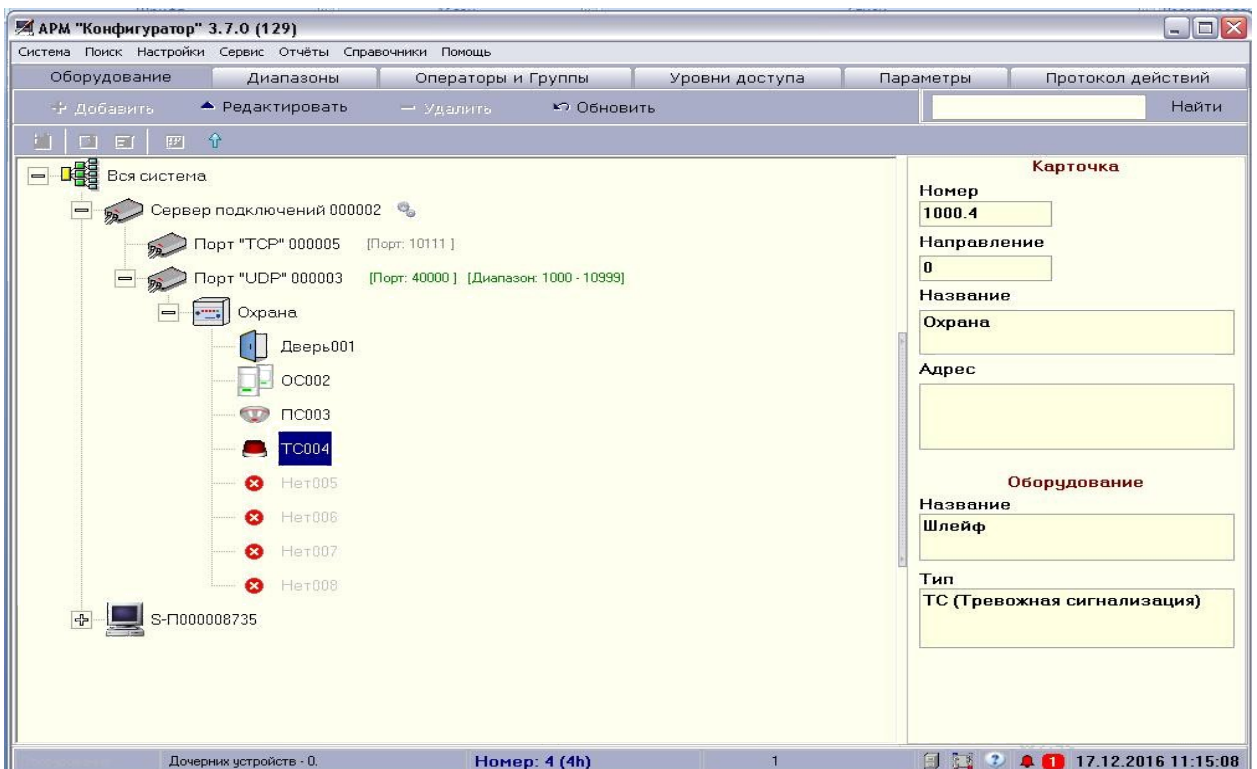
Кликаем на пункт Порт UDP правой кнопкой и выбираем «Создать диапазон». Устанавливаем Начальный номер - 1000



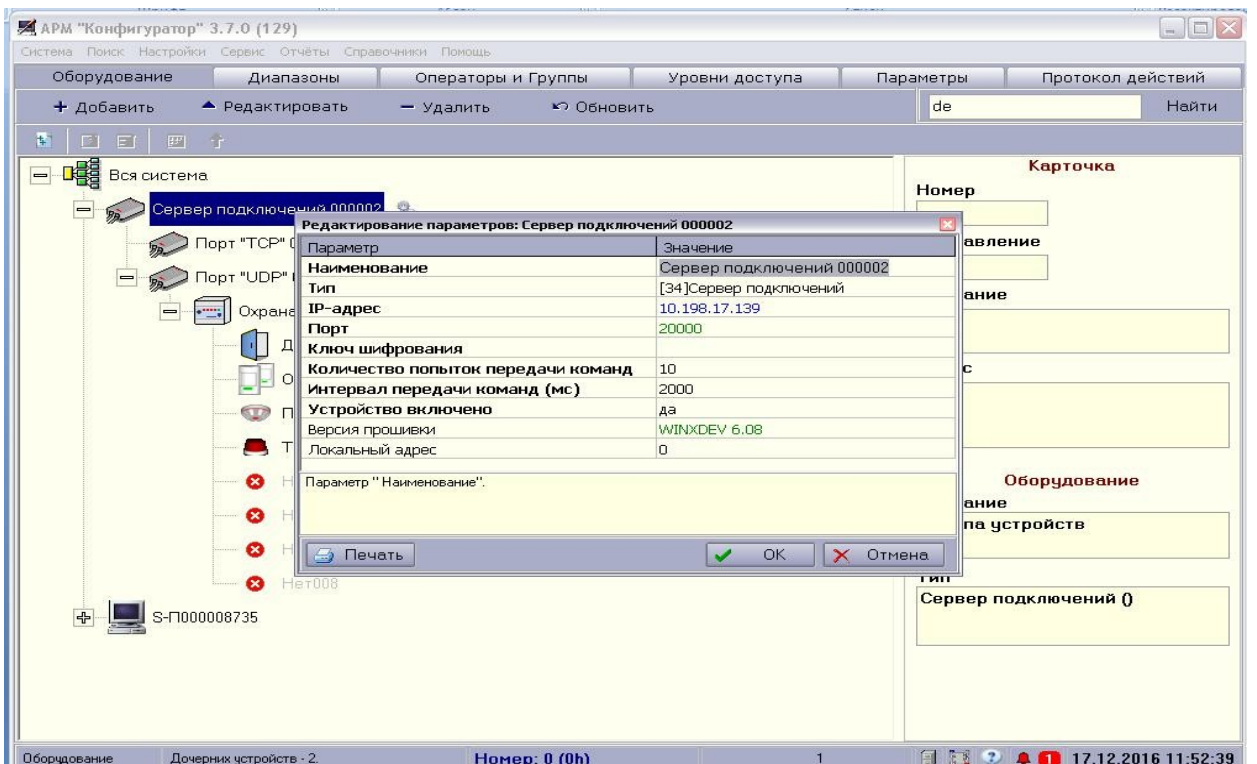
Проверяем установились ли таким образом номера карточек для Двери, Охранной, Пожарной и Тревожной сигнализаций. Для этого переходим в Сервер подключений ->Порт ODP ->Охрана. Кликаем поочередно на каждый пункт списка. В правой части окна появляется поле «Карточка». Проверяем наличие номеров.



