

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине «Организационное и правовое обеспечение информационной безопасности»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

СОДЕРЖАНИЕ

ТЕМА 1. ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ	5
Практическая работа №1-6.....	5
ТЕМА 2. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТДЕЛЬНЫХ ВИДОВ ИНФОРМАЦИИ.....	46
Практическая работа №7-12.....	46
ТЕМА 3. СИСТЕМА ОРГАНОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	57
Практическая работа №13-14.....	57
ТЕМА 4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ	70
Практическая работа №15-16.....	70
7 СЕМЕСТР	80
ТЕМА 1. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА	80
Практическая работа №1-6.....	80
ТЕМА 2. ОРГАНИЗАЦИЯ СЛУЖБЫ БЕЗОПАСНОСТИ ОБЪЕКТА	100
Практическая работа №7-12.....	100
ТЕМА 3. ОРГАНИЗАЦИЯ ВНУТРИОБЪЕКТНОГО РЕЖИМА	105
ТЕМА 4. ОХРАНА ОБЪЕКТОВ.....	105
Практическая работа №13-18.....	105
ТЕМА 5. ПОДБОР СОТРУДНИКОВ И РАБОТА С КАДРАМИ	120
ТЕМА 6. ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ РЕЖИМА СЕКРЕТНОСТИ НА ОБЪЕКТЕ.....	120
Практическая работа №19-20.....	120

Введение

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины: является формирование знаний по организационно-правовому обеспечению информационной безопасности и навыков по их определению необходимых специалисту в области информационной безопасности.

Задачи освоения дисциплины:

1. Выявление угроз информационной безопасности объекта;
2. Организация службы безопасности объекта;
3. Подбор и работа с кадрами в сфере информационной безопасности;
4. Организация и обеспечение режима конфиденциальности.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИД-1 _{ОПК-5} Знаком с действующим законодательством Российской Федерации в области информационной безопасности и защиты информации; системами защиты государственной тайны; определяет перечень сведений, относящихся к конфиденциальной информации и способы ее защиты; знаком с понятием и принципами электронной подписи (ЭП); определяет виды компьютерных вирусов; классифицирует компьютерные преступления; использует понятие и способы защиты интеллектуальной собственности; Знаком с действующим законодательством в области международного и российского права в области защиты информации; знаком со способами совершения преступлений в сфере компьютерной информации; знаком с правовыми режимами защиты информации.	Представление презентационного материала в области Законодательства Российской Федерации по информационной безопасности; системы защиты государственной тайны; перечень сведений, относящихся к конфиденциальной информации и способы ее защиты; понятие и принцип электронной подписи (ЭП); виды компьютерных вирусов; классификацию компьютерных преступлений; понятие и способы защиты интеллектуальной собственности; международное и российское право в области защиты информации; способы совершения преступлений в сфере компьютерной информации; правовые режимы защиты информации
	ИД-2 _{ОПК-5} Определяет рациональные меры по обеспечению организационной защите на объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	Составляет документированный отчет по представлению выбора мер по обеспечению организационной защиты на объекте. Строит организационную структуру работы персонала с конфиденциальной информацией.

	ИД-3 _{ОПК-5} Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Составляет отчет с проведенным анализом действующих нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1 _{ОПК-6} Знаком с нормативно-правовыми механизмами лицензирования, сертификации и аттестации; принципами организационного обеспечения информационной безопасности; основными угрозами информационной безопасности на объекте (в организации); порядком организации службы безопасности на объекте; типовыми структурами службы безопасности, ее основными задачами и функциями должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основами организационной защиты информации, ее современные проблемы и терминологию; основными руководящими документами по обеспечению режима и конфиденциальности на объекте; основными документами, регламентирующими организационную безопасность на объекте.	Разработал и описал детальный проект по обеспечению информационной безопасности согласно нормативно-правовым механизмам лицензирования, сертификации и аттестации; принципам организационного обеспечения информационной безопасности; основным документам по обеспечению режима и конфиденциальности на объекте; основным документам, регламентирующим организационную безопасность на объекте. Учитывая основные угрозы информационной безопасности на объекте (в организации); порядок организации службы безопасности на объекте; типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; роль персонала в обеспечении информационной безопасности на объекте; основы организационной защиты информации, ее современные проблемы и терминологию
	ИД-3 _{ОПК-6} Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Предоставляет детальный отчет с демонстрацией способности при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

ТЕМА 1. ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Практическая работа №1-6

Правовые основы информационной безопасности Российской Федерации

Цель: ознакомиться с назначением системы охранно-пожарной сигнализации, рассмотреть существующие способы построения систем ОПС,

изучить функциональную структуру системы ОПС на базе
оборудования

«КОДОС», научиться настраивать систему ОПС на базе прибора
ППКОП

«КОДОС А-20».

Теоретическое обоснование

Системы охранно-пожарной сигнализации (ОПС) в том или ином виде используются сегодня практически на всех объектах. Это связано с тем, что использование электроники, в конечном счете, всегда выгоднее, чем использование охранников.

Системы охранно-пожарной сигнализации предназначены для определения факта несанкционированного проникновения на охраняемый объект или появления признаков пожара, выдачи сигнала тревоги и включения исполнительных устройств (световых и звуковых оповещателей, реле и т. п.).

Системы охранной и пожарной сигнализации по идеологии построения очень близки друг другу и на небольших объектах, как правило, бывают совмещены на базе единого контрольного блока – прибора приемно-контрольного (ППК)

или контрольной панели (КП). В целом эти системы включают в себя:

технические средства обнаружения (извещатели);
технические средства сбора и обработки информации (приборы приемно-контрольные, системы передачи извещений и т. п.);
технические средства оповещения (звуковые и световые оповещатели, модемы и т. п.).

Рассмотрим более подробно каждую из составляющих системы ОПС.

Технические средства обнаружения – это извещатели, построенные на различных физических принципах действия. Извещатель - это устройство, формирующее определенный сигнал при изменении того или иного контролируемого параметра окружающей среды. По области применения извещатели делятся на охранные, охранно-пожарные и пожарные. В настоящее время охранно-пожарные извещатели практически не выпускаются и не применяются. Охранные извещатели по виду контролируемой зоны подразделяются на точечные, линейные, поверхностные и объемные. По принципу действия - на электроконтактные, магнитоконтактные, ударноконтактные, пьезоэлектрические, оптико-электронные, емкостные, звуковые, ультразвуковые, радиоволновые, комбинированные, совмещенные и др.

Пожарные извещатели делятся на извещатели ручного и автоматического действия. Автоматические пожарные извещатели подразделяются на тепловые,

реагирующие на повышение температуры, дымовые, реагирующие на появление дыма, и пламени, реагирующие на оптическое излучение открытого пламени.

Электроконтактные извещатели - самый простой тип охранных извещателей. Они представляют собой тонкий металлический проводник (фольга, провод), специальным образом закрепленный на защищаемом предмете или конструкции. Предназначены для защиты строительных

конструкций (стекла, двери, люки, ворота, некапитальные перегородки, стены и т.п.) от несанкционированного проникновения через них путем разрушения.

Магнитоконтактные (контактные) извещатели предназначены для блокировки различных строительных конструкций на открывание (двери, окна, люки, ворота и т. п.). Магнитоконтактный извещатель состоит из герметизированного магнитоуправляемого контакта (геркона) и магнита в пластмассовом или металлическом немагнитном корпусе. Магнит устанавливается на подвижной (открывающейся) части строительной конструкции (полотно двери, створка окна и т. п.), а магнитоуправляемый контакт - на неподвижной (коробка двери, рама окна и т.п.). Для блокировки больших открывающихся конструкций (раздвижные и распашные ворота), имеющих значительные люфты, применяются электроконтактные извещатели типа путевых конечных выключателей.

Ударноконтактные извещатели предназначены для блокировки различных остекленных конструкций (окна, витрины, витражи и т.п.) на разбитие. Извещатели состоят из блока обработки сигнала (БОС) и от 5 до 15 датчиков разбития стекла (ДРС). Место расположения составных частей извещателей (БОС и ДРС) определяется количеством, взаимным расположением и площадью блокируемых стеклянных полотен.

Пьезоэлектрические извещатели предназначены для блокировки строительных конструкций (стены, пол, потолок и т.п.) и отдельных предметов (сейфы, металлические шкафы, банкоматы и т. п.) на разрушение. При определении количества извещателей этого типа и места их установки на защищаемой конструкции необходимо учитывать, что возможно использовать их со 100% или 75%-м охватом блокируемой площади. Площадь каждого незащищенного участка блокируемой поверхности не должна превышать $0,1 \text{ м}^2$.

Оптико-электронные извещатели подразделяются на активные и пассивные. Активные оптико-электронные извещатели формируют тревожное извещение при изменении отраженного потока (однопозиционные извещатели)

или прекращении (изменении) принимаемого потока (двухпозиционные извещатели) энергии инфракрасного излучения, вызванного движением нарушителя в зоне обнаружения. Зона обнаружения таких извещателей имеет вид "лучевого барьера", образованного одним или несколькими расположенными в вертикальной плоскости параллельными узконаправленными лучами. Зоны обнаружения разных извещателей различаются, как правило, длиной и количеством лучей. Конструктивно активные оптико-электронные извещатели, как правило, состоят из двухмногоярусная;

отдельных блоков - блока излучения (БИ) и блока приемника (БП),

разнесенных на рабочее расстояние (дальность действия).

Активные оптико-электронные извещатели применяют для защиты внутренних и внешних периметров, окон, витрин и подступов к отдельным предметам (сейфам, музейным экспонатам и т.п.).

Пассивные оптико-электронные извещатели имеют наиболее широкое распространение, поскольку, с помощью специально разработанных для них оптических систем (линз Френеля), можно просто и быстро получать зоны обнаружения различной формы и размеров и использовать их для защиты помещений любой конфигурации, строительных конструкций и отдельных предметов.

Принцип действия извещателей основан на регистрации разницы между интенсивностью инфракрасного излучения, исходящего от тела человека, и фоновой температурой окружающей среды. Чувствительным элементом извещателей является пироэлектрический преобразователь (пироприемник), на котором фокусируется инфракрасное излучение с помощью зеркальной или линзовой оптической системы (последние наиболее широко распространены).

Зона обнаружения извещателя представляет собой пространственную дискретную систему, состоящую из элементарных чувствительных зон в виде лучей, расположенных в один или несколько ярусов или в виде тонких

широких пластин, расположенных в вертикальной плоскости (типа "занавес").

Условно зоны обнаружения извещателей можно разделить на семь следующих видов: широкоугольная одноярусная типа "веер"; широкоугольная многоярусная; узконаправленная типа "занавес", узконаправленная типа

"лучевой барьер"; панорамная одноярусная; панорамная конусная многоярусная.

Благодаря возможности формирования зон обнаружения различной конфигурации, пассивные инфракрасные оптико-электронные извещатели имеют универсальное применение и могут использоваться для блокировки объемов помещений, мест сосредоточения ценностей, коридоров, внутренних

периметров, проходов между стеллажами, оконных и дверных проемов, полов,

потолков, помещений с наличием мелких животных, складских помещений и т.п.

Емкостные извещатели предназначены для блокировки металлических шкафов, сейфов, отдельных предметов, создания защитных заграждений.

Принцип действия извещателей основан на изменении электрической емкости чувствительного элемента (антенны) при приближении или касании человеком охраняемого предмета. При этом охраняемый предмет должен устанавливаться на полу с хорошим изоляционным покрытием или на изолирующей прокладке.

К одному извещателю в помещении допускается подключать несколько металлических сейфов или шкафов. Количество подключаемых предметов зависит от их емкости, конструктивных особенностей помещения и уточняется при настройке извещателя.

Звуковые (акустические) извещатели предназначены для блокировки остекленных конструкций (окон, витрин, витражей и т.п.) на разбитие.

Принцип работы данных извещателей основан на бесконтактном методе

акустического контроля разрушения стеклянного полотна по возникающим при его разрушении колебаниям в звуковом диапазоне частот и распространяющихся по воздуху.

При установке извещателя все участки охраняемой остекленной конструкции должны быть в пределах его прямого обзора.

Ультразвуковые извещатели предназначены для блокировки объемов закрытых помещений, Принцип работы извещателей основан на регистрации возмущений поля упругих волн ультразвукового диапазона, создаваемого специальными излучателями, при движении в зоне обнаружения человека. Зона обнаружения извещателя имеет форму эллипсоида вращения или каплевидную форму.

Из-за низкой помехоустойчивости в настоящее время практически не используются. **Радиоволновые извещатели** предназначены для защиты объемов закрытых помещений, внутренних и внешних периметров, отдельных предметов и строительных конструкций, открытых площадок. Принцип работы радиоволновых извещателей основан на регистрации возмущений электромагнитных волн СВЧ диапазона, излучаемых передатчиком и регистрируемых приемником извещателя при движении человека в зоне обнаружения. Зона обнаружения извещателя (как и у ультразвуковых извещателей) имеет форму эллипсоида вращения или каплевидную форму, Зоны обнаружения разных извещателей различаются только размерами.

Радиоволновые извещатели бывают одно- и двухпозиционные.

Однопозиционные извещатели применяют для защиты объемов закрытых помещений и открытых площадок. Двухпозиционные - для защиты периметров.

При выборе, установке и эксплуатации радиоволновых извещателей следует помнить об одной их особенности. Для электромагнитных волн СВЧ диапазона некоторые строительные материалы и конструкции не являются препятствием (экраном) и они свободно, с некоторым ослаблением, проникают сквозь них. Поэтому зона обнаружения радиоволнового

извещателя может выходить, в некоторых случаях, за пределы охраняемого помещения, что может вызвать ложные срабатывания. К таким материалам и конструкциям относятся, например, тонкие гипсокартонные перегородки, окна, деревянные и пластиковые двери и т.п. Поэтому радиоволновые извещатели не следует ориентировать на оконные проемы, тонкие стены и перегородки, за которыми в период охраны возможно движение крупногабаритных предметов и людей. Не рекомендуется их применять на объектах, вблизи которых расположены мощные радиопередающие средства.

Комбинированные извещатели представляют собой сочетание двух извещателей, построенных на разных физических принципах обнаружения, объединенных конструктивно и схемно в одном корпусе. Причем схемно они объединены по схеме "и", т. е. только при срабатывании обоих извещателей формируется тревожное извещение. Наиболее широко распространена комбинация инфракрасного пассивного и радиоволнового извещателей.

Комбинированные охранные извещатели обладают очень высокой помехоустойчивостью и используются для защиты помещений объектов со сложной помеховой обстановкой, где применение извещателей других типов невозможно или неэффективно.

Совмещенные извещатели представляют собой два извещателя, построенных на разных физических принципах обнаружения, объединенных конструктивно в одном корпусе. Каждый извещатель работает независимо от другого и имеет свою зону обнаружения и свой собственный выход для подключения к шлейфу сигнализации. Наиболее широко распространена комбинация инфракрасных пассивных и звуковых извещателей. Встречаются и другие комбинации.

Извещатели тревожной сигнализации предназначены для ручной или автоматической подачи тревожного извещения на внутренний пультахраны объекта или в органы внутренних дел в случаях возможного преступного нападения на сотрудников, клиентов или посетителей объекта.

В качестве извещателей тревожной сигнализации используются различные кнопки и педали ручного и ногового действия на основе магнито- и

электроконтактных извещателей. Как правило, такие извещатели имеют фиксацию в нажатом состоянии и возврат в исходное положение возможен только с помощью ключа.

В тех же целях разработаны и применяются специальные мини-системы тревожной сигнализации, работающие по радиоканалу. В их состав входит приемник, подключаемый к прибору приемно-контрольному или контрольной панели, и несколько носимых брелоков-передатчиков для беспроводной передачи тревожных извещений. В состав некоторых релоков входит датчик падения. Дальность действия таких систем составляет от нескольких десятков до нескольких сотен метров. Особое место среди извещателей тревожной сигнализации занимают извещатели-ловушки. Они предназначены для подачи тревожного извещения при попытке хищения денег или ограбления охраняемого объекта независимо от действий персонала. Они представляют собой имитацию пачки денег в банковской упаковке объемом 100 купюр, в которую вмонтирован магнит, а в специальную подставку, на которой располагается пачка, магнитный датчик (геркон).

При изъятии (перемещении) имитационной пачки денег с подставки происходит размыкание контактов магнитного датчика и на пульт охраны объекта поступает тревожное извещение. Существуют аналогичные извещатели-ловушки, куда совместно с магнитом встроен специальный патрон,

содержащий цветной (оранжевый) дым, объемом 5 м.² Дымовая композиция распыляется с временной задержкой (3 мин.) после срабатывания магнитного датчика.

Пожарный извещатель – устройство для формирования сигнала о пожаре. Использование термина «датчик» является неправильным, так как датчик — это часть извещателя. Несмотря на это, термин «датчик» используется во многих отраслевых нормах, в значении «извещатель».

Условное обозначение пожарных извещателей должно состоять из следующих элементов: ИП X1X2X3-X4-X5.

Аббревиатура ИП определяет наименование «извещатель пожарный».

Элемент Х1 – обозначает контролируемый признак пожара; вместо Х1 приводят одно из следующих цифровых обозначений:

1 – тепловой; 2 – дымовой; 3 – пламени; 4 – газовый; 5 – ручной; 6...8 – резерв;

9 – при контроле других признаков пожара.

10 Элемент Х2Х3 обозначает принцип действия ПИ; вместо Х2Х3 приводят одно из следующих цифровых обозначений:

01 – с использованием зависимости электрического сопротивления элементов от температуры;

02 – с использованием термо-ЭДС; 03 – с использованием линейного расширения;

04 – с использованием плавких или сгораемых вставок;

05 – с использованием зависимости магнитной индукции от температуры;

06 – с использованием эффекта Холла; 07 – с использованием объемного расширения (жидкости, газа);

08 – с использованием сегнетоэлектриков; 09 – с использованием зависимости модуля упругости от температуры;

11 – с использованием резонансно-акустических методов контроля температуры;

12 – радиоизотопный; 12 – оптический;

13 – электроиндукционный; 14 – с использованием эффекта «памяти формы»;

15...28 – резерв;

29 – ультрафиолетовый; 30 – инфракрасный;

31 – термобарометрический;

32 – с использованием материалов, изменяющих оптическую проводимость в зависимости от температуры;

33 – аэроионный; 34 – термошумовой;

35 – при использовании других принципов действия.

Элемент Х4 обозначает порядковый номер разработки извещателя данного типа.

Элемент Х5 обозначает класс извещателя.