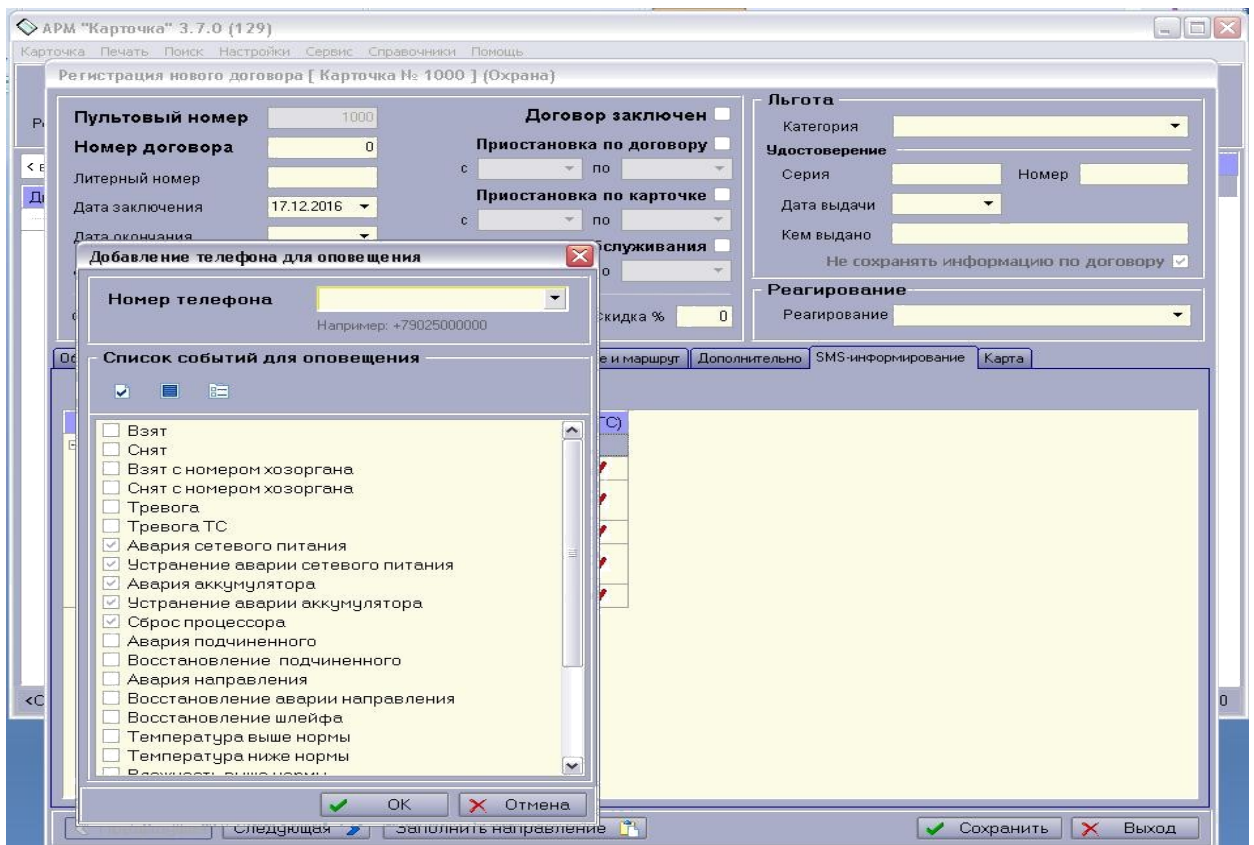




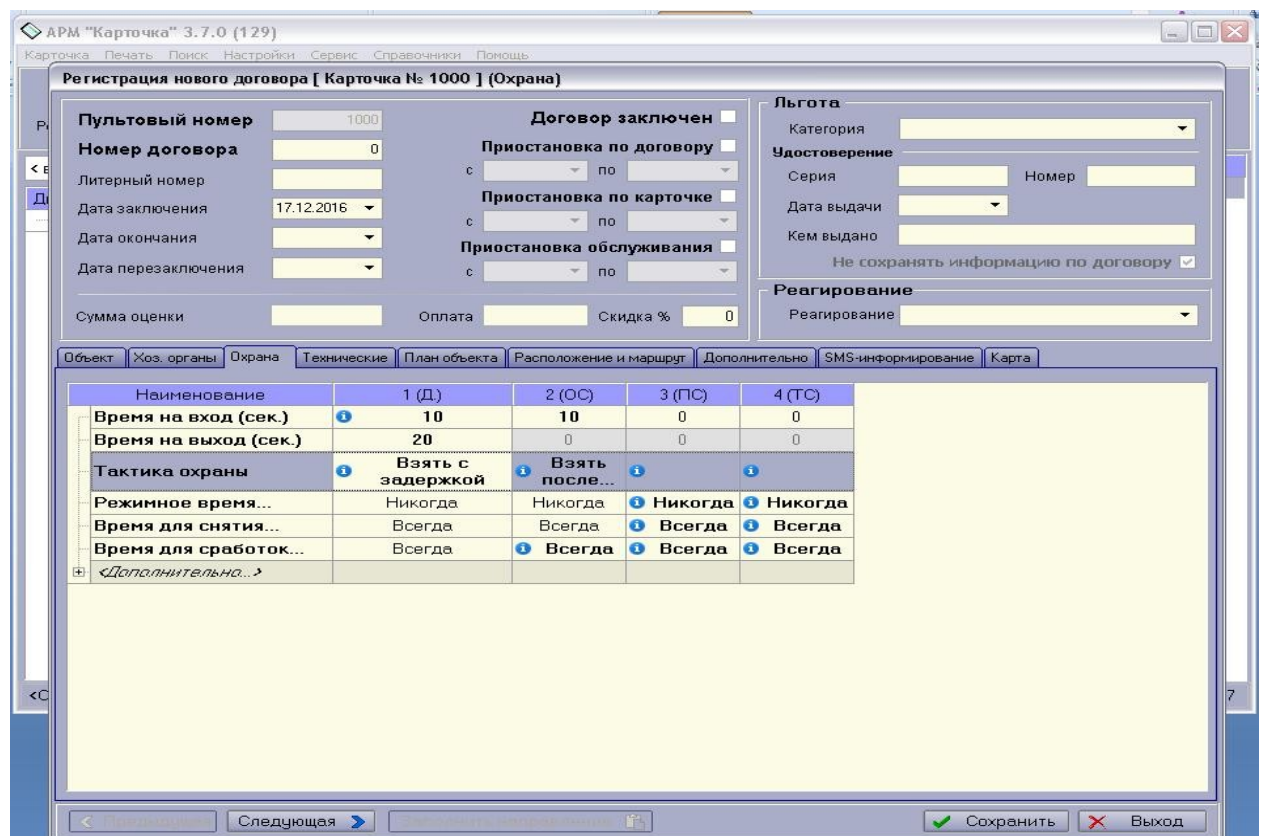
Нажимаем клавишу «F2». Заполняем поля по данным, полученным ранее.



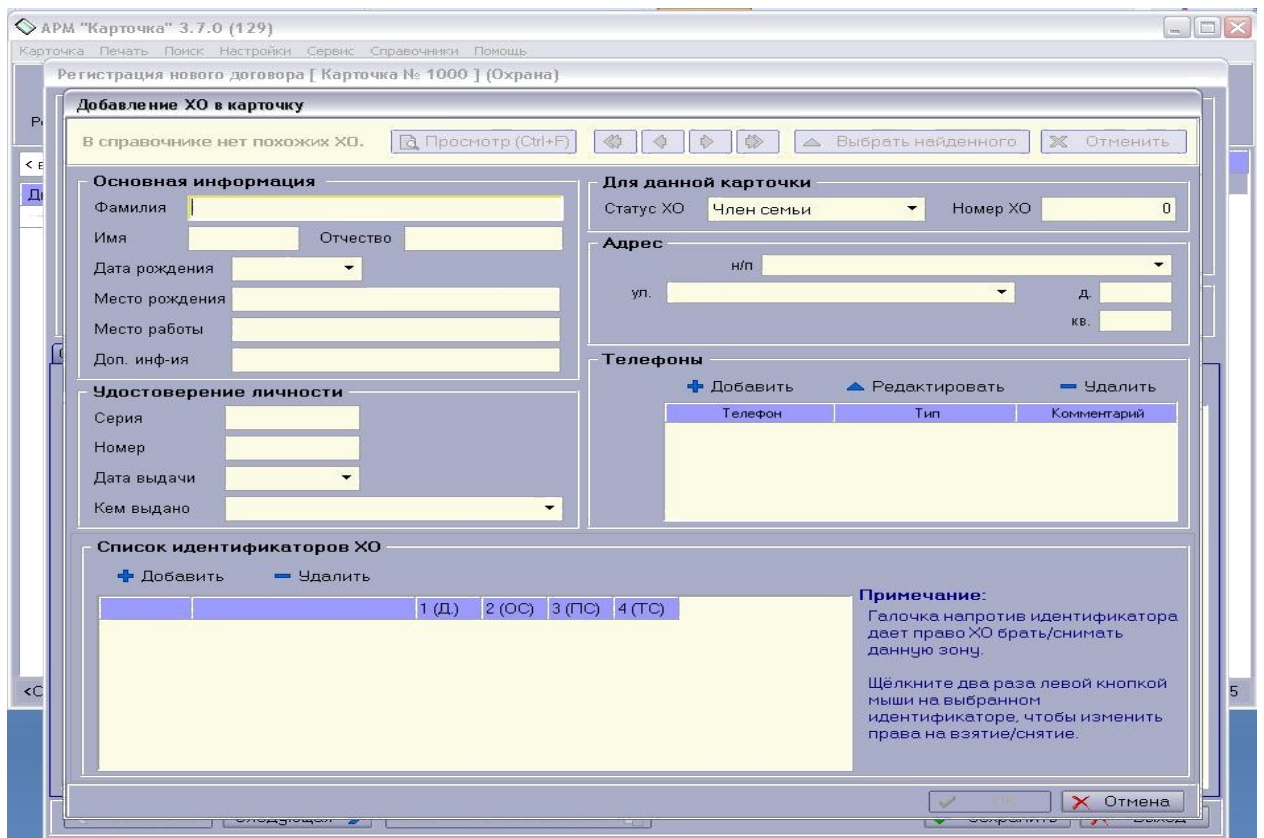
3. Запускаем программу АРМ «Карточка». Так как диапазоны были созданы ранее, кликаем на Пультовый номер «1000». Загружается карточка «Регистрация нового договора» Переходим во вкладку «SMS-информирование», нажимаем кнопку «Добавить». Вводим номер телефона и выбираем следующие пункты. Нажимаем «ОК».



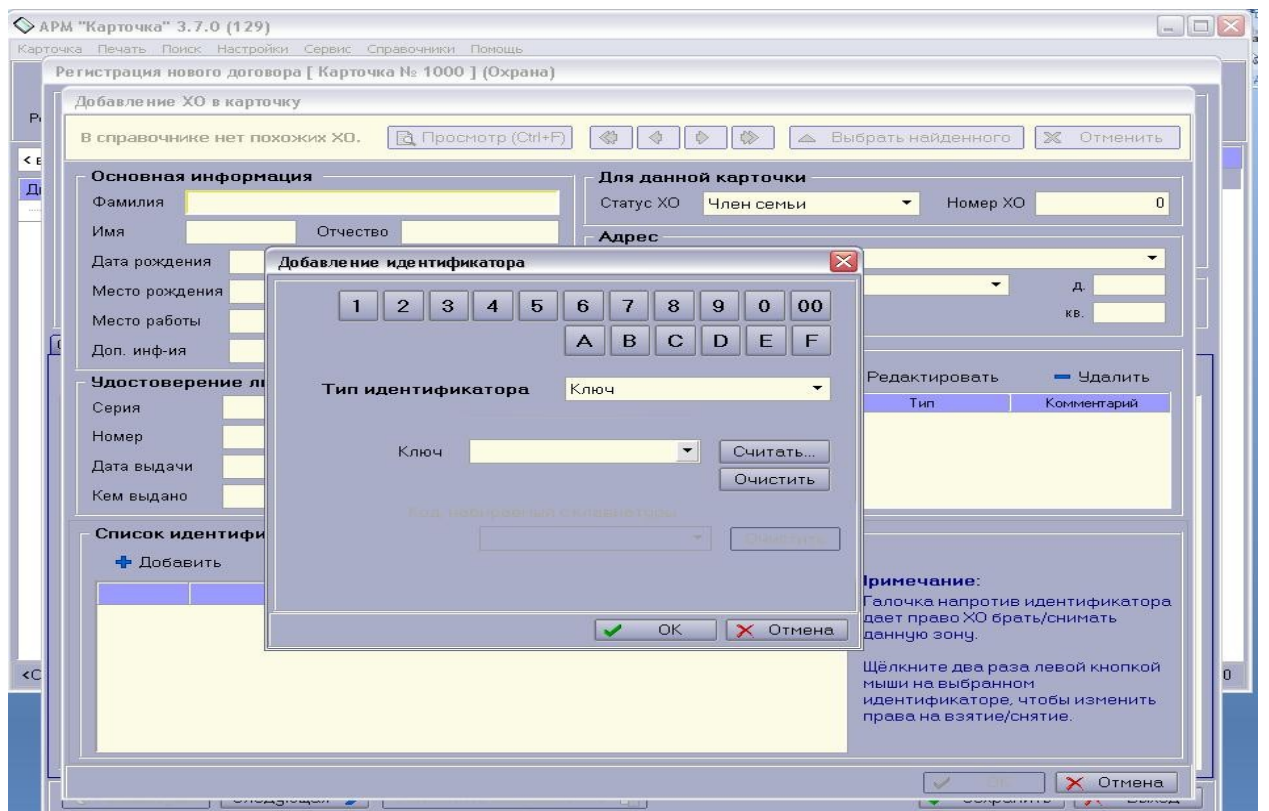
Переходим во вкладку «Охрана» и заполняем следующим образом:



Переходим во вкладку «Хоз.органы». Кликаем на «Добавить ХО». По необходимости заполняем поля «Фамилия» и т.д.