Автоматические пожарные извещатели (ПИ) в зависимости от возможности их повторного включения после срабатывания делятся на следующие типы:

возвратные извещатели с возможностью повторного включения – извещатели, которые из состояния пожарной тревоги могут без замены каких либо узлов снова вернуться в состояние контроля, если только исчезли факторы, приведшие к их срабатыванию. Они подразделяются на типы:

- извещатели с автоматическим повторным включением – извещатели,

которые после срабатывания самостоятельно переключаются в состояние контроля;

- извещатели с дистанционным повторным включением – извещатели,

которые при помощи дистанционно подаваемой команды могут быть переведены в состояние контроля;

- извещатели с ручным включением – извещатели, которые при помощи ручного переключения на самом извещателе могут быть переведены в состояние контроля;

извещатели со сменными элементами – извещатели, которые после срабатывания могут быть переведены в состояние контроля лишь путем замены

некоторых элементов;

извещатели без возможности повторного включения (без заменяемых элементов) – извещатели, которые после срабатывания больше не могут быть переведены в состояние контроля.

Автоматические пожарные извещатели по типу передачи сигналов

делятся:

двухрежимные извещатели с одним выходом для передачи сигнала как об отсутствии так и наличии признаков пожара;

многорежимные извещатели с одним выходом для передачи ограниченного количества (более двух) типов сигналов о состоянии покоя,

пожарной тревоги или других возможных состояний;

аналоговые извещатели, которые предназначены для передачи сигнала о величине значения контролируемого ними признака пожара, или аналогового/цифрового сигнала, и который не является прямым сигналом пожарной тревоги.

Тепловые извещатели применяются, если на начальных стадиях пожара выделяется значительное количество теплоты, например в складах горючесмазочных материалов. Либо в случаях, когда применение других извещателей невозможно. Применение в административно – бытовых помещениях запрещено.

Поле наибольшей температуры располагается на расстоянии 10...23 см от потолка. Поэтому именно в этой области желательно располагать теплочувствительный элемент извещателя. Тепловой извещатель,

расположенный под потолком на высоте шести метров над очагом пожара сработает при тепловыделении пожара 420 кВт, а на высоте 10 метров — при

1,46 МВт.

Точечный

Извещатель, реагирующий на факторы пожара в компактной зоне.

Многоточечный

Тепловые многоточечные извещатели — это автоматические извещатели,

чувствительные элементы которых представляют собой совокупность точечных сенсоров дискретно расположенных на протяжении линии. Шаг их установки определяется требованиями нормативных документов и техническими характеристиками, указываемыми в технической документации на конкретное изделие. Линейный (термокабель)

Существует несколько типов линейных тепловых пожарных извещателей, конструктивно отличающихся друг от друга:

полупроводниковый — линейный тепловой пожарный извещатель, у

которого в качестве сенсора температуры используется покрытие проводов веществом, имеющим отрицательный температурный коэффициент. Данный вид термокабеля работает только в комплекте с электронным управляющим блоком. При воздействии температуры на любой участок термокабеля изменяется сопротивление в точке воздействия. С помощью управляющего

блока можно задать разные пороги температурного срабатывания;

механический — в качестве сенсора температуры данного извещателя используется герметичная металлическая трубка, заполненная газом, а также датчик давления, подключенный к электронному блоку управления. При воздействии температуры на любой участок сенсорной трубки изменяется внутреннее давление газа, значение которого регистрируется электронным блоком. Данный тип линейного теплового пожарного извещателя многократного действия. Длина рабочей части металлической трубки сенсора

имеет ограничение по длине до 300 метров.

электрохимический — линейный тепловой пожарный извещатель, у которого в качестве сенсора температуры используется термочувствительный материал, нанесенный на два механически напряженных провода (витая пара),

Под воздействием температуры термочувствительный слой размягчается, и

два проводника накоротко замыкаются.

Дымовые извещатели (рисунок 3.1) – извещатели, реагирующие на продукты горения, способные воздействовать на поглощающую или рассеивающую способность излучения в инфракрасном, ультрафиолетовом или видимом диапазонах спектра.



Рисунок 1 – Дымовой извещатель

Дымовые извещатели могут быть точечными, линейными,

аспирационными и автономными.

Применение

Признак, на который реагируют дымовые извещатели – дым. Наиболее распространенный тип извещателя. При защите системой пожарной сигнализации административно-бытовых помещений необходимо использовать только дымовые извещатели. Использование других типов извещателей в административно-бытовых помещениях запрещено.

Количество извещателей,

защищающих помещение зависит от размеров помещения, типа извещателя,

наличие систем (пожаротушения, дымоудаления, блокировки оборудования)

которыми управляет пожарная сигнализация.

До 70% пожаров возникает из тепловых микроочагов, развивающихся в условиях с недостаточным доступом к ним кислорода. Такое развитие очага,

сопровожающееся выделением продуктов горения и протекающее в течение нескольких часов, характерно для целлюлозосодержащих

материалов.

Обнаруживать подобные очаги наиболее эффективно регистрацией продуктов горения в небольших концентрациях. Это позволяют делать дымовые или газовые извещатели.

Дымовые извещатели, использующие оптические средства обнаружения, реагируют по-разному на дым разных цветов. В настоящее время производители предоставляют ограниченную информацию о реакции дымовых извещателей в технических характеристиках. Информация о реакции извещателя включает только номинальные значения реакции (чувствительности) на серый дым, а не чёрный. Часто указывается диапазон чувствительности вместо точного значения.

Точечный извещатель реагирует на факторы пожара в компактной зоне.

Принцип действия точечных оптических извещателей основан на рассеивании серым дымом инфракрасного излучения. Хорошо реагируют на серый дым,

выделяющийся при тлении на ранних стадиях пожара. Плохо реагирует на чёрный дым, поглощающий инфракрасное излучение.

Для периодического обслуживания извещателей необходимо разъёмное соединение, так называемая «розетка» с четырьмя контактами, к которой подключается дымовой извещатель. Для контроля отключения датчика от шлейфа существуют два отрицательных контакта, которые замыкаются при установке извещателя в розетку.

Во всех точечных дымовых оптических пожарных извещателях ИП 212-XX по классификации НПБ 76-98 используется эффект диффузного рассеивания излучения светодиода на частицах дыма. Светодиод располагается таким образом, чтобы исключить прямое попадание его излучения на фотодиод. При появлении частиц дыма часть излучения отражается от них и попадает на фотодиод. Для защиты от внешнего света оптопара – светодиод и фотодиод, размещаются в дымовой камере из

пластика чёрного цвета.

Экспериментальные исследования показали, что время обнаружения тестового очага пожара при расположении дымовых извещателей на расстоянии 0,3 м от потолка возрастает в 2..5 раз. А при установке извещателя

на расстоянии 1 м от перекрытия можно прогнозировать увеличение времени

определения пожара уже в 10..15 раз.

Когда разрабатывались первые советские оптические дымовые извещатели, не было специализированной элементной базы, стандартных светодиодов и фотодиодов. В дымовом фотоэлектрическом извещателе ИДФ-1М в качестве оптопары использовались лампы накаливания типа СГ24-1,2 и фоторезистор типа ФСК-Г1. Это определяло

низкие технические характеристики извещателя ИДФ-1М и слабую защиту от внешних воздействий: инерционность срабатывания при оптической плотности 15 – 20 %/м составляла 30 с, напряжение питания $27 \pm 0,5$ В, ток потребления более 50 мА, масса 0,6 кг, фоновая освещенность до 500 лк, скорость воздушного потока до 6 м/с.

В комбинированном дымо-тепловом извещателе ДИП-1 были применены светодиод и фотодиод, причем расположенные в вертикальной плоскости.

Использовалось уже не непрерывное излучение, а импульсное: длительность 30 мкс, частота 300 Гц. Для защиты от помех было применено синхронное детектирование, т.е. вход усилителя был открыт только во время излучения светодиода. Это обеспечило более высокую защиту от помех, чем в извещателе ИДФ-1М и значительно улучшило характеристики извещателя: инерционность снизилась до 5 с при оптической плотности 10%/м, т.е. в 2 раза меньшей, масса снизилась в 2 раза, допустимая фоновая освещенность увеличилась в 20 раз, до

10000 лк, допустимая скорость воздушного потока увеличилась до 10 м/с.
В

режиме "Пожар" включался светодиодный индикатор красного цвета. Для

передачи сигнала тревоги в извещателях ДИП-1 и ИДФ-1М использовалось реле, что определяло значительные токи потребления: более 40 мА в дежурном режиме и более 80 мА в тревоге, при напряжении питания $24 \pm 2,4$ В и необходимости использования отдельных сигнальных цепей и цепей питания.

Линейный – двухкомпонентный извещатель (рисунок 3.2) состоящий из блока приемника и блока излучателя (либо одного блока приемника-излучателя и отражателя) реагирует на появление дыма между блоком приемника и излучателя.



Рисунок 2 – Линейный извещатель

Устройство линейных дымовых пожарных извещателей основано на принципе ослабления электромагнитного потока между разнесенными в пространстве источником излучения и фотоприемником под воздействием частиц дыма. Прибор такого типа состоит из двух блоков, один из которых содержит источник оптического излучения, а другой – фотоприемник. Оба блока располагают на одной геометрической оси в зоне прямой видимости.

Особенностью всех линейных дымовых извещателей является функция самотестирования с передачей сигнала «Неисправность» приемно-

контрольному прибору. Из-за этой особенности правильным является применение только в знакопеременных шлейфах. Включение линейных извещателей в знакопостоянные шлейфы ведет к блокировке сигналом

«Неисправность» сигнала «Пожар», что противоречит НПБ 75.

В один из первых советских линейных извещателей имел название ДОП-1

и использовал в качестве источника света лампу накаливания СГ-24-1,2. В качестве фотоприемника использовался германиевый фотодиод. Извещатель состоял из приемно-передающего блока, служащего для излучения и приема светового луча, и светоотражателя, устанавливаемого перпендикулярно направленному световому лучу на требуемом расстоянии. Номинальное расстояние между приемно-передающим блоком и отражателем $2,5 \pm 0,1$ м.

Устройство фотолучевое ФЭУП-М советского производства состояло из излучателя и фотоприёмника инфракрасного луча.

Аспирационный извещатель (рисунок 3.3) использует принудительный отбор воздуха из защищаемого объема с мониторингом ультрачувствительными лазерными дымовыми извещателями обеспечивает сверхраннее обнаружение критической ситуации. Аспирационные дымовые пожарные извещатели позволяют защитить объекты, в которых невозможно непосредственно разместить пожарный извещатель.



Рисунок 3 – Аспирационный извещатель

Пожарный аспирационный извещатель применим в помещениях архивов,

музеев, складов, серверных, коммутаторных помещений электронных узлов связи, центров управления, «чистых» производственных зон, больничных помещений с высокотехнологичным диагностическим оборудованием,

телевизионных центров и радиовещательных станций, компьютерных залов и других помещений с дорогостоящим оборудованием. То есть для наиболее важных помещений, где хранятся материальные ценности или где огромны средства, вложенные в оборудование, либо где велик ущерб от остановки производства или прерывания функционирования, либо велика упущенная выгода от потери информации. На таких объектах крайне важно достоверно обнаружить и ликвидировать очаг на самой ранней стадии развития, на этапе тления – задолго до появления открытого огня, либо при возникновении перегрева отдельных компонент электронного устройства. При этом, учитывая,

что такие зоны обычно оснащены системой контроля температуры и влажности, в них производится фильтрация воздуха, имеется возможность значительно увеличить чувствительность пожарного извещателя, избежав при этом ложных срабатываний.

Недостатком аспирационных извещателей является их высокая стоимость.

Радиоизотопный извещатель – это дымовой пожарный извещатель,

который срабатывает вследствие воздействия продуктов горения на ионизационный ток внутренней рабочей камеры извещателя (рисунок 4).



Рисунок 4 – Радиозотопный извещатель

Принцип действия радиоизотопного извещателя основан на ионизации воздуха камеры при облучении его радиоактивным веществом. При введении в

такую камеру противоположно заряженных электродов возникает ионизационный ток. Заряженные частички «прилипают» к более тяжелым частичкам дыма, снижая свою подвижность – ионизационный ток уменьшается.

Его уменьшение до определенного значения извещатель воспринимает как сигнал «тревога». Подобный извещатель эффективен в дымах любой природы.

Однако наряду с описанными выше достоинствами, радиоизотопные извещатели имеют существенный недостаток, о котором не следует забывать.

Речь идет об использовании в конструкции извещателей источника радиоактивного излучения. В связи с этим возникают проблемы соблюдения мер безопасности при эксплуатации, хранении и транспортировке, а также утилизации извещателей после окончания срока эксплуатации. Эффективен для обнаружения возгораний сопровождающихся появлением так называемых «черных» видов дыма, характеризующихся высоким уровнем поглощения света.

В советских радиоизотопных извещателях (РИД-1, КИ) источником ионизации являлся радиоактивный изотоп плутония-239. Извещатели входят в первую группу потенциальной радиационной опасности.

Основным элементом радиоизотопного извещателя РИД-1 являются две ионизационные камеры, включенные последовательно. Точка соединения подключена к управляющему электроду тиратрона. Одна из камер является открытой, другая закрыта и выполняет роль компенсирующего элемента.

Ионизация воздуха в обеих камерах создается изотопом плутония. Под действием приложенного напряжения в камерах протекает ионизационный ток.

При попадании дыма в открытую камеру, её проводимость уменьшается, напряжение на обеих камерах перераспределяется, в результате чего возникает напряжение на управляющем электроде тиратрона. При достижении напряжения зажигания тиратрон начинает проводить ток. Увеличение потребления тока приводит к срабатыванию сигнализации. Встроенные в извещатель источники радиации не представляют опасности, так как излучение полностью поглощается в объеме ионизационными камерами. Опасность может возникнуть только при нарушении целостности источника излучения. Также в извещателе используется тиратрон ТХ11Г с незначительным количеством радиоактивного никеля, излучение поглощается объемом тиратрона и его стенками. Опасность может возникнуть при разбитии тиратрона.

Назначенным сроком службы радиоактивных источников извещателей составлял:

РИД-1; КИ-1; ДИ-1 – 6 лет;

РИД-6; РИД-6м и подобные – 10 лет.

Высокая чувствительность позволяет использовать радиоизотопные извещатели как составной компонент аспирационных извещателей. При прокачке через извещатель воздуха защищаемых помещений, он может обеспечивать подачу сигнала при появлении даже ничтожного количества дыма — от 0,1 мг/м³. При этом длина трубок для забора воздуха практически неограничивается. К примеру, практически всегда регистрирует факт воспламенения спичечной головки на входе воздухозаборной трубки длиной 100 м.

Принцип работы электроиндукционного извещателя: аэрозольные частицы засасываются из окружающей среды в цилиндрическую трубку (газоход) при помощи малогабаритного электрического насоса и попадают в зарядную камеру. Здесь, под воздействием униполярного коронного разряда, частицы приобретают объемный электрический заряд и, двигаясь далее по газоходу, попадают в измерительную камеру, где наводят на её

измерительном электроде электрический сигнал, пропорциональный объемному заряду частиц и, следовательно, их концентрации. Сигнал с измерительной камеры попадает в предварительный усилитель и далее в блок обработки и сравнения сигнала.

Датчик осуществляет селекцию сигнала по скорости, амплитуде и длительности и выдает информацию при превышении заданных порогов в виде замыкания контактного реле.

Электроиндукционные извещатели используются в системах пожарной сигнализации модулей «Заря» и «Пирс» МКС.

Извещатель пламени – извещатель, реагирующий на электромагнитное излучение пламени или тлеющего очага (рисунок 5).



Рисунок 5 – Извещатель пламени

Извещатели пламени применяются, как правило, для защиты зон, где необходима высокая эффективность обнаружения, поскольку

обнаружение пожара извещателями пламени происходит в начальной фазе пожара, когда температура в помещении ещё далека от значений, при которых срабатывают тепловые пожарные извещатели. Извещатели пламени обеспечивают возможность защиты зон со значительным теплообменом и открытых площадок, где невозможно применение тепловых и дымовых извещателей. Извещатели пламени применяются для организации контроля наличия перегретых поверхностей агрегатов при авариях, например, для обнаружения пожара в салоне автомобиля, под обшивкой агрегата, контроля наличия твердых фрагментов перегретого топлива на транспорте.

Ручной извещатель – устройство, предназначенное для ручного включения сигнала пожарной тревоги в системах пожарной сигнализации и пожаротушения. Ручные пожарные извещатели следует устанавливать на высоте 1,5 м от уровня земли или пола. Освещенность в месте установки ручного пожарного извещателя должна быть не менее 50 Лк.

Ручные пожарные извещатели должны устанавливаться на путях эвакуации в местах, доступных для их включения при возникновении пожара.

В сооружениях для наземного хранения легковоспламеняющихся и горючих жидкостей ручные извещатели устанавливаются на обваловке.

К 1900 году в Лондоне были установлены 675 ручных извещателей с выводом сигнала в пожарную службу. К 1936 году количество увеличилось до 1732.

В 1925 году в Ленинграде ручные извещатели были в 565 пунктах, они передали за 1924 год около 13% всех сообщений о пожарах в городе. В начале XX века существовали ручные извещатели, включаемые в кольцевой шлейф регистрирующего прибора. При включении извещатель производил индивидуальное количество замыканий и размыканий и таким образом передавал сигнал на аппарат Морзе, установленный на регистрирующем приборе. Ручные извещатели конструкции того времени состояли из часового механизма с маятниковым спуском, состоящим из двух главных зубчатых колес и сигнального колеса с тремя трущимися контактами. Механизм приводится в действие при помощи ленточной спиральной пружины, причем механизм извещателя, приведенный в действие, повторяет номер сигнала четыре раза.

Одного завода пружины хватает на подачу шести сигналов. Контактные части механизма, во избежание окисления, покрыты серебром. Этот тип сигнализации был предложен в 1924 г. Заведующим Мастерскими Пожарного Телеграфа Рюльманом А.Ф., аппараты которой и были в целях опыта установлены в 7-ми пунктах Центральной части города с приемной станцией в части им. т. Ленина.

Действие сигнализации было открыто 6 марта 1924 г. После десятимесячной опытной эксплуатации, показавшего, что не было случая неполучения

сигнала и что в работе сигнализации отмечается полное безотказное и точное действие, система была рекомендована к повсеместному применению.

К техническим средствам сбора и обработки информации относятся приборы приемно-контрольные, контрольные панели, сигнально-пусковые устройства, системы передачи извещений и т.п. Они предназначены для непрерывного сбора информации от технических средств обнаружения (извещателей), включенных в шлейфы сигнализации, анализа тревожной ситуации на объекте и ее отображения, управления местными световыми и звуковыми оповещателями, индикаторами и другими устройствами (реле, модем, передатчик и т. п.), а также формирования и передачи извещений о состоянии объекта на центральный пост или пульт централизованного наблюдения, Они же обеспечивают сдачу под охрану и снятие объекта (помещения) с охраны по принятой тактике, а также в ряде случаев электропитание извещателей.