В поле «Список идентификаторов ХО» нажимаем на кнопку «Добавить». В поле «Ключ» вставляем ключ, сгенерированный в программе UniProg.



По необходимости вводим данные - данном случае «Наименование» - Охрана, и Сохраняем.

АРМ "Карточка" 3.7.0 (129)

Карточка Печать Поиск Настройки Сервис Справочники Помощь

### Регистрация нового договора [ Карточка № 1000 ] (Охрана)

**Пультовый номер** 1000 **Договор заключен**

**Номер договора** 0 **Приостановка по договору**

Литерный номер  с  по

Дата заключения 17.12.2016 **Приостановка по карточке**

Дата окончания  с  по

Дата перезаключения  **Приостановка обслуживания**

с  по

Сумма оценки  Оплата  Скидка % 0

**Льгота**

Категория

**Удостоверение**

Серия  Номер

Дата выдачи

Кем выдано

Не сохранять информацию по договору

**Реагирование**

Реагирование

Объект Хоз. органы Охрана Технические План объекта Расположение и маршрут Дополнительно SMS-информирование Карта

**Наименование** Охрана **Тип объекта** Квартира

**Адрес**

н/п

ул.  д.  кв.

**Телефоны**

+ Добавить ▲ Редактировать - Удалить

Телефон	Тип	Комментарий

**Характеристика объекта**

Подъезд  Этаж  Комнат

Окон всего  Фасад  Торец  Тыл

Балкон

Тип постройки

Категория объекта

Вскрытие объекта Без понятия

Код подъезда

Код двери лестничной клетки

Ключей от объекта 0 Пароль

Ключей от подъезда 0 Пенал

Принял на хранение

Сохранить Выход

Параметры готовы. Нажимаем на «1000», далее кликаем на «Копировать», выбираем каждый пункт из списка, т.е. «1000.1», «1000.2», «1000.3», «1000.4» и нажимаем «Вставить»

АРМ "Карточка" 3.7.0 (129)

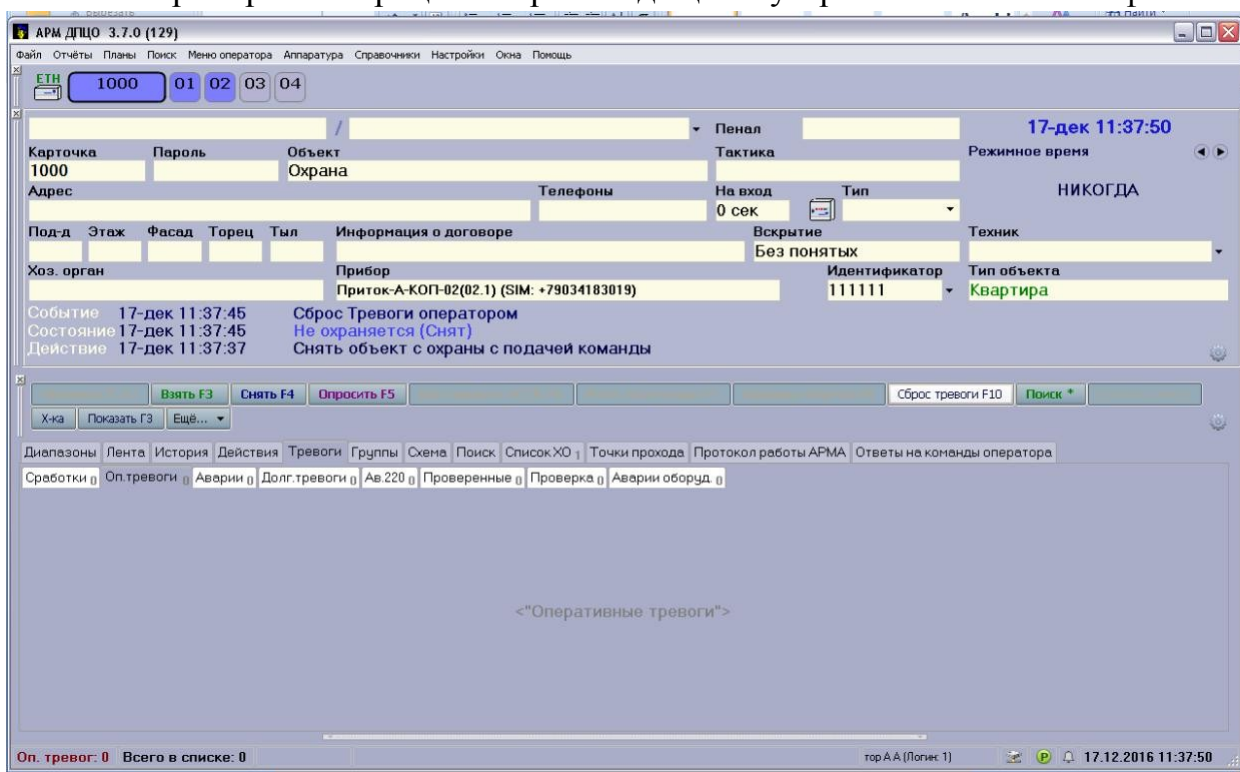
Карточка Печать Поиск Настройки Сервис Справочники Помощь

Редактировать Печать Выборка Копировать Вставить По направлению Частично Фильтр Найти Обновить Вкл. "Проверка" Выкл. "Проверка"

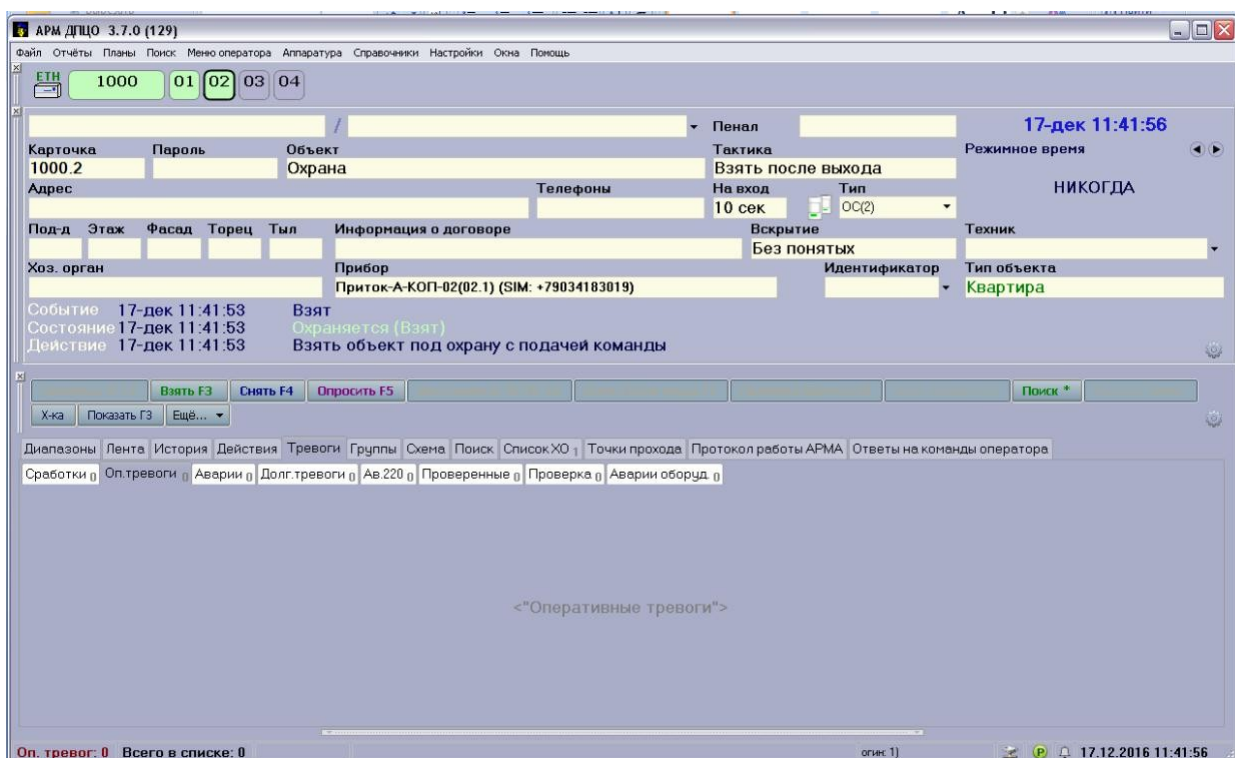
Пультовый номер	Договор	Литерный	Тип объекта	Наименование объекта
1000			Квартира	Охрана
1000.1			Квартира	Охрана
1000.2			Квартира	Охрана
1000.3			Квартира	Охрана
1000.4			Квартира	Охрана

<Ctrl>+<DownArrow> - найти след Запомнили: 1000 001000-010999 5 1@S-I 17.12.2016 11:32:09

#### 4. Запускаем программу АРМ ДПЦО 3.7, которая позволяет контролировать процессы происходящие в устройствах и на шлейфах.

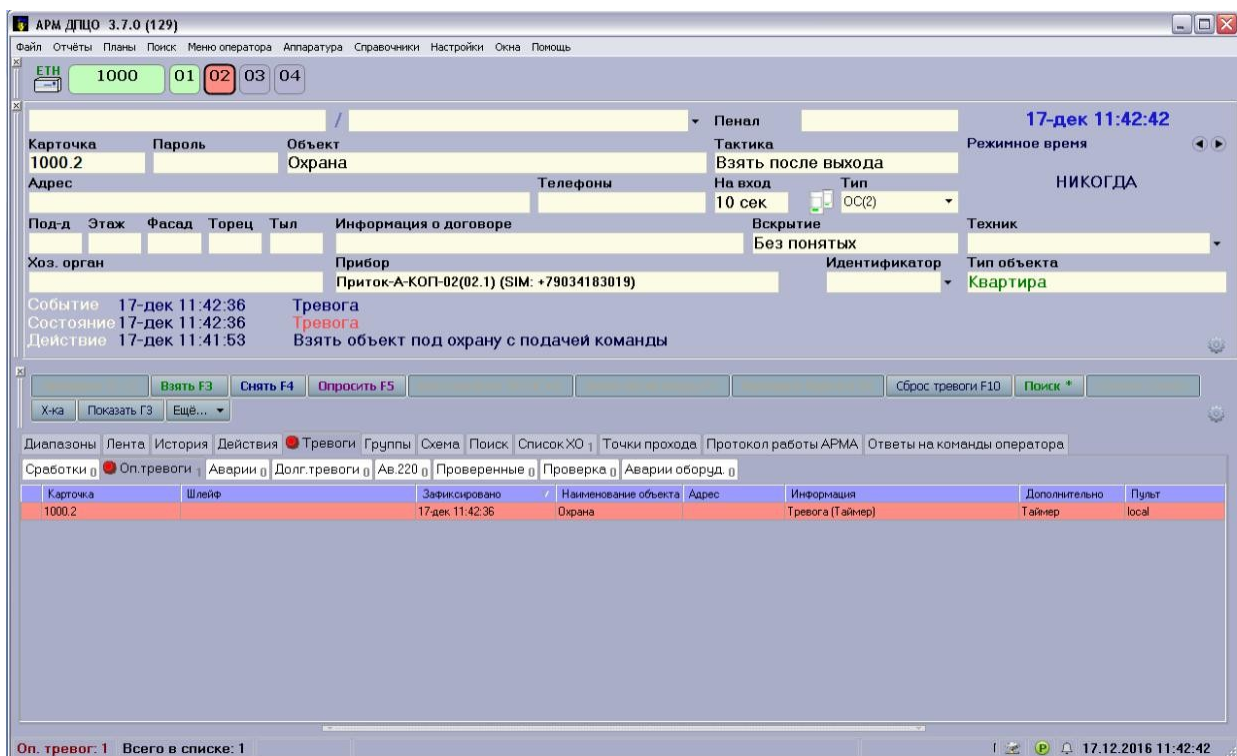


Для проверки работоспособности системы кликаем на кнопку «1000» ПКМ и выбираем «Взять под охрану», аналогично проделываем с остальными шлейфами.





Ожидаем сработку тревоги (на стенде создаем обрыв на нужном нам шлейфе). Индикаторы показывают шлейф, на котором произошел обрыв.