Приборы приемно-контрольные классифицируются по информационной емкости (количеству контролируемых шлейфом сигнализации) на приборы малой (до 5 ШС), средней (от 6 до 50 ШС) и большой (свыше 50 ШС) информационной емкости. По информативности приборы могут быть малой (до 2-х видов извещений), средней (от 3 до 5 видов) и большой (свыше 5 видов) информативности.

Системы передачи извещений классифицируются по информационной емкости (количеству охраняемых объектов) на системы с постоянной информационной емкостью и с возможностью наращивания информационной емкости.

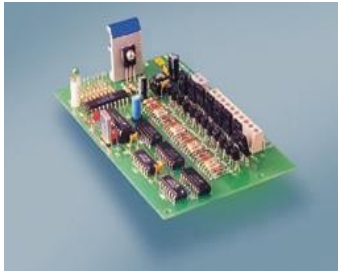
По информативности системы подразделяются на системы малой (до 2-х видов извещений), средней (от 3 до 5 видов) и большой (свыше 5) информативности.

По типу используемых линий (каналов) связи системы подразделяются на системы, использующие линии телефонной сети (в том числе переключаемые), специальные линии связи, радиоканалы, комбинированные линии связи и др. По количеству направлений передачи

информации они подразделяются на системы с одной- и двунаправленной передачей информации (с наличием обратного канала).

По алгоритму обслуживания объектов системы передачи сообщений подразделяются на неавтоматизированные системы с ручной тактикой взятия (снятия) объектов под охрану (с охраны) после ведения телефонных переговоров с дежурным пульта управления и автоматизированные с автоматическим взятием и снятием (без ведения телефонных переговоров). По способу отображения поступающей на пульт централизованного наблюдения информации системы передачи извещений подразделяются на системы с индивидуальным или групповым отображением информации в виде световых и звуковых сигналов, с отображением информации на дисплее с применением устройств обработки и накопления базы данных. Контрольные панели по основным решаемым задачам соответствуют отечественным приборам приемно-контрольным. Уточним также понятия зоны охраны (термин, применяемый в иностранной литературе) и шлейфа сигнализации, используемого в отечественной литературе.

Рассмотрим основные технические средства сбора и информации представленные в настоящее время на Адресные блоки

Наименование	Кол-во контролируемых шлейфов	Описание	Цена	Внешний вид
Эфес БАВП-8	до 8-ми	Блок предназначен для адресного приема и обработки информации от локальных шлейфов пожарной сигнализации и передачи информации на модуль адресной линии сигнализации МАЛС. Настройка режима работы блока БАВП-8 осуществляется с помощью специализированного программного обеспечения диагностики и настройки системы безопасности ДСБ-9.1.	2450 руб	
Эфес БАВП-4	До 4-х	БАВП-4 обеспечивает подключение четырех шлейфов пожарной сигнализации; прием и обработку информации от тепловых пожарных извещателей типа ИП-104-1, ИП-105-2/1, ручных пожарных извещателей типа ИПР с квитированием, извещателей дыма и пламени типа ИП-212-5, ИП-329-2, а также аналогичных им по техническим параметрам.	1680 руб	

Наименование	Кол-во контролируемых шлейфов	Описание	Цена	Внешний вид
Астра-712/2	До 2-х	контроль состояния 2 шлейфов сигнализации (ШС) с включенными охранными или пожарными извещателями; управление средствами оповещения; выдача тревожных извещений на ПЦН через релейные выходы; выдача информации по линии расширения на релейные модули Астра-821/822, модули индикации Астра-861, коммуникатор GSM Астра-882, радиопередающее устройство РПД Астра-РИ; обеспечение питающим напряжением активных извещателей и других устройств.	1247 руб	
Астра-712/4	До 4-х	контроль состояния 4 шлейфов сигнализации (ШС) с включенными охранными или пожарными извещателями; управление средствами оповещения; выдача тревожных извещений на ПЦН через релейные выходы; выдача информации по линии расширения на релейные модули Астра-821/822, модули индикации Астра-861, коммуникатор GSM Астра-882, радиопередающее устройство РПД Астра-РИ; обеспечение питающим напряжением активных извещателей и других устройств.	1548 руб	

Наименование	Кол-во контролируемых шлейфов	Описание	Цена	Внешний вид
Астра-712/8	До 8-х	контроль состояния 8 шлейфов сигнализации (ШС) с включенными охранными или пожарными извещателями; управление средствами оповещения; выдача тревожных извещений на ПЦН через релейные выходы; выдача информации по линии расширения на релейные модули Астра-821/822, модули индикации Астра-861, коммуникатор GSM Астра-882, радиопередающее устройство РПД Астра-РИ; обеспечение питающим напряжением активных извещателей и других устройств.	1730 руб	
КОДОС А-06/2**	До 2-х	контроль двух пожарных шлейфов; подключение датчиков типа «Пульсар»; передача на центральную панель сообщений: «норма», «тревога», «короткое замыкание» и «обрыв шлейфа»; подключение к ППКОП «КОДОС А-20» до 50 адресных блоков «КОДОС А-06/2»; питание от линии связи.	1000 руб.	
КОДОС А-07/8	До 8-ми	снабжен датчиком вскрытия корпуса; контроль за восемью охранными шлейфами, к которым может быть подключено большинство распространенных охранных датчиков с выходами «сухой контакт»; передача на центральную панель сообщений: «норма», «тревога», «короткое замыкание» и «обрыв шлейфа»; подключение к прибору «КОДОС А-20» до 25 адресных блоков «КОДОС А-07/8»; питание от линии связи с прибором «КОДОС А-20» либо от	2000 руб	

Наименование	Кол-во контролируемых шлейфов	Описание	Цена	Внешний вид
		внешнего источника.		

Адресные блоки управления

Наименование	Кол-во контролируемых шлейфов	Описание	Цена	Внешний вид
Эфес БА-РВ-3КЛ-12	До 3-х независимых релейных канала	БА-РВ-3КЛ обеспечивает подключение трех шлейфов с датчиками. В шкафах КСБ –ЭФЕС блок обеспечивает контроль состояния СББП. Блок имеет три независимых канала управления. Каждый канал имеет по две группы контактов: нормально замкнутый и нормально разомкнутый. В цепи переменного тока 220 В допускается коммутация цепей нагрузки с током до 1 А. В цепи постоянного тока 24 В допускается коммутация цепей нагрузки с током до 5 А.	850 руб	
"С2000-СП1"	До 4-х релейных канала	* Управление четырьмя реле по интерфейсу RS-485 * Программируемая логика управления реле позволяет: Управлять различными исполнительными устройствами (световые и звуковые оповещатели, электромагнитные замки и другие) Использовать реле для передачи извещений на	1000 руб	

Блоки индикации

Наименование	Кол-во контролируемых шлейфов	Описание	Цена	Внешний вид
Астра-861	8 светодиодных индикаторов	Выдача извещений на 8 светодиодных индикаторов по командам управляющего устройства. автоматическое определение типа подключенного управляющего устройства; двухцветная индикация извещений, состояния модуля индикации и управляющих устройств; звуковое сопровождение извещений; отключение звукового сигнализатора переключкой; возможность обновления программного обеспечения.	576 руб	
НВП Bolid "С2000-БИ"	60 двухцветных светодиодных индикаторов	60 двухцветных светодиодных индикаторов и 8 одноцветных светодиодных системных индикаторов Возможность отображения на каждом из 60 двухцветных индикаторов состояния контролируемого раздела (не подключен, взят, снят, невзят, тревога, тихая тревога, неисправность, внимание, пожар) Возможность отображения на 8 одноцветных светодиодных системных индикаторах приходящих на блок извещений (невзятие,	4179.00 р	

Сравнивая данные, представленные в таблицах, о продукции различных представителей можно сделать вывод о том, что продукция, выпускаемая под торговой маркой КОДОС, является наиболее оптимальным выбором для построения системы ОПС, так как она имеет хорошее отношение цена/качество и отвечает современным российским и международным стандартам. Рассмотрим более подробно состав и принцип работы системы ОПС, использующей технические средства сбора и обработки информации марки КОДОС.

Прибор приемно-контрольный охранно-пожарный (ППКОП) «КОДОС А-20» (далее – прибор А-20, панель А-20, пульт А-20 (рисунок 6)) предназначен для обнаружения появления признаков нарушителя на охраняемом объекте и подачи извещения о тревоге для принятия мер по задержанию нарушителя, а также для обнаружения пожара и подачи извещения о тревоге для принятия необходимых мер (включения, в том числе автоматического, системы пожаротушения, эвакуации персонала и т.д.).



Рисунок 6 – ППКОП КОДОС А-20

Основные функции системы ОПС:

а) регистрация, обработка и передача на центральный пункт наблюдения информации от шлейфов охранной и пожарной сигнализации;

- б) управление по заданным алгоритмам исполнительными устройствами систем пожаротушения и дымоудаления, а также оповещения и эвакуации;
- в) в случае работы в составе интегрированных комплексов - формирование управляющих сигналов для других систем безопасности (например, на включение камер видеонаблюдения, блокирования или разблокирования исполнительных устройств системы контроля и управления доступом и др.).

Центральным модулем управления Системой является прибор «КОДОС А-20», который имеет двухпроводную линию связи с периферийным оборудованием (адресную линию), к которой, в свою очередь, подключаются адресные блоки различных типов. Каждый адресный блок имеет аппаратный адрес, служащий для идентификации устройства в Системе. Адресные блоки контролируют охранные (пожарные) зоны через шлейфы сигнализации, управляют исполнительными устройствами через каналы управления, причем каждому входу сигнального адресного блока (см. ниже) ставится в соответствие одна охраняемая зона, каждому выходу адресного блока управления ставится в соответствие исполнительное устройство.

Прибор А-20 поочередно опрашивает адресные блоки, получая от них информацию о состоянии шлейфов (и, соответственно, зон и каналов), отображает ее в удобном для оператора виде, по заданным алгоритмам управляет исполнительными устройствами.

Система осуществляет контроль четырех состояний («Норма», «Тревога», «Короткое замыкание» и «Обрыв») как пожарных, так и охранных шлейфов, которые, в свою очередь, контролируют один или несколько датчиков, в зависимости от пожарных норм и токопотребления датчиков. В

Системе используются адресные блоки следующих типов:

а) сигнальные адресные блоки:

– «КОДОС А-06/2» (контролирует две пожарные зоны),

- «КОДОС А-06/8» (контролирует восемь пожарных зон);
- «КОДОС А-07/4» (контролирует четыре охранные зоны);
- «КОДОС А-07/8» (контролирует восемь охранных зон);
- «КОДОС А-09» (контролирует два ручных пожарных извещателя (ИПР-ЗСУ));

б) командные адресные блоки – «КОДОС АКП» (предназначен для ввода команд управления в Систему);

в) адресные блоки управления «КОДОС А-08» различных модификаций (каждый для включения / выключения двух исполнительных устройств):

- «КОДОС А-08»;
- «КОДОС А-08/24»,
- «КОДОС А-08/220»;
- «КОДОС А-08/220А».

Питание адресных блоков осуществляется преимущественно по адресной линии связи.

К сигнальным адресным блокам подключаются пожарные или охранные извещатели (датчики). В качестве пожарных извещателей в ОПС на базе прибора А-20 могут использоваться любые двухпроводные пожарные извещатели с питанием от сигнальной линии, принцип срабатывания которых основана дискретном уменьшении внутреннего сопротивления до величины, не превышающей некоторого порогового значения (например,

ИП212-46, ДИП-3 и др.). К адресному блоку «КОДОС А-09» подключаются ручные пожарные извещатели типа ИПР-ЗСУ. В качестве охранных извещателей применяются любые датчики типа «сухой контакт».

К адресным блокам управления подключаются исполнительные устройства. Такими устройствами могут быть световые и звуковые устройства оповещения (например, табло и сирены), устройства дымоудаления и пожаротушения, системы оповещения и управления эвакуацией (СОУЭ). Питание исполнительных устройств может осуществляться как от источников

постоянного тока с напряжением до 30 В, так и от источников переменного тока с напряжением 24 ... 265 В. Для питания адресных блоков «КОДОС А-08», «КОДОС А-08/220А» и «КОДОС А-08/24» используются внешние источники питания, что позволяет исключить возможность сброса управляющего сигнала при обрыве линии связи с прибором «КОДОС А-20».

Командный адресный блок «КОДОС АКП» позволяет поставить на охрану (снять с охраны) зоны Системы, объединенные в разделы, а также снять состояние тревоги, возникшее в разделе путем ввода пользователем кода соответствующей команды с клавиатуры блока.

Кроме адресной линии к прибору А-20 предусмотрено подключение сирены (для оповещения сотрудников охраны о возникновении в Системе тревожного события), выносных модулей индикации «КОДОС МИ-50» (рисунок 3.7), предназначенных для отображения состояния зон и каналов Системы, и считывателей постановки на охрану и снятия с охраны серии «КОДОС RD» (RD-1100, RD-1030, RD-1040). При установленных считывателях постановка зон Системы на охрану и снятие их с охраны возможны при помощи кодоносителей - электронных карт различных типов (например, типов HID, PHILIPS MIFARE и др.), подносимых к соответствующим считывателям. Считыватели постановки на охрану (снятия с охраны) могут также подключаться и к модулям индикации, дублируя функции считывателей, подключенных непосредственно к прибору А-20.



Рисунок 7 – Модуль индикации КОДОС МИ-50

Для передачи на пульт централизованного наблюдения (ПЦН) вневедомственной охраны МВД извещения о возникновении в системе ОПС тревожного события предусмотрено подключение к прибору А-20 оконечного устройства системы передачи извещений (УО СПИ).

Управление системой ОПС может осуществляться как с клавиатуры прибора А-20, так и дистанционным способом. Для этого предусмотрена возможность подключения прибора А-20 к персональному компьютеру (ПК).

Управление с ПК позволяет упростить интерфейс взаимодействия с Системой, а также предоставляет возможность ее интеграции, в случае необходимости, с другими системами безопасности. Для работы системы ОПС под управлением ПК разработано оригинальное программное обеспечение «КОДОС-ОПС».

Подключение прибора А-20 к ПК может осуществляться несколькими способами:

- 1) напрямую к ПК или через адаптеры «КОДОС АД-01»; в этих случаях связь осуществляется по протоколам RS-232 или RS-485;
- 2) при помощи сетевого контроллера «КОДОС СК-Е», который позволяет управлять Системой через сеть Ethernet или (при наличии в ЛВС выхода в глобальную сеть) посредством Интернета (рисунок 8).

Адресные блоки «КОДОС А-06/2» и «КОДОС А-06/8» предназначены для контроля состояния пожарных шлейфов («КЗ», «Тревога», «Норма», «Обрыв»), подключенных к токопотребляющим пожарным извещателям типа ИП212-46, ДИП-3, «Пульсар» и передачи информации в линию связи с прибором «КОДОС А-20»

Адресные блоки «КОДОС А-07/4» и «КОДОС А-07/8» предназначены для контроля состояния охранных шлейфов («КЗ», «Тревога», «Норма», «Обрыв»), подключенных к извещателям с выходами «сухой контакт», и

передачи информации в линию связи с прибором «КОДОС А-20» (рисунок 9).



Рисунок 8 – Сетевой контроллер «КОДОС СК-Е»



Рисунок 9 – Адресный блок «КОДОС А-07/8»

Адресный блок «КОДОС А-09» контролирует 2 ручных пожарных извещателя ИПР-3СУ и передает извещение о нажатии кнопки с индикацией подтверждения о получении сообщения (рисунок 10).

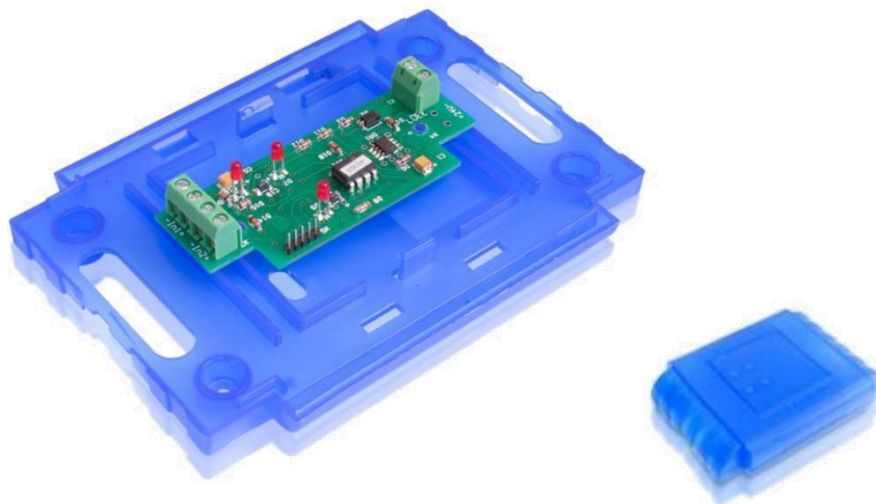


Рисунок 10 – Адресный блок «КОДОС А-09»

Изолятор линии «КОДОС ИЗЛ-01» предназначен для контроля состояния линии и отключения участка линии связи, находящегося за изолятором, в случае появления на нем КЗ. На кожухе изолятора линии расположены два светодиодных индикатора: №2 – «Питание», №3 – «Защита».

С помощью изолятора линии адресная линия разделяется на два участка: входной и выходной. Входной участок линии связи подключается к клеммам «+Lin-», а выходной – к клеммам «+Lout-» изолятора линии. Питание устройства осуществляется от линии связи с прибором А-20.

На одном луче линии связи может устанавливаться последовательно только один изолятор линии, так как в случае подключения нескольких изоляторов линии короткое замыкание на выходе любого изолятора вызовет отключение всех остальных подключенных к его выходу изоляторов линии.

Удлинитель линии связи «КОДОС УЛ-01» предназначен для увеличения длины линии связи прибора «КОДОС А-20» с адресными блоками (АБ) серии «КОДОС», а также для отключения части линии связи, находящейся за удлинителем, в случае ее короткого замыкания (КЗ) (рисунок 11). Устройство применяется в составе адресной охранно-пожарной системы на базе прибора приемно-контрольного охранно-пожарного ППКОП 01059-42/126-1 «КОДОС А-20».



Рисунок 11 – Удлинитель линии связи «КОДОС УЛ-01»

В процессе работы удлинитель линии связи выполняет следующие функции:

1. Передача и усиление сигналов при информационном обмене устройств входного и выходного участков линии связи.
2. Контроль короткого замыкания на выходном участке линии связи.

Отключает части линии, находящейся за удлинителем, в случае КЗ.

Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.

2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомиться с теоретическим материалом.
2. Выполнить классификацию оборудования охранно-пожарной сигнализации, составить сводную таблицу по результатам.
3. Провести классификацию видов извещателей, по результатам составить сводную таблицу.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполнения индивидуального задания лабораторной работы.
5. Вывод.

Контрольные вопросы

1. Что такое технические средства обнаружения?
2. Виды охранных извещателей?
3. Классификация пожарных извещателей?
4. Назначение и типы тепловых извещателей?
5. Назначение дымовых извещателей?
6. Назначение и виды оптических извещателей?

7. Принцип действия аспирационного извещателя?
8. Принцип действия радиоизотопного извещателя?
9. Принцип действия электроиндукционного извещателя?
10. Для чего предназначены извещатели пламени?
11. Ручные извещатели. Назначение?
12. Назначение, состав, функции «КОДОС А-20».
13. Типы адресных блоков используемых в системе «КОДОС А-20».

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П.,

Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.

8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

ТЕМА 2. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТДЕЛЬНЫХ ВИДОВ ИНФОРМАЦИИ

Практическая работа №7-12

Цель: ознакомиться с назначением системы охранно-пожарной сигнализации, рассмотреть существующие способы построения систем ОПС, изучить функциональную структуру системы ОПС на базе оборудования «КОДОС», научиться настраивать систему ОПС на базе прибора ППКОП «КОДОС А-20».

Теоретическое обоснование

Стенд ОПС на базе оборудования «КОДОС» представлен на рисунке 12.

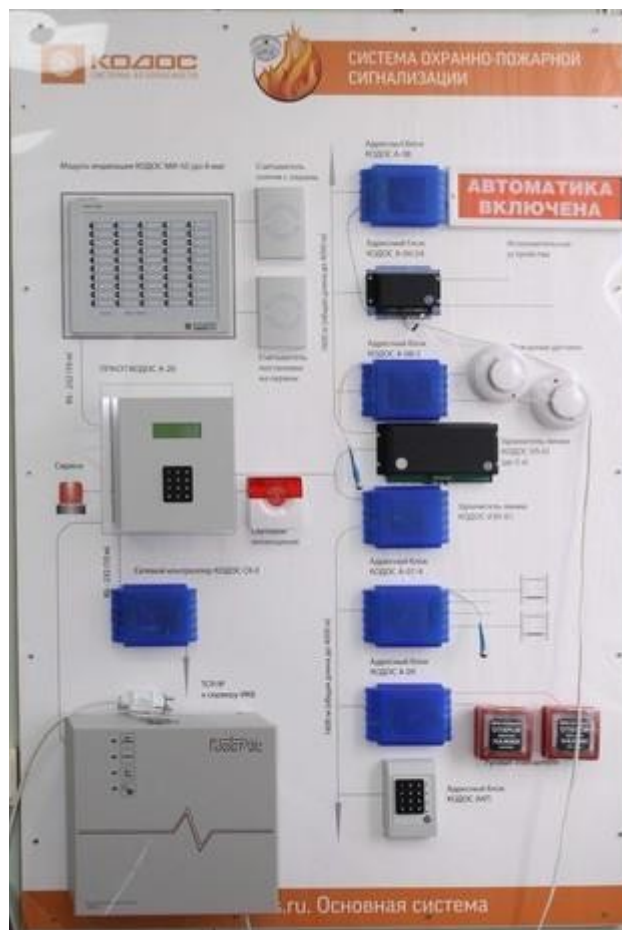


Рисунок 12 – Стенд охранно-пожарной сигнализации

На стенде установлено следующее оборудование:

- 1) Адресный блок СК-Е (IP-адрес: 192.168.31.251);
- 2) ППКОП «КОДОС А-20»;

- 3) Блок бесперебойного питания «КОДОС Р-01-3»;
- 4) Модуль индикации МИ-50 (аппаратный адрес: 23);
- 5) Адресный блок А-08 (аппаратный адрес: 56144);
- 6) Адресный блок А-08/24 (аппаратный адрес: 53961);
- 7) Адресный блок А-06/8 (аппаратный адрес: 53002);
- 8) Удлинитель линии УЛ-01;
- 9) Изолятор линии ИЗЛ-01;
- 10) Адресный блок А-07/4 (аппаратный адрес: 02298);
- 11) Адресный блок А-09 (аппаратный адрес: 61146);
- 12) Адресный блок АКП (аппаратный адрес: 44264).

Для того чтобы войти в меню настроек ППКОП «КОДОС А-20» необходимо нажать любую кнопку на панели ввода и далее ввести пароль пользователя, который осуществляет вход в систему.

По умолчанию у нового ППКОП «КОДОС А-20» в системе есть только один пользователь, который является администратором, его пароль 1111.

На лабораторном стенде пароль изменён на 0000(не меняется на 1111 при сбросе всех настроек).

Ввод данных подтверждается кнопкой #, отмена ошибочно введённых данных осуществляется кнопкой *.

Для сброса настроек необходимо выполнить следующие действия из основного меню А-20:

1. # прокрутка списка вниз
2. 5 настройка
3. # прокрутка списка вниз
4. 8 сброс

5. 1 сброс событий

6. #

Да

7. 2 сброс настроек

8. # Да

9. 3 очистка паролей

10. # Да

Первое что необходимо выполнить при настройке – создать список опроса, первым в списке должен быть указан адресный блок АКП.

Для создания списка опроса необходимо:

1. 5 – Настройка

2. 1 – Адресные блоки

3. 3 – Порядок опроса

4. 2 – Изменить список

Далее в порядке очередности вводим аппаратные адреса адресных блоков (аппаратный адрес указан на наклейке с обратной стороны адресного блока).

В методологии КОДОС изначально одна зона соответствует одному датчику (или исполнительному устройству), т.е. количество зон – это количество шлейфов в системе (учитываются даже незадействованные).

После формирования списка опроса необходимо задать количество зон.

1. 5 – Настройка

2. 1 – Адресные блоки

3. 1 число зон/каналов

4. вводим общее количество шлейфов и жмём #

Примечание: количество зон на лабораторном стенде 18.

Зоны нумеруются по следующему принципу (для примера у нас два адресных блока по 2 шлейфа): первый шлейф первого адресного блока будет первой зоной, второй шлейф первого адресного блока будет второй зоной, первый

шлейф второго адресного блока будет третьей зоной, второй шлейф второго блока будет четвёртой зоной. Порядок адресных блоков определяется списком опроса.

Настройка зон осуществляется из следующего меню:

2 зоны и каналы

1. 3 конф. зон и каналов
2. жмём 1 (настройка 1й зоны), затем #

Так можно попасть в меню настроек первой зоны. Меняя номер зоны на третьем шаге последовательности можно начать конфигурирование с любой зоны.

Для настройки доступны следующие параметры:

Зона на охране X

Инверсия

Контроль

Отлож. сраб. 00

Отлож. пост 00

Автопостановка

Для настройки канала доступны следующие параметры:

Канал активен

Контроль канала

Отлож. сраб. 00

Время работы 00

Зона на охране:

значение «зона поставлена на охрану» отмечается знаком «х». В случае срабатывания извещателей в зоне поставленной на охрану, система подает сигнал тревоги и выводит соответствующее сообщение на экран прибора.

значение «зона снята с охраны» отмечается снятием (отсутствием) метки.

Инверсия:

значение «извещатель зоны нормально-замкнутый (инверсный)» отмечается знаком «х». значение «извещатель зоны нормально-разомкнутый» отмечается снятием метки.

Контроль:

значение «контроль зоны включен» отмечается меткой «х».

Информация о состоянии данной зоны: «Норма», «Короткое замыкание», «Обрыв» выводится на экран прибора.

Отложенное срабатывание и отложенная постановка – задержка срабатывания охранного датчика и задержка поставки охранного датчика, соответственно. Диапазон значений от 0 до 255 секунд.

Автопостановка – прибор автоматически поставит зону на охрану после сброса тревоги в этой зоне. Для работы функции должен быть включен параметр «Зона на охране».

Важно: Функция автопостановки должна быть включена для всех охранных зон, действующих в группах.

Канал активен:

состояние «канал активен» отмечается знаком «х». Исполнительное устройство, подключенное к данному каналу управления, будет автоматически включаться при наступлении определенных событий.

состояние «канал неактивен» отмечается снятием (отсутствием)

метки. Включить исполнительное устройство данного канала сможет только пользователь.

Контроль канала:

состояние «контроль канала включен» отмечается знаком «х».

Система будет выводить информацию о состоянии данного канала («Включен», «Выключен») на экране прибора.

Отложенное срабатывание – задержка включения исполнительного устройства. Диапазон значений от 0 до 255 секунд.

Время работы – задает время работы исполнительного устройства. Диапазон значений от 1 до 255 секунд. 0 — непрерывная работа, выключить канал может только пользователь.

При установке настроек для зон, относящихся к адресному блоку А-06/8 установить время отложенного срабатывания 10 секунд.

Для управления стендом с АКП необходимо ввести пароль пользователя(4 цифры) и одну из 4-х команд:

«1» – поставить раздел на охрану,

«2» – снять раздел с охраны,

«3» – поставить раздел на охрану за исключением неисправных зон, «4»

– снять состояние тревоги, возникшее в разделе данного пользователя.

Сразу после нажатия 5-й цифры будет выполнена введенная операция.

Для включения модуля индикации МИ-50 необходимо выполнить: 5 –
Настройка

6 – Модули индикации Ввести номер согласно описанию рабочего

места# – записать изменения

* – нажать кнопку отмены 4 раза подряд, чтобы оставить пустыми значения для зон с 51-100, 101-150, 151-200

При правильной настройке и подключении светодиода «Связь с панелью» на МИ-50 начнут моргать.

Примечание: Мы можем подключить к А-20 до 8 панелей МИ-50. По одной основной и одной дополнительной на каждые 50 зон из 200

возможных.

Для включения исполнительного устройства необходимо:

Подайте из главного меню прибора команду: 2 - Зоны и каналы

2 - Включить/выключить На экране прибора появится запрос (рисунок 13):

Включить/выключить канал управления Канал:  Рисунок 13 – Запрос смены

состояния канала

Введите номер интересующего канала и нажмите клавишу #. Отменить неправильно набранный номер можно клавишей * (до нажатия клавиши #).

Нажмите соответствующую клавишу:

– включить канал управления (и, следовательно, включить устройство).

0 – выключить канал управления (и, следовательно, выключить устройство).

Прибор предложит перейти к включению/выключению следующего по порядку номеров канала. Это позволяет быстро включить или выключить сразу несколько каналов.

Нажмите клавишу * для возврата к запросу номера канала.

Повторное нажатие клавиши * вернет экран в меню «2.Зоны и каналы».

Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомится с теоретической частью лабораторной работы.
2. С разрешения преподавателя включить стенд ОПС.
3. Сбросить все настройки прибора ППКОП «КОДОС А-20».
4. Выполнить конфигурирование учебного стенда с блока управления прибора ППКОП «КОДОС А-20»:
добавить все адресные блоки; выполнить конфигурирование зон и каналов;
подключить модуль индикации МИ-50.
5. Проверить работоспособность настроенного стенда.

Внимание! При конфигурировании стенда адресный блок А-07/4 настраивать следующим образом:

- 1) первый шлейф настроить инверсным;
- 2) второй и третий шлейфы не использовать;
- 3) четвертый шлейф настроить как любой другой нормально разомкнутый датчик.

У всех нормально разомкнутых датчиков (все за исключением вышеупомянутого случая являются нормально разомкнутыми датчиками)

конфигурация должна быть следующей:

Зона на охране – вкл; Контроль – вкл; Автопостановка – вкл;

Отложенное срабатывание – 10 секунд (только пожарные шлейфы).

В настройках канала должны быть установлены следующие настройки:

Канал активен; Контроль канала;

Время работы – 60 сек. Проверка настроенного стенда осуществляется по следующей методике:

- 1) Модуль индикации МИ-50 должен отображать состояние 16 зон;
- 2) Блок А-20 должен выводить информацию о том, что 12 зон в норме и 4 канала активны;
- 3) Проверяется включение тревоги с тревожного извещателя (любой на выбор преподавателя);
- 4) Осуществляется снятие тревоги с блока А-20;
- 5) Проверяется включение тревоги с адресного блока А-07/4, используя эмуляцию датчика;
- 6) Осуществляется снятие тревоги с блока АКП;
- 7) Проверяется включение тревоги с адресного блока А-06/8, используя эмуляцию пожарного датчика в виде кнопки (А-20 должен сигнализировать, что в соответствующей зоне начался пожар);
- 8) Осуществляется снятие тревоги с блока АКП;
- 9) Включить одно из устройств управления (любое на выбор преподавателя).

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Схематично изобразить функциональную структуру стенда.
5. Описание выполненной работы (какие адресные блоки в каком порядке внесли, какие и как датчики настроили).
6. Краткое описание характеристик одного из адресных блоков (количество каналов, питание, для чего в основном используется, какие-то ограничения).
7. Вывод.

Контрольные вопросы

1. Назначение ППКОП «КОДОС А-20»
2. Опишите порядок подключения пожарных шлейфов для блока А-06/8
3. Дайте характеристику адресного блока А-07/4
4. Опишите общий порядок конфигурирования стенда.
5. Назовите порядок конфигурирования шлейфа адресного блока.
6. Назовите порядок настройки блока МИ-50.
7. Назовите порядок настройки блока АКП.
8. Назовите порядок снятия тревоги с использованием блока АКП.
9. Что означают свойства «Зона на охране» «Контроль», «Автопостановка», «Отложенное срабатывание»?
10. Что означают свойства «Канал активен», «Контроль канала»?

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш.учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.:Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

ТЕМА 3. СИСТЕМА ОРГАНОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Практическая работа №13-14

Цель: научиться настраивать систему ОПС на базе прибора ППКОП «КОДОС А-20» при помощи программного обеспечения КОДОС.

Теоретическое обоснование

Стенд ОПС на базе оборудования «КОДОС» представлен на рисунке 15.



Рисунок 15 – Стенд охранно-пожарной сигнализации

На стенде установлено следующее оборудование:

- 1) Адресный блок СК-Е (ip-адрес: 192.168.31.251);
- 2) ППКОП «КОДОС А-20»;
- 3) Блок бесперебойного питания «КОДОС Р-01-3»;
- 4) Модуль индикации МИ-50 (аппаратный адрес: 23);

- 5) Адресный блок А-08 (аппаратный адрес: 56144);
- 6) Адресный блок А-08/24 (аппаратный адрес: 53961); Адресный блок А-06/8 (аппаратный адрес: 53002);
- 7) Удлинитель линии УЛ-01;
- 8) Изолятор линии ИЗЛ-01;
- 9) Адресный блок А-07/4 (аппаратный адрес: 02298);
- 10) Адресный блок А-09 (аппаратный адрес: 61146);
- 11) Адресный блок АКП (аппаратный адрес: 44264).

Настройка ППКОП «КОДОС А-20» программным путём начинается с установки сетевого адреса контроллера СК-Е и проверки его доступности по сети. Для этого необходимо воспользоваться программой Confske

(«Конфигуратор СКЕ»).

После запуска утилиты необходимо нажать кнопку «Поиск» и дождаться результатов поиска.

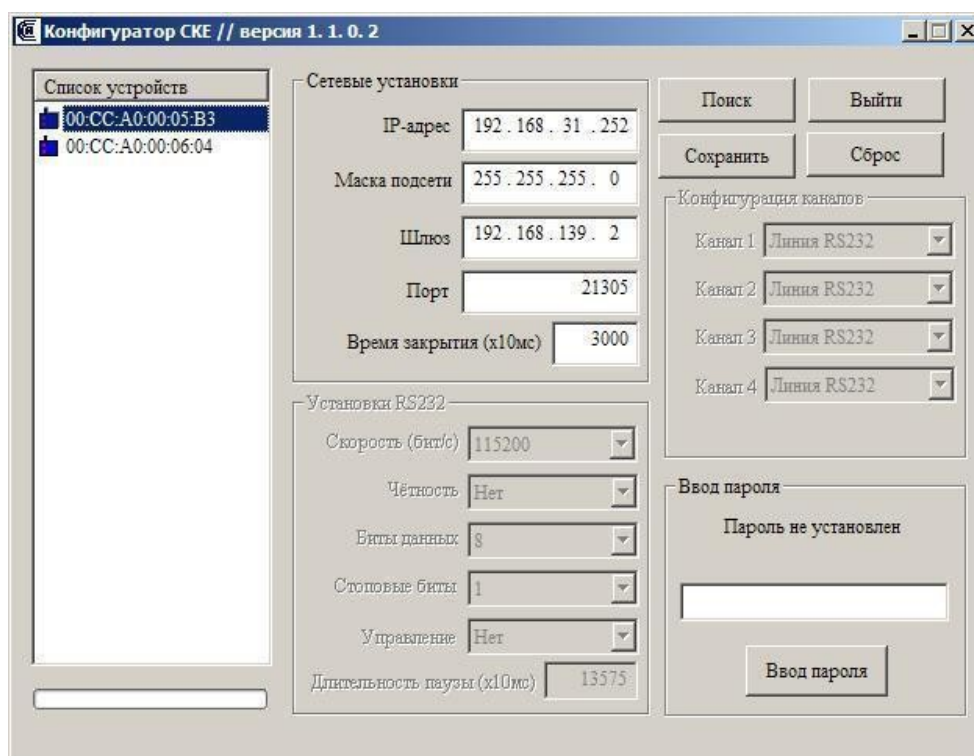


Рисунок 16 – Настройка сетевой контроллера «КОДОС СК-Е» при помощи утилиты «Confske»: информация о первом сетевом контроллере

Найденным контроллерам СК-Е с помощью данной утилиты можно назначить IP-адреса (в контексте выполнения лабораторной работы выполнять смену IP-адреса не нужно).

Если включён только стенд ОПС, то будет обнаружен только один контроллер, его IP-адрес должен быть 192.168.31.251.

Вторым этапом настройки является внесение изменений в файл hosts (данный файл расположен в директории «C:\WINDOWS\system32\drivers\etc»).

В данном файле необходимо задать соответствие IP-адреса АРМ на котором устанавливается данный программный комплекс и IP-адресов и сетевых имён сетевых контроллеров СК-Е.

Файл должен иметь структуру подобную той, что представлена на рисунке 17 (у вас должны быть указаны свои имена компьютеров и ip-адреса)

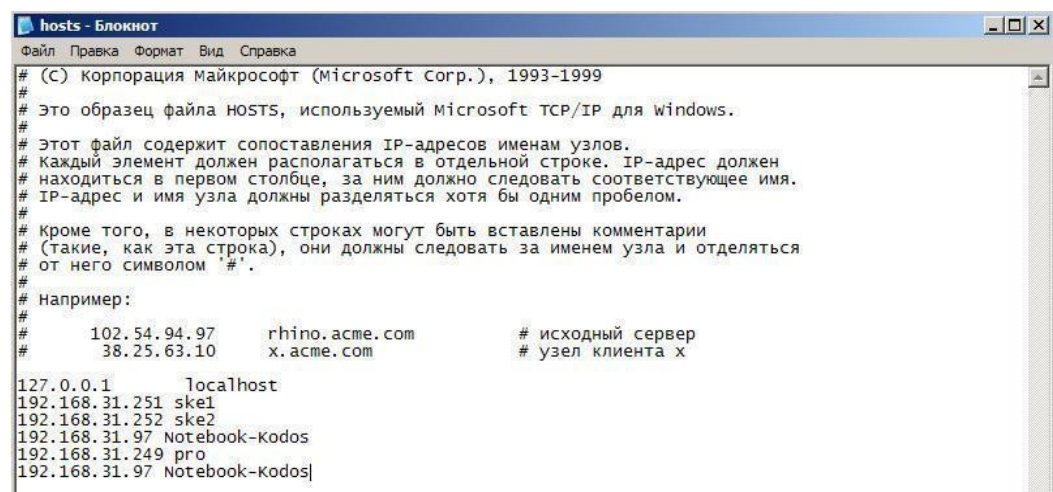


Рисунок 17 – Пример содержимого файла hosts

192.168.31.251 ske1 – IP-адрес и имя сетевого контроллера для ОПС КОДОС;

192.168.31.252 ske2 – IP-адрес и имя сетевого контроллера для СКУД КОДОС;

192.168.31.97 Notebook-Kodos – IP-адрес и имя АРМ, на котором устанавливается данный программный комплекс;

192.168.31.249 pro – IP-адрес и имя сетевого контроллера КОДОС-

ПРО;192.168.31. 97 Notebook-Kodos – IP-адрес и имя АРМ, на котором установлен GLOBOSS. Создание конфигурации программным путём для ППКОП «КОДОС А-20» осуществляется при помощи программы «Конфигуратор».

После запуска программы необходимо ввести следующие данные:

Логин 1: SYSDBA

Пароль 1: masterkey

Логин 2: ADMIN

Пароль 2: power

После запуска программы необходимо будет удалить имеющуюся конфигурацию, данное действие выполняется из контекстного меню ПК, таким образом, дерево с левой стороны экрана должно стать пустым. После удаления всех элементов можно приступить к конфигурированию.

Первое что необходимо сделать это добавить ПК на котором установлен данный программный комплекс (добавление элементов осуществляется через контекстное меню в левой части экрана, где была удалена текущая конфигурация).

Далее необходимо вызвать контекстное меню и указать следующие настройки (окно для задания параметров указано на рисунке 2.4):

- 1) Имя ПК на котором установлен программный комплекс КОДОС (имя указанное в файле hosts);
- 2) IP-адрес ПК на котором установлен программный комплекс КОДОС (IP-адрес указанный в файле hosts);
- 3) Выбрать рабочим COM-порт под номером COM 1;
- 4) Описание можно оставить неизменным, а можно изменить на любое название, данное поле используется исключительно для удобства создания конфигурации

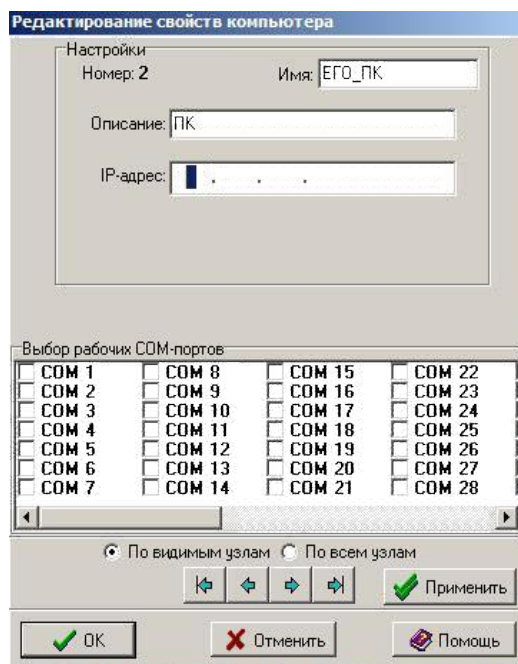


Рисунок 18 – Окно конфигурирования элемента ПК

После добавления ПК необходимо создать программную схему аналогичную смонтированной системе охраны. Порядок добавления адресных блоков будет определять порядок опроса на приборе.

Устройство ОПС таково, что сначала необходимо добавить сетевой контроллер (у контроллера необходимо указать IP-адрес и его имя, в соответствии с файлом hosts), потом к сетевому контроллеру добавить блок А-20, далее к блоку добавлять адресные блоки. После добавления адресного блока будет автоматически добавлено количество устройств/датчиков которые можно будет задействовать на данном устройстве, по умолчанию все шлейфы считаются незадействованными (свободными).

Параметры зон и каналов совпадают с настройками, осуществляемыми с блока управления А-20.

После создания конфигурации её необходимо сохранить Команды Сохранить конфигурацию.

Для загрузки конфигурации в панель А-20 необходимо вызвать правой кнопкой мыши контекстное меню на элементе схемы «ПУЛЬТ А20» и

выбрать пункт «Загрузить конфигурацию в панель», при запросе ответить «ДА» и далее дождаться окончания загрузки (в панели задач появится небольшой значок при наведении на него, можно убедиться, что процесс загрузки идёт).

По окончании загрузки конфигурации в панель необходимо будет вручную ввести аппаратный адрес модуля индикации, для того чтобы модуль индикации начал отображать состояние шлейфов (настроить модуль индикации из программы Конфигуратор невозможно).

Одной из особенностей прибора ППКОП «КОДОС А-20» является необходимость перезагрузки модуля после внесения глобальных изменений, таких как загрузка конфигурации или сброс настроек.

Мониторинг событий в системе построенной на оборудовании КОДОС осуществляется при помощи программы Сервер ИКБ, также с помощью этой программы осуществляются другие дополнительные действия, такие как управление устройствами, частичное изменение конфигурации А-20. Данная программа работает только с подключённым в USB-порт токеном.

Перед началом работы с программой «Сервер ИКБ» необходимо выполнить добавление лицензии.

Подключение ключа защиты к USB порту и его установку целесообразно осуществлять после окончания инсталляции программы ИКБ.

В случае сбоя программы при установке драйвера ключа защиты, установку драйвера можно осуществить через диспетчер внешних устройств D:\БАЗОВЫЙ КУРС\Утилиты КОДОС\ДРАЙВЕРА ДЛЯ КЛЮЧЕЙ ЗАЩИТЫ\SMKEYUSB.

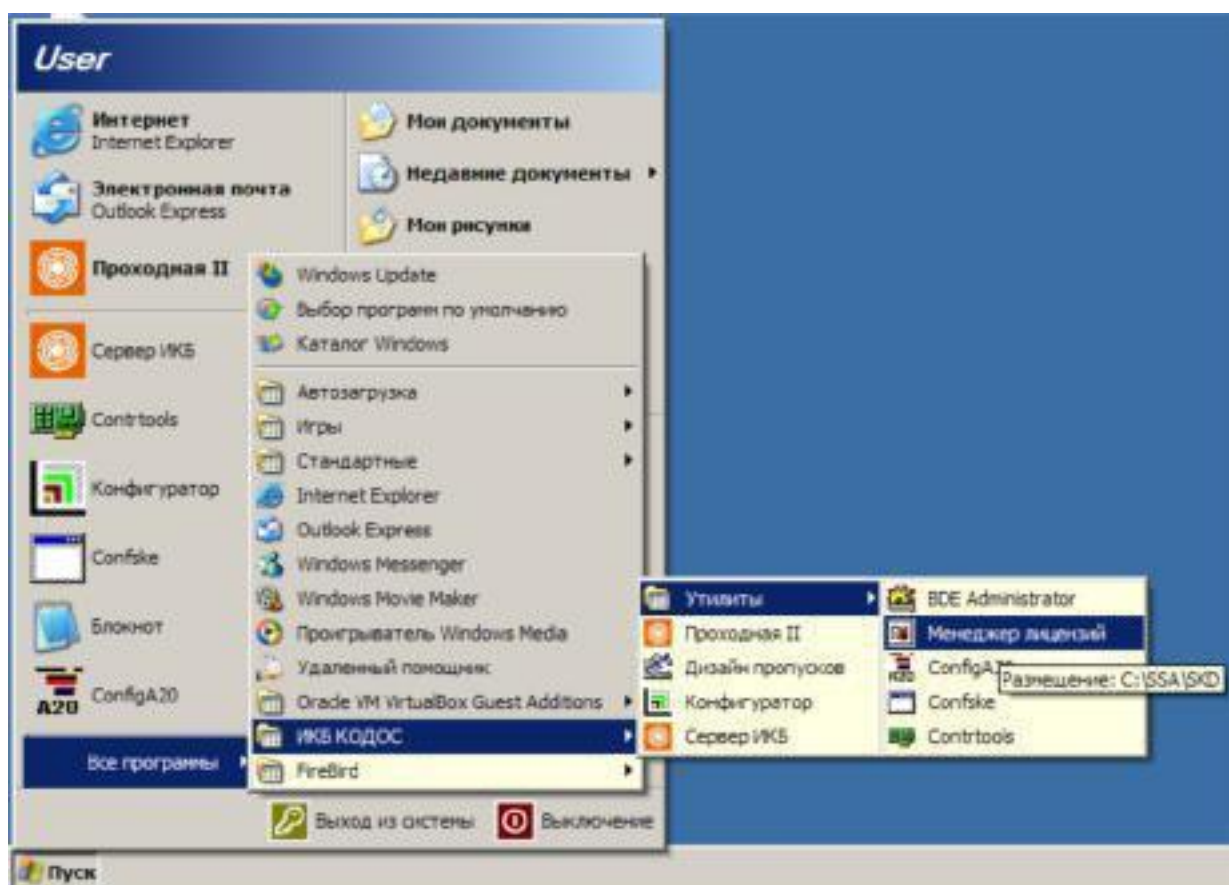


Рисунок 19 – Установка ключа защиты и лицензии: путь к «Менеджеру лицензий»

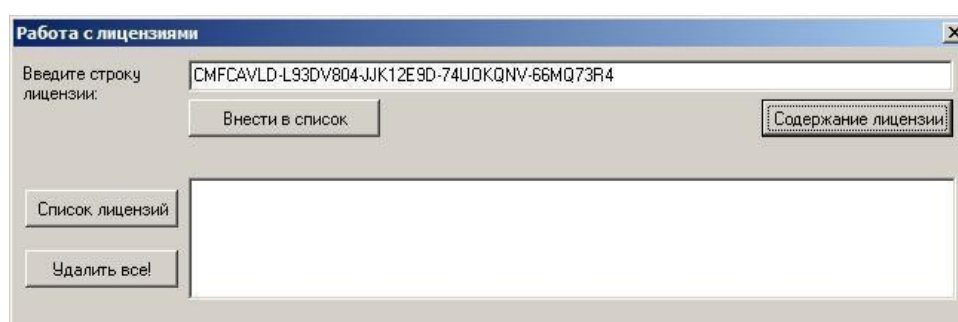


Рисунок 20 – Установка ключа защиты и лицензии: работа с лицензией

Что бы просмотреть информацию о лицензионном ключе надо нажать на кнопку «Содержание лицензии». После чего откроется информационное окно, представленное на рисунке 21.

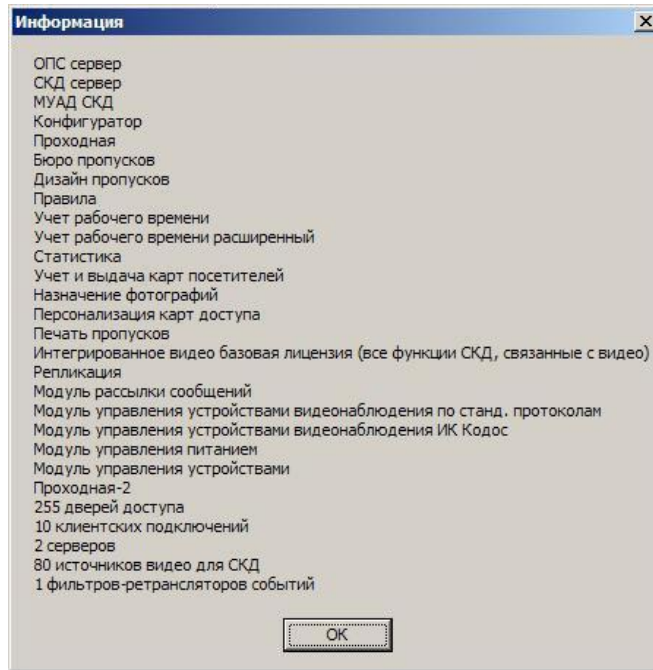


Рисунок 21 – Установка ключа защиты и лицензии: информация о лицензии

При нажатии «Внести в список» появится сообщение об успешной инсталляции лицензии и он отобразится в списке лицензий.

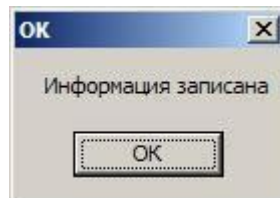


Рисунок 22 – Установка ключа защиты и лицензии: сообщение об успешной инсталляции лицензии

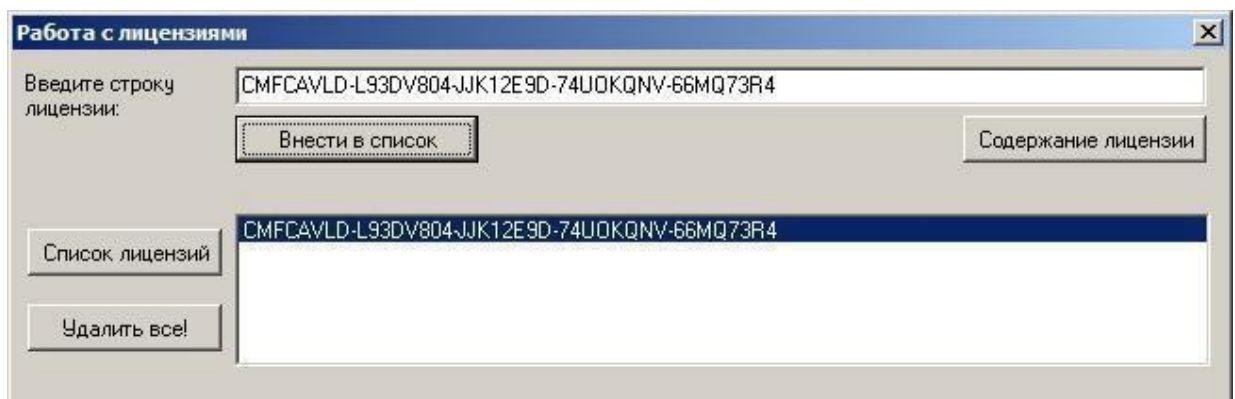


Рисунок 23 – Установка ключа защиты и лицензии: выбор лицензии

После добавления лицензии можно запустить «Сервер ИКБ».

После открытия программы появится стартовое окно

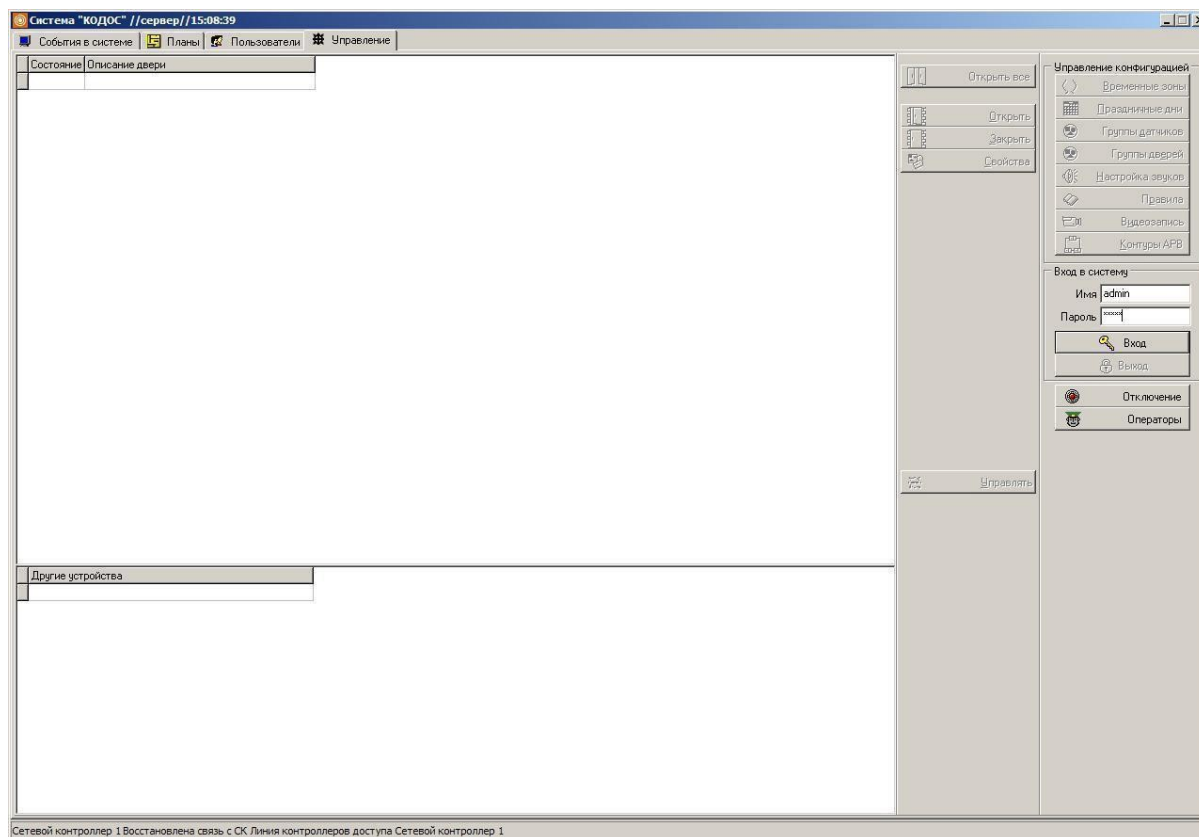


Рисунок 24 – Запуск программы «Сервер ИКБ»: стартовое окно

Для входа в систему необходимо ввести логин и пароль:

Логин: admin

Пароль: power

Далее после входа в систему на первой вкладке будут отображаться события в системе, данный список событий носит информативный характер и служит для оповещения о происходящих событиях.