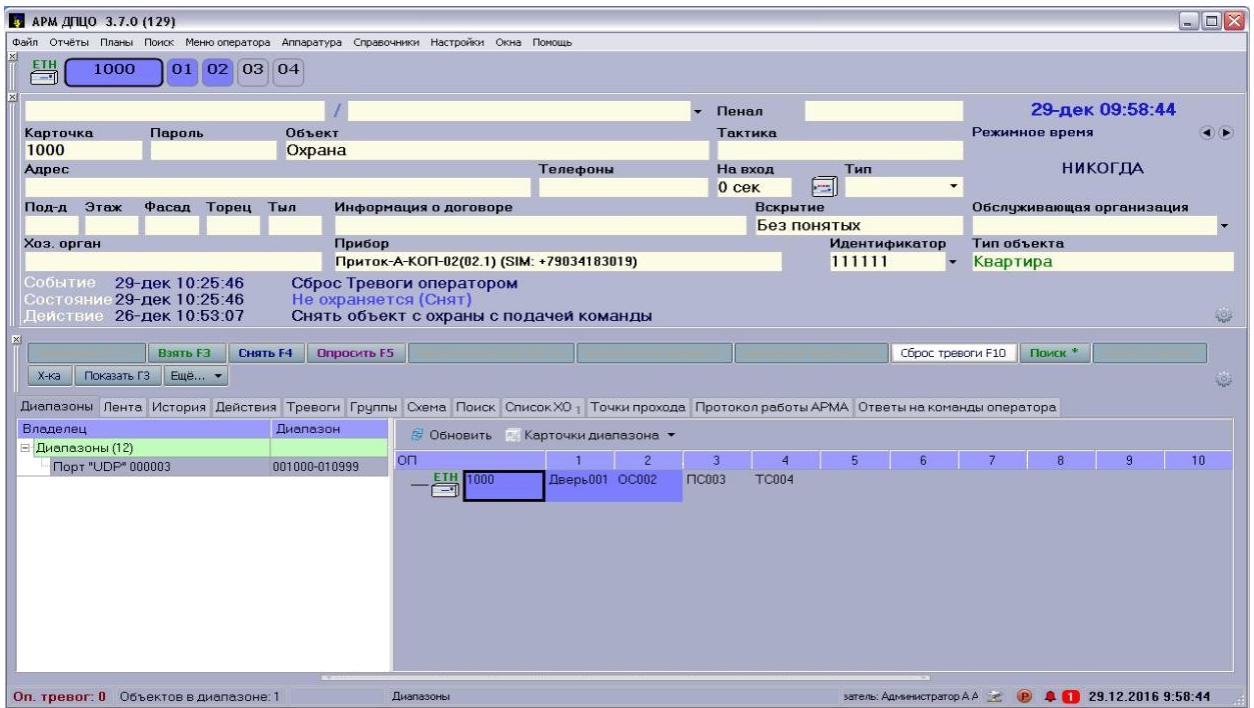


Настройка Приток-А-КОП-02 произошла успешно.

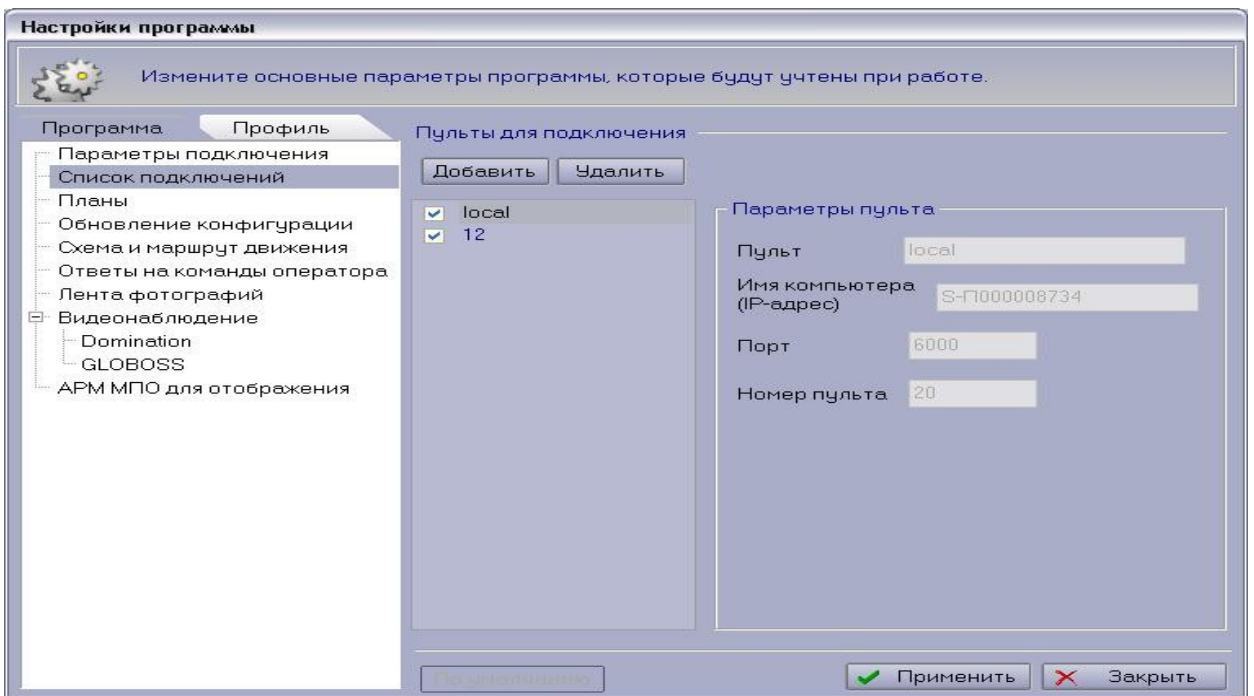
### Создание второго пульта наблюдения

Скопировали на следующий ПК БД (prtx\_db.fdb)

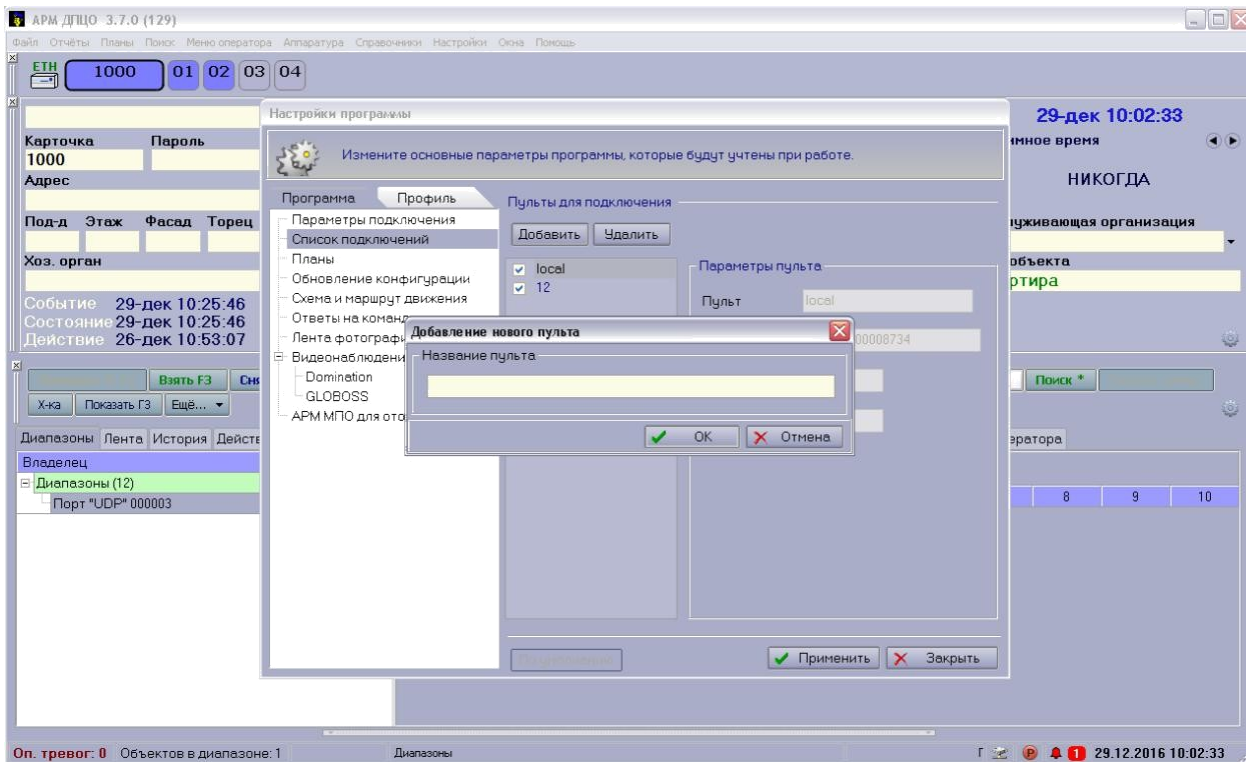
Необходимо произвести установку, скачанного с официального сайта ПО, далее запуском программу АРМ ДПЦО 3.7. Нажимаем на вкладку «Настройки» -> «Настройки программы».