На вкладке «Планы» указываются все планы помещений, созданные в программе «Конфигуратор».

На вкладке «Управление» можно осуществлять управление устройствами на стенде ОПС, для этого необходимо выбрать соответствующее устройство

(оно будет иметь имя, которое было задано в программе Конфигуратор) и нажать кнопку «Управлять», после чего откроется окно, где будет предоставлена возможность включить/отключить устройство.

На вкладке «Пользователи» осуществляется управление пользователями системы.

Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомится с теоретической частью лабораторной работы.
2. С разрешения преподавателя включить стенд ОПС.
3. Сбросить все настройки прибора ППКОП «КОДОС А-20».
4. Выполнить настройку программного обеспечения «КОДОС» на рабочем месте.
5. При помощи программы «Конфигуратор» создать схему ОПС и выполнить конфигурирование стенда при помощи программных средств.

6. Проверить работоспособность настроенного стенда.
7. При помощи программы «Сервер ИКБ» проверить работоспособность мониторинга событий в системе.
8. При помощи программы «Сервер ИКБ» включить одно из устройств установленных на стенде (по выбору преподавателя).
9. Добавить пользователя в систему, задав для пользователя в обязательном порядке пароль и код карты доступа.
10. Используя введенную карту доступа осуществить постановку и снятие с охраны системы.

Внимание! При конфигурировании стенда адресный блок А-07/4 настраивать следующим образом:

- 1) первый шлейф настроить инверсным;**
- 2) второй и третий шлейфы не использовать;**
- 3) четвертый шлейф настроить как любой другой нормально разомкнутый датчик.**

У всех нормально разомкнутых датчиков (все за исключением вышеупомянутого случая являются нормально разомкнутыми датчиками)

конфигурация должна быть следующей:

Зона на охране – вкл; Контроль – вкл; Автопостановка – вкл;

Отложенное срабатывание – 10 секунд (только пожарные шлейфы).

В настройках канала должны быть установлены следующие настройки:

Канал активен; Контроль канала;

Время работы – 60 сек. Проверка настроенного стенда осуществляется по следующей методике:

- 1) Модуль индикации МИ-50 должен отображать состояние 16 зон; Блок А-20 должен выводить информацию о том, что 12 зон в норме и 4 канала активны;
- 2) Проверяется включение тревоги с тревожного извещателя (любой на

выбор преподавателя);

- 3) Осуществляется снятие тревоги с блока А-20;
- 4) Проверяется включение тревоги с адресного блока А-07/4, используя эмуляцию датчика;
- 5) Осуществляется снятие тревоги с блока АКП;
- 6) Проверяется включение тревоги с адресного блока А-06/8, используя эмуляцию пожарного датчика в виде кнопки (А-20 должен сигнализировать, что в соответствующей зоне начался пожар);
- 7) Осуществляется снятие тревоги с блока АКП;
- 8) Включить одно из устройств управления (любое на выбор преподавателя).

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Схематичное изобразить функциональную схему стенда стенда.
5. Описание, назначение и выполняемые функции программ «Конфигуратор» и «Сервер ИКБ».
6. Краткое алгоритмическое описание выполненной работы.
7. Вывод

Контрольные вопросы

1. С чего начинается настройка ППКОП «КОДОС А-20» программным путём?

2. Для чего изменяем содержимое файла hosts?
3. Как выполнить добавление лицензии в модуле «Сервер ИКБ»?
4. Как осуществляется добавление нового пользователя в систему?
5. Перечислите способы загрузки конфигурации в модуль А-20.

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

ТЕМА 4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Практическая работа №15-16

Правовое регулирование деятельности по защите информации

Цель: научиться управлять конфигурацией пользователей оборудования ОПС; выполнить добавление нового пользователя с занесением в базу карты для считывания; выполнить конфигурирование ОПС задав условия включения устройств.

Теоретическое обоснование

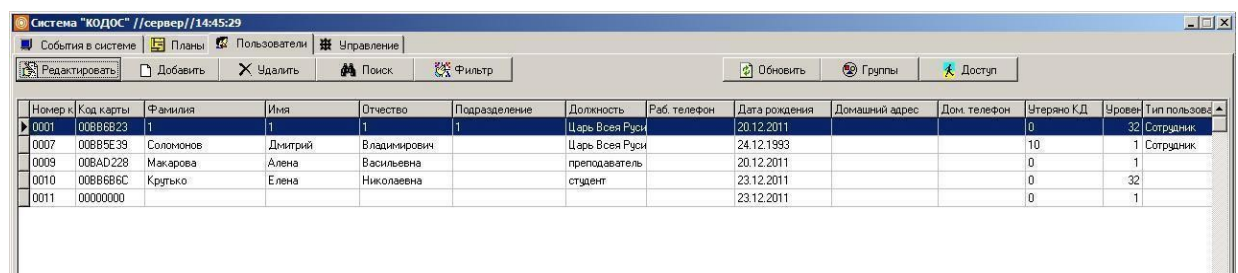
Для того чтобы ОПС реагировала на постановку/снятие с охраны необходимо в конфигурации датчиков выключить свойство Автопостановка.

Для этого в программе «Конфигуратор» необходимо выполнить изменение конфигурации. Изменённую конфигурацию необходимо записать в прибор А-20.

После записи изменённой конфигурации в прибор необходимо добавить пользователя, для этого необходимо выполнить следующие действия.

Запустите «Сервер ИКБ» и войдите в систему:

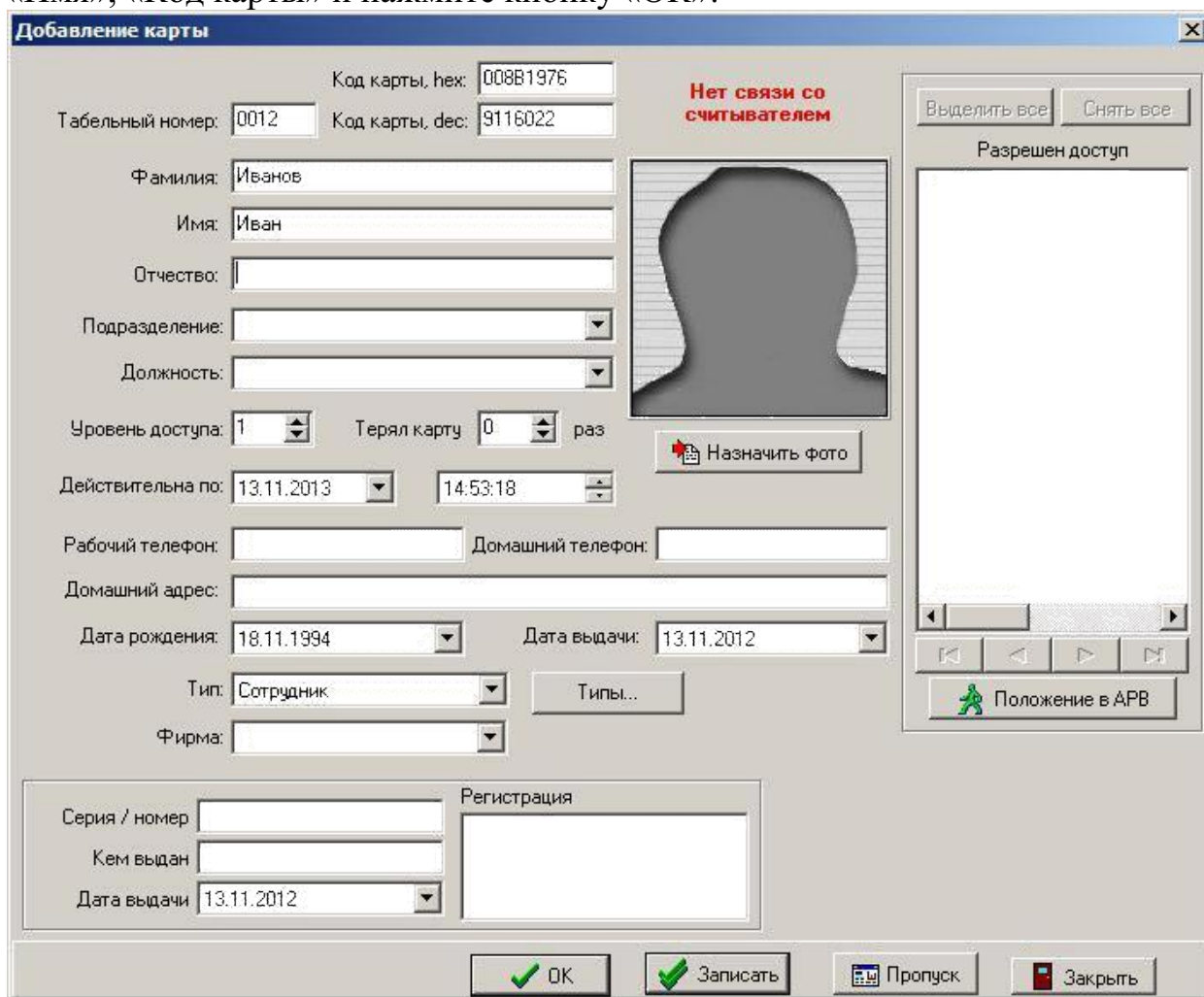
Перейдите на вкладку пользователи:



Номер к.	Код карты	Фамилия	Имя	Отчество	Подразделение	Должность	Раб. телефон	Дата рождения	Домашний адрес	Дом. телефон	Утеряно КД	Уровень	Тип пользов.
0001	00B86823	1	1	1	1	Царь Всея Руси		20.12.2011			0	32	Сотрудник
0007	00B85E39	Соломонов	Дмитрий	Владимирович		Царь Всея Руси		24.12.1993			10	1	Сотрудник
0009	00B4D228	Макарова	Алена	Васильевна		преподаватель		20.12.2011			0	1	
0010	00B8686C	Кругляко	Елена	Николаевна		студент		23.12.2011			0	32	
0011	00000000							23.12.2011			0	1	

Рисунок 25 – Окно приложения «Сервер ИКБ» с открытой вкладкой «Пользователи»

Нажмите кнопку добавить, затем заполните на форме поля «Фамилия», «Имя», «Код карты» и нажмите кнопку «ОК»:



Добавление карты

Код карты, hex: 008B1976
Табельный номер: 0012 Код карты, dec: 9116022

Нет связи со считывателем

Фамилия: Иванов
Имя: Иван
Отчество:
Подразделение:
Должность:
Уровень доступа: 1 Терял карту: 0 раз
Действительна по: 13.11.2013 14:53:18
Рабочий телефон: Домашний телефон:
Домашний адрес:
Дата рождения: 18.11.1994 Дата выдачи: 13.11.2012
Тип: Сотрудник
Фирма:
Назначить фото

Разрешен доступ

Серия / номер
Кем выдан
Дата выдачи: 13.11.2012

Регистрация

ОК Записать Пропуск Закреть

Рисунок 26 – Окно ввода данных пользователя системы

Для получения hex-кода карты необходимо перевести десятизначный код карты (номер карты) в шестнадцатеричную систему. Проще всего эту процедуру выполнить с помощью стандартного калькулятора Windows в режиме «программист». Необходимо установить переключатель в режим «Дес» ввести код с карты и установить переключатель в режим «Hex». Полученный шестнадцатеричный код слева дополнить нулями (число должно содержать 8 символов).

Если ввести код карты в десятичном виде в поле «Код карты, dec:» то код будет автоматически переведён в hex-код. Аналогичное преобразование

только из hex в dec осуществляется при изменении значений в поле «Код карты, hex:»

Перейдите на вкладку «Управление», выберите «Пульт А20» и нажмите «Настройка пультов», перейдите на вкладку «Операторы», затем нажмите кнопку «Добавить».

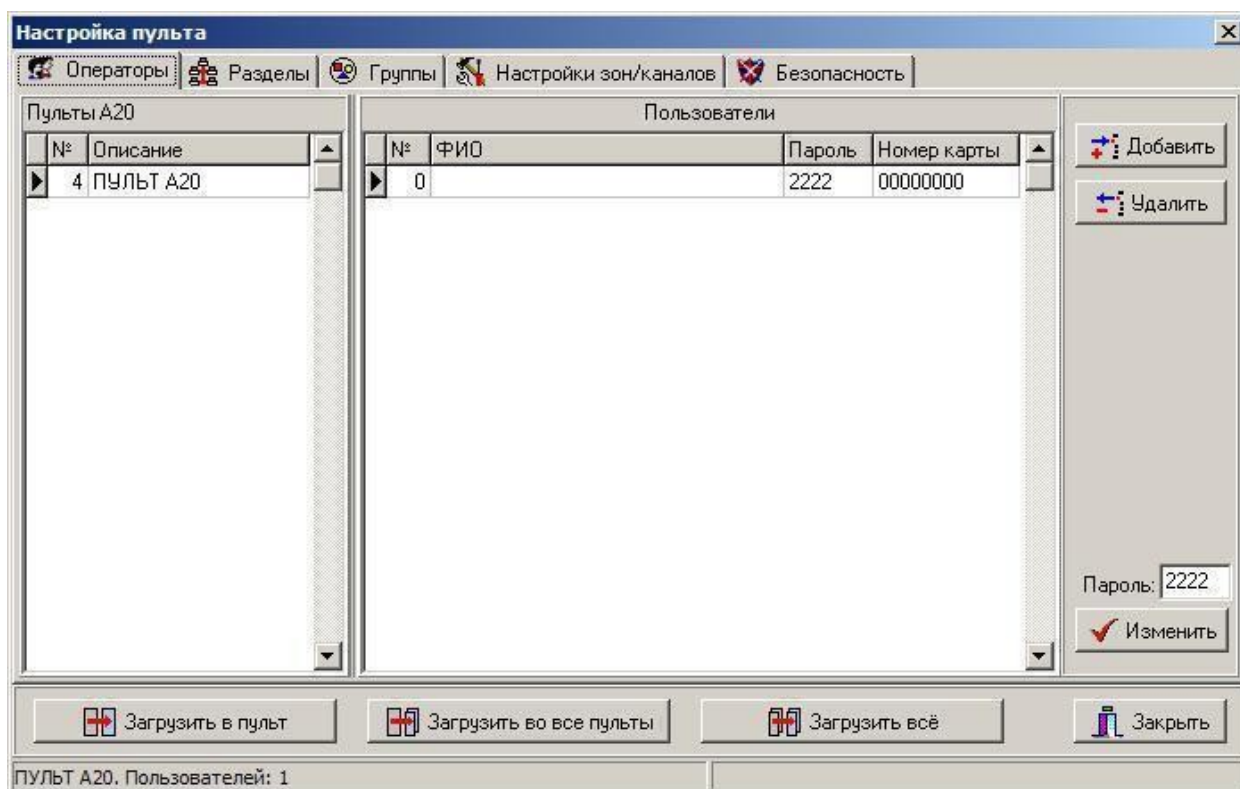


Рисунок 27 – Окно настроек Пульта А20

Выберите из списка созданного вами пользователя, измените поле «№» (чтобы исключить совпадения) и «Пароль» (он также должен быть уникальным).

Добавление нового пользователя

№	Фамилия	Имя	Отчество	Таб. номер	Код карты (DEC)	Код карты (HEX)
2	Соломонов	Дмитрий	Владимирович	0007	12279353	00B85E39
7	Иванов	Иван		0012	9116022	008B1976
3	1	1	1	0001	12282659	00B86B23
4	Макарова	Алена	Васильевна	0009	12243496	00BAD228
5	Крутько	Елена	Николаевна	0010	12282732	00B86B6C
6				0011	0	00000000

Фильтр

☒ По фамилии
 ☐ По коду карты (HEX)

№:
 Пароль:

Рисунок 28 – Окно добавления нового пользователя

После этого нажмите кнопку «Добавить».

На вкладке «Операторы» должен отобразиться добавленный пользователь.

После чего необходимо нажать кнопку «Загрузить в пульт» и дождаться окончания загрузки пользователей.

Далее рекомендуется проверить корректность занесения данного пользователя в пульт, осуществив вход в систему с блока А-20 под данным пользователем.

Далее необходимо создать два раздела одна содержащая выбранные датчики, другая все остальные. Также необходимо будет создать группу датчиков, содержащую выбранные датчики.

Перейдя на вкладку «Разделы»

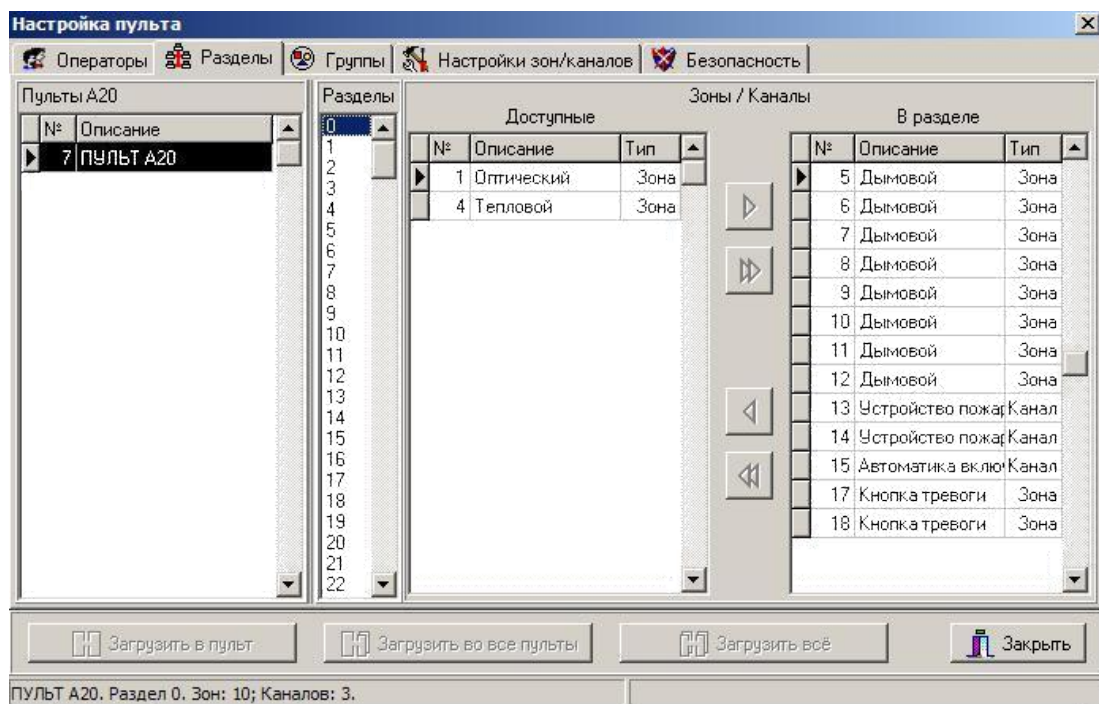


Рисунок 29 – Окно настройки разделов

В раздел с индексом 0 необходимо выполнить перенос всех датчиков которые не были выбраны как датчики с управлением постановки на охрану,

а в раздел с индексом 1 перенести выбранные датчики которые пользователь должен устанавливать и снимать с охраны.

После окончания изменений разделов необходимо нажать кнопку «Загрузить в пульт» и дождаться окончания загрузки.

Перейдя на вкладку «Группы» необходимо в группу с индексом 1 перенести выбранные датчики.

После окончания изменений групп необходимо нажать кнопку «Загрузить в пульт» и дождаться окончания загрузки.

После этого необходимо перейти на вкладку «Управление». На вкладке управление справа в группе кнопок «Управление конфигурацией» нажать кнопку «Группы датчиков».

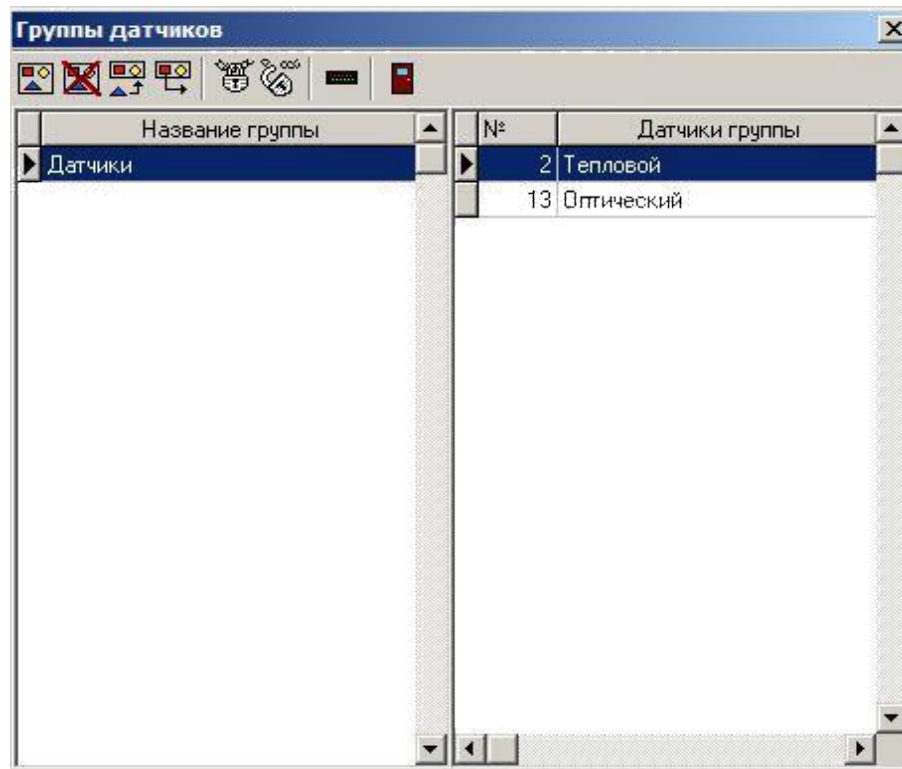


Рисунок 30 – Окно формирования групп датчиков

Далее необходимо создать новую группу и добавить в группу датчики, постановка на охрану которых осуществляется пользователем вручную. После этого в данном окне необходимо нажать кнопку «Индикация», откроется следующее окно.

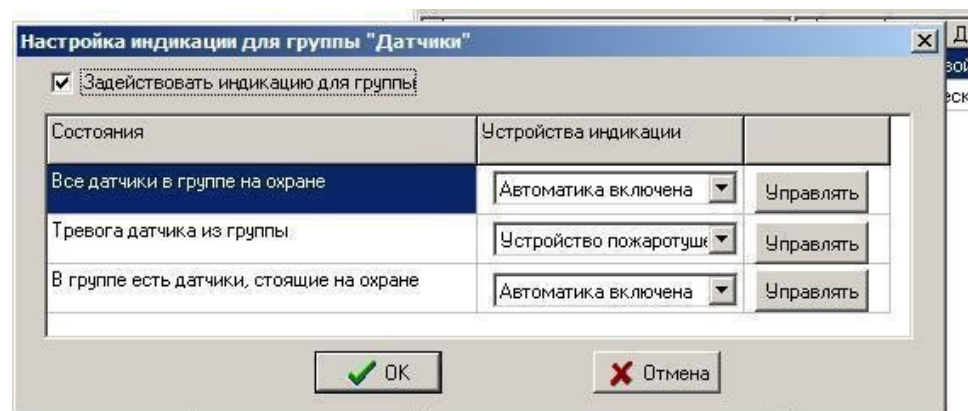


Рисунок 31 – Окно настройки индикации для выбранной группы датчиков

Необходимо будет поставить галочку «Задействовать индикацию для группы». И выбрать действия устройств при определённых событиях в системе. Необходимо отметить тот факт, что устройства будут реагировать на события только при запущенном сервере ИКБ.

Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомится с теоретической частью лабораторной работы.
2. С разрешения преподавателя включить стенд ОПС.
3. При помощи программы конфигуратор выполнить изменение конфигурации созданной ранее, отключив свойство Автопоставнока у двух датчиков (рекомендуется использовать датчики А07).

4. Изменённую конфигурацию загрузить в А-20.
5. При помощи программы Сервер ИКБ добавить нового пользователя, с указанием Proximity-карты.
6. При помощи программы Сервер ИКБ создать раздел содержащий два выбранных ранее датчика, и второй раздел с остальными датчиками.
7. При помощи программы Сервер ИКБ создать группу, в которую входят выбранные ранее датчики.
8. При помощи программы ИКБ создать группу датчиков в окне «Группы датчиков» и выполнить настройку действий(После постановки на охрану должна включаться надпись «Автоматика включена», в случае тревоги должен включаться светодиод на адресном блоке А08).

Проверка настроенного стенда осуществляется по следующей методике:

1. Используя Proximity-карту добавленного пользователя проверятся постановка/снятие с охраны, при этом должна наблюдаться работа устройств.
2. При поставленных(-ом) на охране датчиках(-ке) должна вызывается тревожная ситуация, а также включать устройство подключаться к адресному блоку А08.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполнения индивидуального задание лабораторной работы.
5. Вывод.

Контрольные вопросы

1. Для чего в конфигурации датчиков необходимо свойство Автопостановка?
2. Назовите основные поля, которые необходимо заполнить длядобавления нового пользователя.
3. Для чего необходимо группировать датчики?
4. Что называется «раздел» в терминологии КОДОС?
5. Перечислите все способы постановки и снятия с охраны блока А-20.

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П.,

Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.

8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

7 СЕМЕСТР

ТЕМА 1. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА

Практическая работа №1-6

Цель: научиться настраивать СКУД на базе контроллера «КОДОС PRO» при помощи программного обеспечения КОДОС.

Теоретическое обоснование

Стенд СКУД на базе контроллера «КОДОС PRO» представлен на рисунке 32.

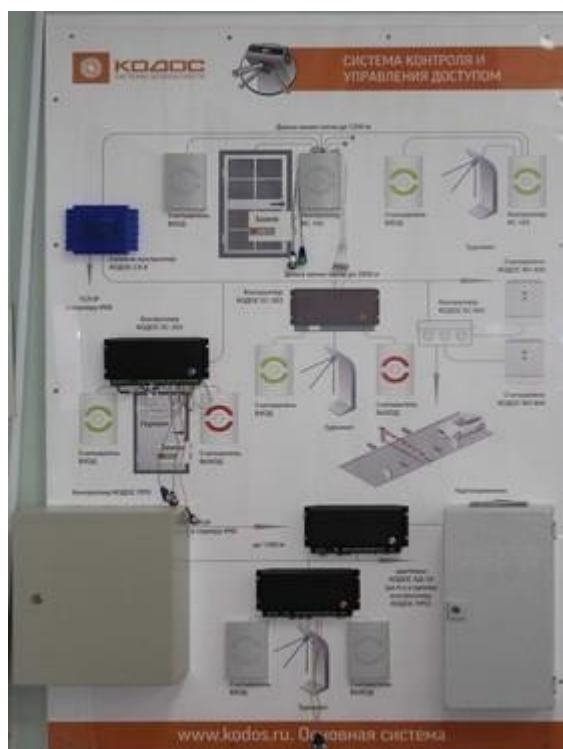


Рисунок 32 – Стенд СКУД на базе контроллера «КОДОС PRO»

Система контроля и управления доступом (далее – СКУД, Система) **на базе контроллера «КОДОС PRO»** «КОДОС PRO» предназначена для контроля и разграничения доступа на контролируемый объект (помещение, территорию, зону) сотрудников, клиентов, посетителей. СКУД позволяет в любое время обеспечить контроль над ситуацией на объекте, порядок, безопасность персонала и посетителей, сохранность материальных ценностей и информации.

Основные функции СКУД:

- а) предоставление допуска в находящуюся под контролем Системы зону лицам, имеющим в данное время право прохода и запрещение доступа лицам, не имеющим такого права;
- б) автоматизированное управление режимом прохода в контролируемую зону, дистанционное управление состоянием исполнительных устройств;
- в) предоставление пользователю в реальном времени информации о текущих событиях Системы с помощью текстовых, звуковых и речевых сообщений;
- г) автоматическое ведение протоколов событий, происходящих в Системе, включая изменение режимов работы оборудования, программного обеспечения (ПО) и фиксацию действий операторов, работающих с Системой;
- д) ведение учета рабочего времени, формирование отчетов о событиях Системы;
- е) ведение автоматизированного учета постоянных, временных и разовых пропусков (идентификаторов) и хранение в базе данных информации об их владельцах (включая фотоизображения);
- ж) обеспечение возможности дистанционной визуальной идентификации владельцев пропусков.

Основным предназначением системы контроля и управления доступом на базе контроллера «КОДОС PRO» является организация крупных проходных с большим числом точек прохода и высокой интенсивностью потока. Такое применение Системы обусловлено техническими параметрами контроллера «КО-ДОС PRO» и особенностями Системы в целом.

Структурная схема системы контроля и управления доступом на базе контроллера «КОДОС PRO», представлена на рисунке 33.

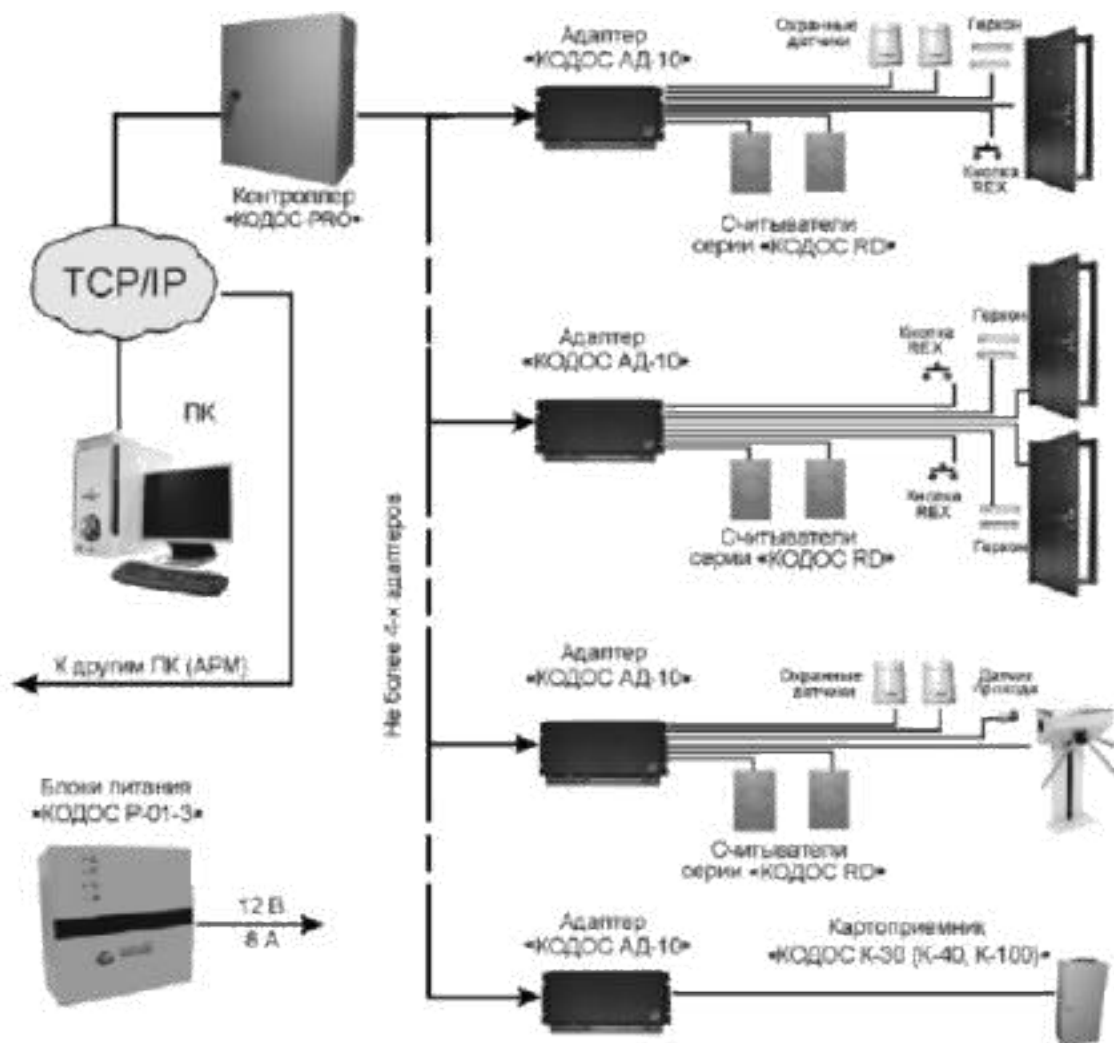


Рисунок 33 – Схема СКУД на базе контроллера «КОДОС PRO»

Основным управляющим устройством Системы является контроллер «КОДОС PRO», который имеет следующие особенности:

- а) имеет энергонезависимую память повышенной емкости, в которой может храниться до 65 000 пользователей, и содержаться информация о 100 000 событий;
- б) предназначен для управления несколькими исполнительными устройствами, (например, дверными замками, турникетом, картоприемником), подключение которых может осуществляться в различных сочетаниях; управление исполнительными устройствами осуществляется при помощи специальных адаптеров «КОДОС АД-10» (см.

ниже);

в) не требует наличия специализированного блока питания (питается от сети переменного тока напряжением 220 В); благодаря наличию энергонезависимой памяти сохраняет работоспособность не только в случае отсутствия связи с ПК, но и при отсутствии напряжения в сети переменного тока, переключаясь на питание от аккумуляторной батареи (АКБ)

г) имеет свой IP-адрес, что позволяет подключать контроллер непосредственно к существующим компьютерным сетям, использующим для информационного обмена семейство протоколов межсетевого взаимодействия TCP/IP, и управлять им по сети Ethernet или (при наличии в локальной вычислительной сети (ЛВС) доступа в глобальную сеть)

посредством Интернета.

В процессе работы контроллер «КОДОС PRO» выполняет следующие функции:

а) принимает, обрабатывает и хранит информацию, поступающую через адаптеры «КОДОС АД-10» от считывателей, исполнительных устройств и охранных шлейфов; при необходимости передает информацию в ПК;

б) управляет исполнительными устройствами при помощи адаптеров «КОДОС АД-10» по алгоритмам, заложенным в управляющей программе, или по командам с ПК;

в) осуществляет контроль доступа пользователей в зависимости от кодов считанных карт, временных зон и уровней доступа.

Структурная схема контроллера «КОДОС PRO» представлена на рисунке 34.

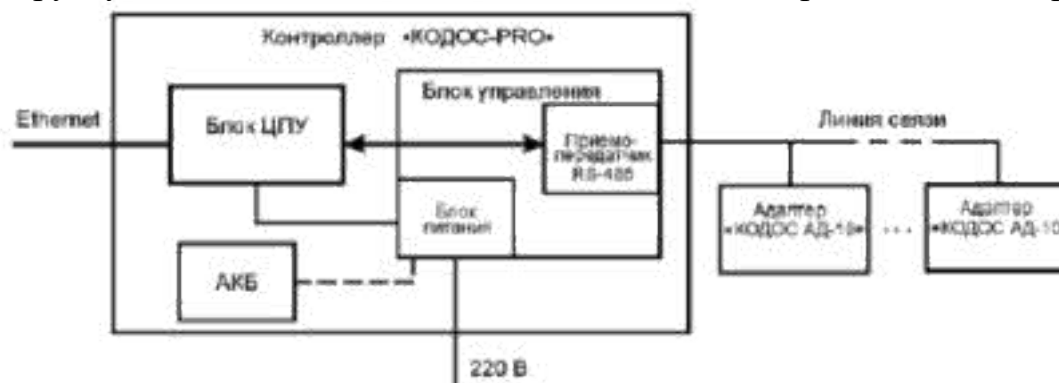


Рисунок 34 – Структурная схема контроллера «КОДОС PRO»

Подключение к контроллеру «КОДОС PRO» исполнительных устройств, считывателей кодов карт пользователей, охранных шлейфов осуществляется при помощи адаптеров «КОДОС АД-10». Максимально к контроллеру

«КОДОС PRO» может быть подключено четыре адаптера «КОДОС АД-10».

Каждый адаптер имеет по два канала управления исполнительными устройствами, два входа для подключения двух считывателей, четыре входа для подключения различных датчиков (например, датчика (геркона) прохода, кнопки принудительного открытия блокирующего устройства (кнопки REX), охранного шлейфа и др.).

Адаптер «КОДОС АД-10» (см. рисунок 35) выполнен в корпусе, в котором имеются клеммы для подключения датчиков, исполнительных устройств, линий питания и связи с контроллером, считывателей идентификационных кодов. Кроме того, на лицевой стороне корпуса имеются светодиоды индикации режимов работы адаптера, а с обратной стороны корпуса (см. рисунок 36) – переключатели, при помощи которых устанавливается аппаратный адрес адаптера и настраиваются выходы адаптера для работы с исполнительными устройствами прямого или инверсного типа. Адаптер может быть установлен на поверхность любого типа. Для крепления устройства в комплекте поставки имеются самонарезающие винты и дюбели (для крепления на бетонную или кирпичную



поверхности).