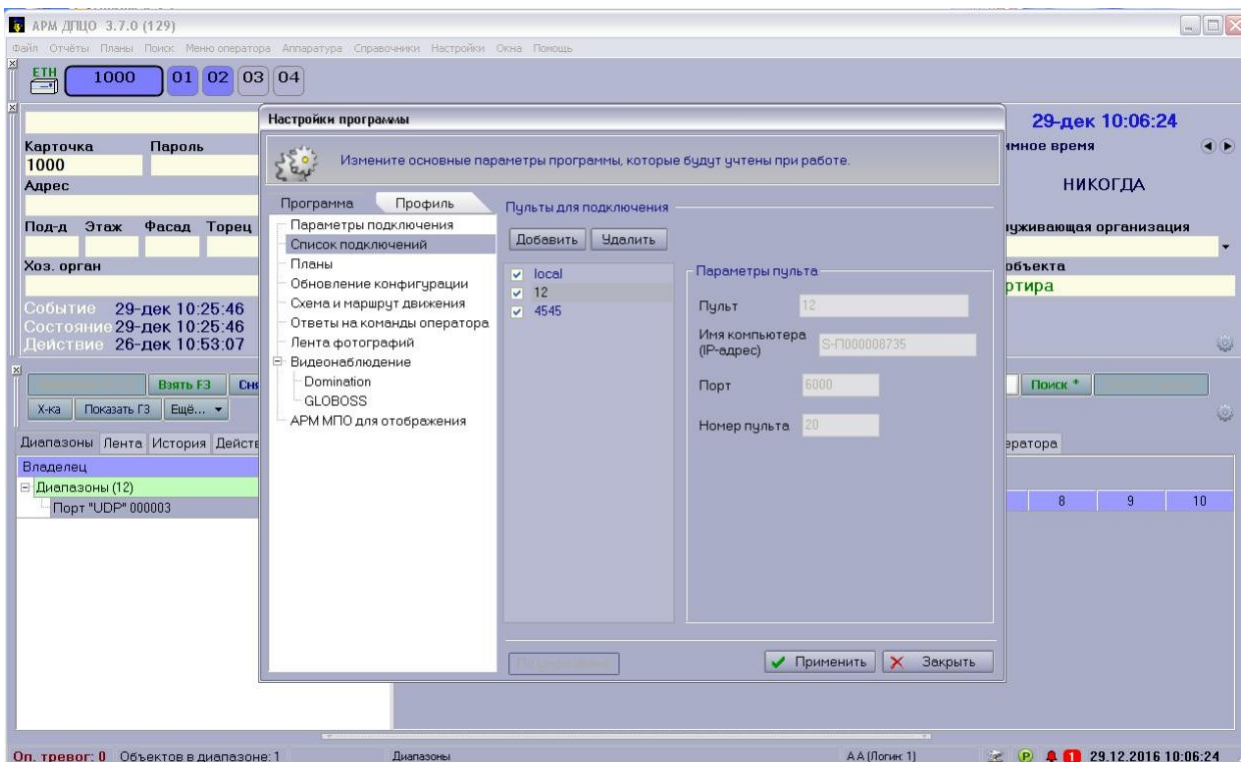
Во вкладке «Профиль» выбираем «Список подключений», нажимаем «Добавить».



Вводим название пульта (например, ip-адрес или название ПК)



Изменяем параметры пульта. Вводим «Имя компьютера», на котором установлено ПО и все остальные параметры по надобности.



Нажимаем «Применить».

**Отчет должен содержать:**

1. Название, цели и задачи работы;

2. Скриншоты о проделанной работе;
3. Заключение и выводы.

**Контрольные вопросы:**

1. Каково назначение контролера «ПРИТОК-А-КОП-02»?
2. Сколько извещений «ПРИТОК-А-КОП-02» передаёт на ПЦН?
3. Перечислите каналы связи с протоколами обмена данных?
4. Возможно ли одновременно подать сообщение на SIM-карту и в сеть Интернет?

## Приложение

Таблица №2 Исходные данные адресов приборов и пожарных извещателей интегрированной системы «Орион» используемые на стенде.

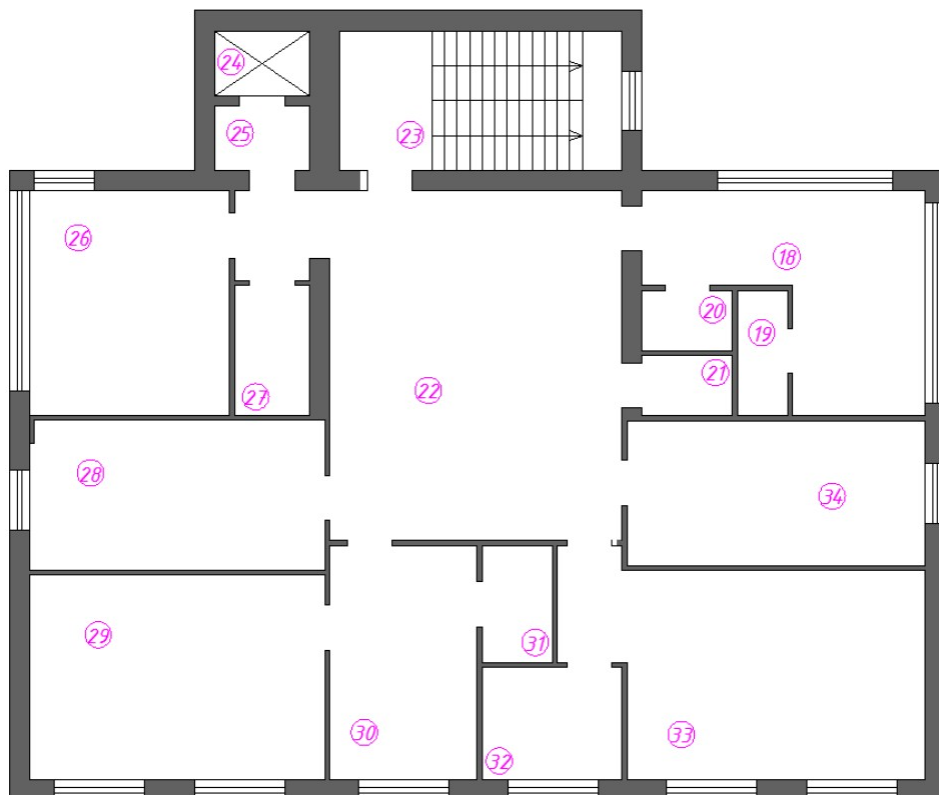
№ п/п	Наименование приборов и извещателей	Адреса	Версии приборов
1	ПКУ С2000М	1	2.05
2	ППКОП Сигнал-10	2	
3	ППКОП Сигнал-20М	3	
4	ППКОП Сигнал-20П	4	
5	Рупор	5	
6	С2000-КДЛ	6	1.46
7	С2000-СП2 исп. 01	1-2	
8	С2000-АР8	3-10	
9	С2000-КТ	18	
10	С2000-ИК	19	
11	С2000-СТИК	20-21	
12	С2000-ПИК	22	
13	С2000-СМК	23	

Вариант для четных студентов в списке преподавателя



Экспликация помещения		
№ помеще ния	Наименование	Площадь м <sup>2</sup>
35	зал ЛФК	105,6
36	раздевалка	17,8
37	душевая	3,4
38	санузел	1,3
39	санузел	1,2
40	коридор	14,3
41	лифт	1,7
42	лестничная клетка	15,8
43	коридор	1,7
44	кабинет	8,8
45	кабинет	9,0
46	кабинет	13,6
47	кабинет	20,7
48	коридор	5,2

Вариант для нечетных студентов в списке преподавателя



Экспликация помещения		
№ помеще ния	Наименование	Площадь м <sup>2</sup>
18	кабинет	20,1
19	санузел	1,9
20	раздевалка	17,2
21	подсобное помещение	23,9
22	холл	13,9
23	лестничная клетка	15,8
24	лифт	1,7
25	коридор	1,7
26	кабинет	18
27	кладовая	3,8
28	кабинет	17,2
29	кабинет	23,9
30	кабинет	13,9
31	подсобное помещение	3,4
32	пультовая	6,5
33	кабинет	27,5
34	кабинет	16,8

Таблица №1.

Индивидуальные задания для лабораторной работы.

№ п/п	Разделы	Охранные извещатели	Реле 2	
			Задержка вкл.	Время упр.
1	Гл. Вход Холл Кабинет	С2000-СМК С2000-ИК С2000-КТ	0	30
2	Офис Лаборатория	С2000-СТИК С2000-ПИК	10	40
3	Склад	С2000-АР8, С2000-ИК	0	40
4	Кабинет Приемная	С2000-СМК, С2000-ИК С2000-КТ	30	60
5	Коридор Охрана	С2000-АР8, С2000-ПИК С2000-КТ	20	80
6	Холл Кабинет Зам. директора	С2000-ИК, С2000-СМК С2000-ПИК С2000-КТ	0	60
7	Касса	С2000-КТ, С2000-СМК, С2000- СТИК	15	30
8	Кабинет Администратор	С2000-ИК, С2000-СМК С2000-КТ	0	30
9	Экономист Библиотека	С2000-КТ, С2000-СМК С2000-СТИК	10	40
10	Директор Офис	С2000-КТ, С2000-ИК С2000-АР8	0	40
11	Зап. выход Холл	С2000-СМК С2000-СТИК, С2000-ПИК	30	60
12	Кабинет Гл. врач Магазин	С2000-ИК С2000-КТ, С2000-СМК С2000-СТИК	20	80
13	Отдел кадров	С2000-ИК, С2000-СМК	0	60
14	Аудитория Пост охраны	С2000-АР8 С2000-КТ	15	30
15	КПП Вестибюль	С2000-КТ; С2000-ИК, С2000-СМК	0	200

Таблица №2

Исходные данные адресов приборов и пожарных извещателей интегрированной системы «Орион» используемые на стенде.



№ п/п	Разделы	Пожарные изв-ли	Реле 1		Реле 2		Речевое оповещ.	
			Задерж- ка вкл.	Время упр.	Задерж- ка вкл.	Время упр.	Задерж- ка вкл.	Время упр.
1	Коридор Холл Кабинет	С2000-АР2 ИПР-513-3А ДИП-34А	0	30	0	30	0	60
2	Кухня Лаборатор ия	С2000-ИП ИПР-513-3А	10	30	10	40	20	60
3	Бухгалтери я	С2000-АР2, ИПР-513-3А	0	40	0	40	20	60
4	Кабинет Приемная	ДИП-34А С2000-ИП	30	60	30	60	30	100
5	Коридор Охрана	С2000-АР2 ДИП-34А	20	80	20	80	0	100
6	Холл ЭЦ АТС	ИПР-513-3А ДИП-34А С2000-АР2	15	30	0	60	60	180
7	Раздевалка	С2000-АР2, ИПР-513-3А	0	60	15	30	0	180
8	Кабинет Тамбур	ДИП-34А ИПР-513-3А	0	30	0	30	0	60
9	Экономист Гладильня	ДИП-34А; С2000-ИП, ИПР-513-3А;	10	30	10	40	20	60
10	Вестибюль Офис	ИПР-513-3А С2000-АР2	0	40	0	40	20	60
11	Столовая Холл	С2000-ИП ИПР-513-3А	30	60	30	60	30	100
12	Кабинет Гл. врач Тамбур	С2000-ИП ДИП-34А ИПР-513-3А	20	80	20	80	0	100
13	Отдел кадров	ДИП-34А, ИПР-513-3А	15	30	0	60	60	180
14	Аудитория Коридор	С2000-АР2 ИПР-513-3А	0	60	15	30	0	180
15	Кухня Вестибюль	С2000-ИП; С2000-АР2, ИПР-513-3А;	0	900	0	900	0	1800

Таблица №3

Индивидуальные задания для практического занятия №4.

№ п/п	Наименование приборов и извещателей	Адреса	Версии приборов
1	ПКУ С2000М	1	2.05

2	ППКОП Сигнал-10	2	
3	ППКОП Сигнал-20М	3	
4	ППКОП Сигнал-20П	4	
5	Рупор	5	
6	С2000-КДЛ	6	1.46
7	С2000-СП2 исп. 01	1-2	
8	С2000-АР8	3-10	
9	С2000-КТ	18	
10	С2000-ИК	19	
11	С2000-СТИК	20-21	
12	С2000-ПИК	22	
13	С2000-СМК	23	

### Литература

1. Руководство пользователя RProg – М. : Изд-во «ЗАО НВП "Болид"» - 2012.
2. Контроллер доступа "С2000-2". Руководство по эксплуатации АЦДР.425723.001 РЭ – М. : Изд-во «ЗАО НВП "Болид"» - 2012.