Рисунок 35 – Внешний вид адаптера



Рисунок 36 – Внешний вид адаптера (вид сзади)

С целью обеспечения взаимодействия контроллера «КОДОС PRO» с управляющим ПК через локальную вычислительную сеть (ЛВС) в контроллере реализована поддержка семейства протоколов TCP/IP. Для обращения к контроллеру как к сетевому устройству необходимо перед началом его эксплуатации ввести в энергонезависимую память устройства IP-

адрес контроллера в сети, маску подсети и адрес шлюза (если между управляющим ПК и контроллером есть маршрутизация). По умолчанию в контроллере установлен IP-адрес 192.168.139.101. В

случае использования контроллера в сети, позволяющей обращаться к нему по данному адресу, изменения сетевых настроек контроллера не требуется.

Ввод сетевых настроек осуществляется при помощи сервиса «telnet» операционной системы управляющего ПК. Для этого необходимо подключить контроллер к ПК при помощи кроссоверного кабеля и в папке «Сеть и удаленный доступ к сети» операционной системы создать новое подключение с IP-адресом, отличающимся от адреса контроллера только последним октетом (например, 192.168.139.1).

Последовательность действий при вводе сетевых настроек следующая:

ввода набрать cmd ;

Важно! После набора каждой команды (цифры, логина, пароля), выделенных полужирным шрифтом необходимо нажатие клавиши Enter.

б) в приглашении командной строки C:\ набрать telnet ;

в) в приглашении telnet-сервиса Microsoft Telnet> набрать open xxx.xxx.xxx.xxx, где xxx.xxx.xxx.xxx – IP-адрес контроллера «КОДОС PRO». Если в файле «hosts» IP-адресу контроллера поставлено в соответствие некоторое имя, можно обратиться к устройству по имени, т. е. open <имя контроллера>;

*Если при попытке соединения не происходит установления связи с контроллером, возможно, с ним нет физического соединения. Для проверки соединения с контроллером необходимо запустить из командной строки Windows утилиту **ping** (например, ping 192.168.139.101 или ping <имя контроллера>). Если в результате появляется:*

Ответ от 192.168.139.101: число байт=32 время<10мс TTL=64

Ответ от 192.168.139.101: число байт=32 время<10мс TTL=64

Ответ от 192.168.139.101: число байт=32 время<10мс TTL=64

Ответ от 192.168.139.101: число байт=32 время<10мс TTL=64 *то связь с контроллером есть. Если же появляется строка:*

Превышен интервал ожидания для запроса, то связь с контроллером отсутствует из-за проблем в ЛВС.

г) после входа в ОС контроллера (в первой строке появится надпись *PicoBSD <...> <...>*) в приглашениях *login:* и *password:* ввести соответственно **root** и **setup**.

*Имя **root** и пароль **setup** установлены в контроллере по умолчанию. При необходимости пользователь может изменить пароль.*

После ввода имени и пароля появится основное меню контроллера (см. рисунок 4.6):

Для выполнения сетевых настроек необходимо в приглашении *Command:* ввести **5** для выбора пункта меню *IP address*, после чего появится меню редактирования сетевых настроек:

0 - Exit 1 - Edit 2 - Commit 3 - Load Default

После ввода **1** («Редактировать») в появившемся текстовом редакторе необходимо внести изменения **IP-адреса** и **маски** в строку

`ifconfig_da0=«inet 192.168.139.101 netmask 0xfffff00».` :

В строке для редактирования имя сетевой карты (могут присутствовать различные имена: **ed1** и **da0**) не менять!

В соответствии с вышеприведенной строкой сетевых настроек контроллера *PRO* маска подсети должна вводиться в

шестнадцатеричном формате. Для перевода значения маски из десятичного в шестнадцатеричный формат необходимо воспользоваться программой

«Калькулятор» операционной системы Windows.

После выхода из редактора с сохранением произведенных изменений (**Escape**, затем **a**) необходимо применить новые настройки. Для этого вводится **2** («Применить»), затем **0** («Выход»).



Рисунок 26 – Основное меню контроллера «КОДОС PRO»

Рисунок 37 – Основное меню контроллера

После введения в основном меню контроллера команды 4 («Перезагрузка системы») появится:

Подключение к узлу утеряно. Нажмите любую клавишу, и после выполнения данного действия – окно сервиса telnet. После набора команды

Microsoft Telnet> quit, пользователь оказывается в стандартном окне командной строки.

Также для корректного определения контроллера «КОДОС PRO» программой «Конфигуратор» необходимо в файле «hosts», расположенном в папке WINNT\system32\drivers\etc\ операционной системы Windows 2000 (или WIN-DOWS\system32\drivers\etc\ для ОС Windows XP), управляющего ПК задать соответствие имени контроллера его IP-адресу. Файл «hosts»

открывается (клик правой кнопкой мыши на файле => Открыть с помощью...)

при помощи встроенных текстовых редакторов операционной системы «Блокнот» или «Wordpad».

Ниже приведен пример файла «hosts»(рисунок 38).

```
# 102.54.94.97 rhino.acme.com # исходный сервер
# 38.25.63.10 x.acme.com # узел клиента x
127.0.0.1 localhost
192.168.139.101 pro
```

Рисунок 38 – Пример содержимого файла hosts

Если по каким-либо причинам в процессе эксплуатации Системы происходит смена IP-адреса контроллера, необходимо в файле «hosts» задать новое соответствие IP-адреса контроллера его имени

Для конфигурирования контроллера необходимо убедиться, что он включён в сеть и подключён к сети ЛВС. На лабораторном стенде контроллеру присвоен IP-адрес 192.168.31.249. Перед началом работ необходимо убедиться, что контроллер доступен по данному адресу,

выполнив попытку подключения к контроллеру по протоколу telnet.

Также необходимо проверить файл hosts, в файле должен быть прописан контроллер PRO с IP-адрес 192.168.31.249.

```
127.0.0.1 localhost
192.168.31.251 ske1
192.168.31.252 ske2
192.168.31.111 Notebook-Kodos
192.168.31.249 pro
192.168.31.111 Notebook-Kodos
```

Рисунок 39 – Пример правильного файла hosts.

Далее запустив программу конфигуратор необходимо выполнить добавление контроллера КОДОС PRO.

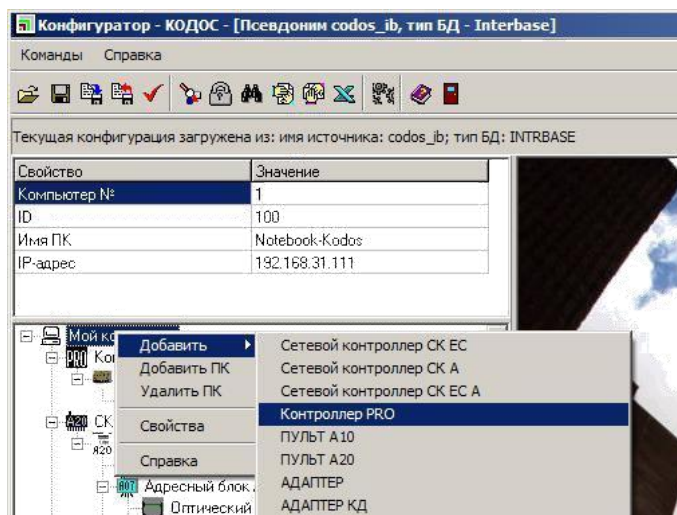


Рисунок 40 – Добавление контроллера «КОДОС PRO»

Далее необходимо добавить контроллер турникета из контекстного меню контроллера КОДОС PRO.

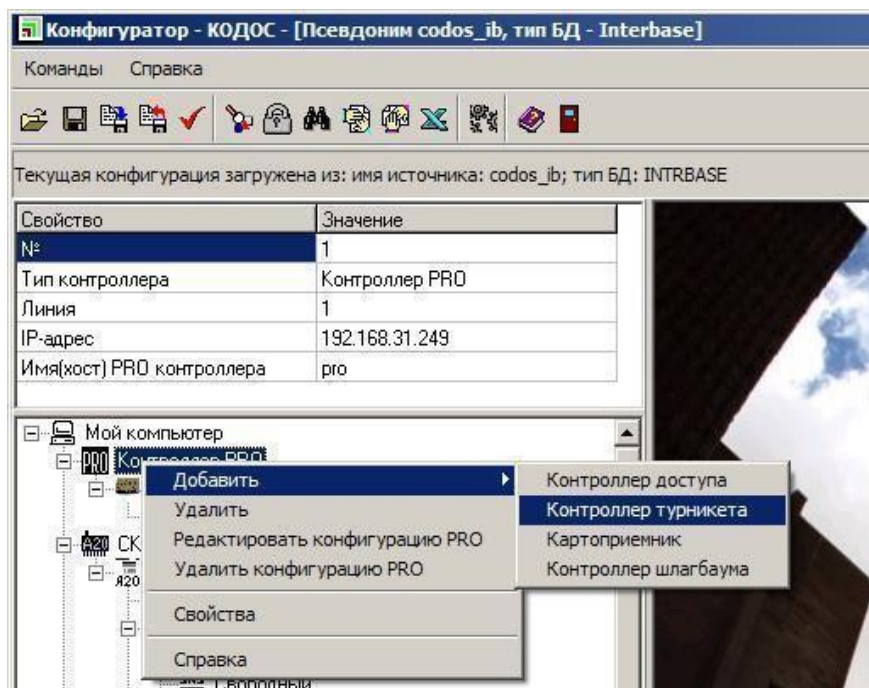


Рисунок 41 – Добавление котроллера турникета

В свойствах добавленного контроллера необходимо изменить адрес добавленного контроллера, в соответствии с адресом, выставленным при помощи переключателей на контроллере, на лабораторном стенде

установленный аппаратный адрес равен 1, остальные настройки можно ставить неизменными. Если требуется более частый опрос контроллеров, для более быстрого отображения информации о событиях контроллера можно снизить приоритет, чем ниже приоритет, тем чаще выполняется опрос контроллера.

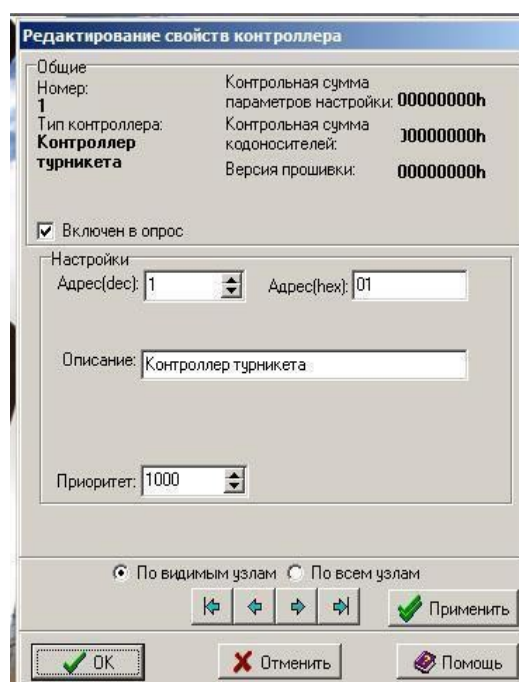
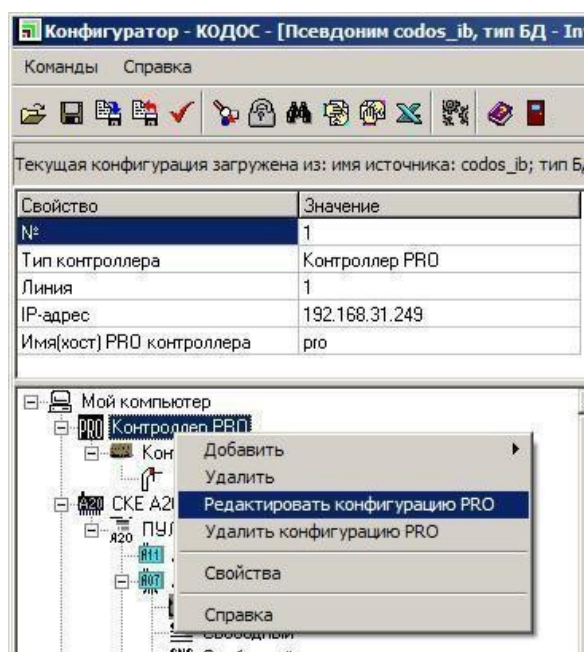


Рисунок 42 – Редактирование свойств контроллера турникета

Далее необходимо выполнить редактирование конфигурации контроллера



КОДОС PRO.

Рисунок 43 – Выбор меню редактирования конфигурации контроллера

Откроется следующее окно

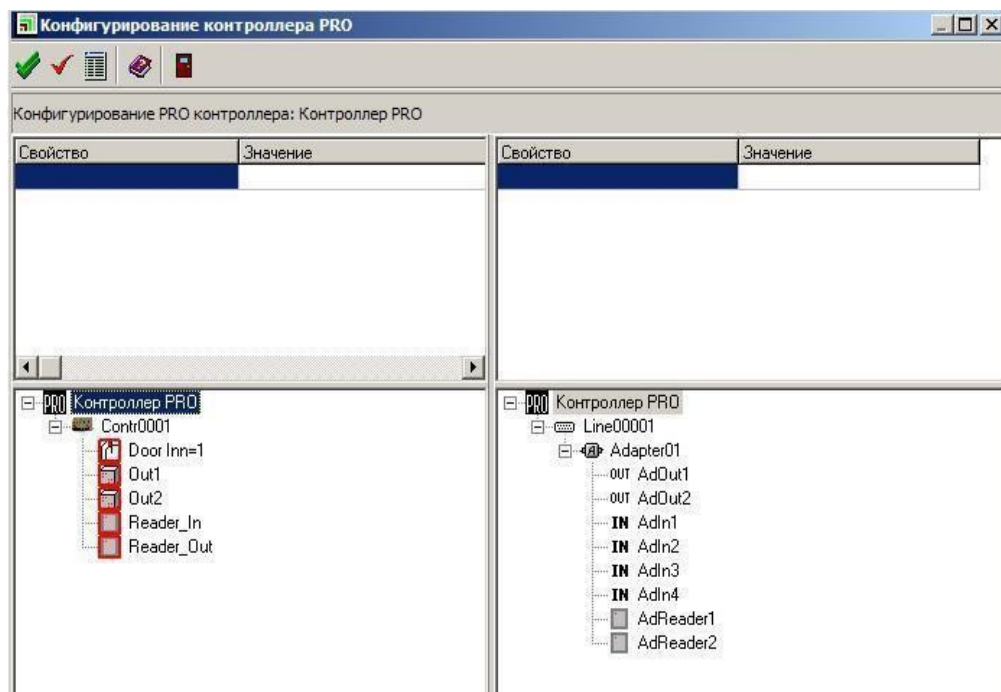


Рисунок 44 – Окно редактирования конфигурации контроллера

С левой стороны находятся контроллеры, добавленные к контроллеру КОДОС PRO, справа указываются линии контроллера, которые необходимо связать с аппаратным подключением.

Для того чтобы выполнить связывание шлейфов с программным представлением необходимо добавить линию контроллера. К линии необходимо добавить контроллер. В свойствах контроллера необходимо указать аппаратный адрес контроллера выставленного с помощью DIP-переключателя. На лабораторном стенде контроллер турникета имеет аппаратный адрес 1.

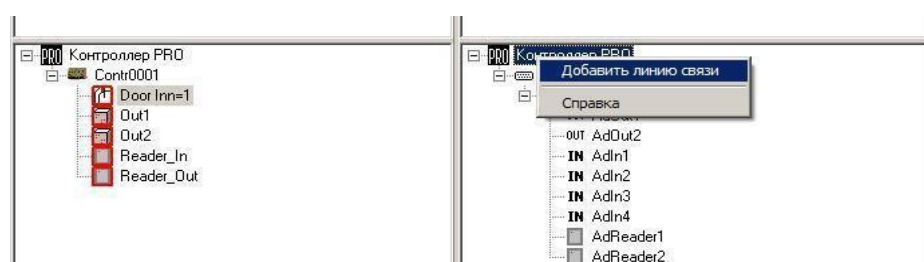


Рисунок 45 – Добавление линии связи

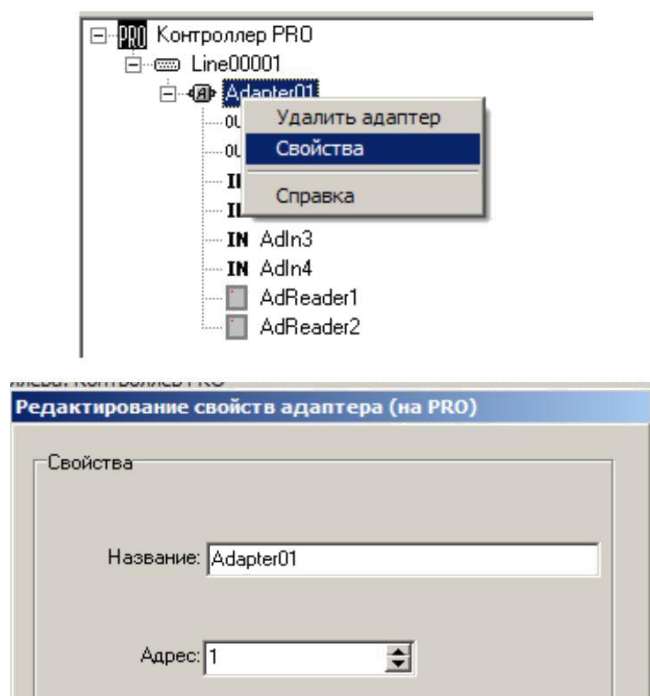


Рисунок 46 – Присваивание адаптеру соответствующего адреса

Для выполнения связывание необходимо вызвать контекстное меню слева на соответствующем программном представлении.

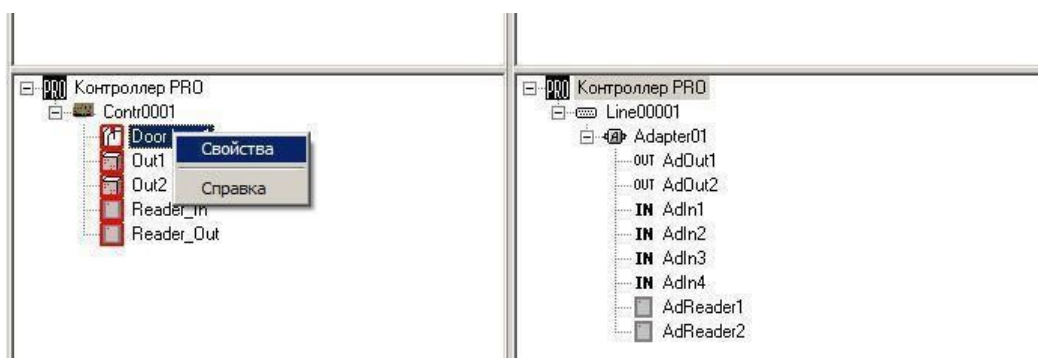


Рисунок 47 – Выбор контекстного меню свойства турникета

В открывшемся окне выбираем линию связи

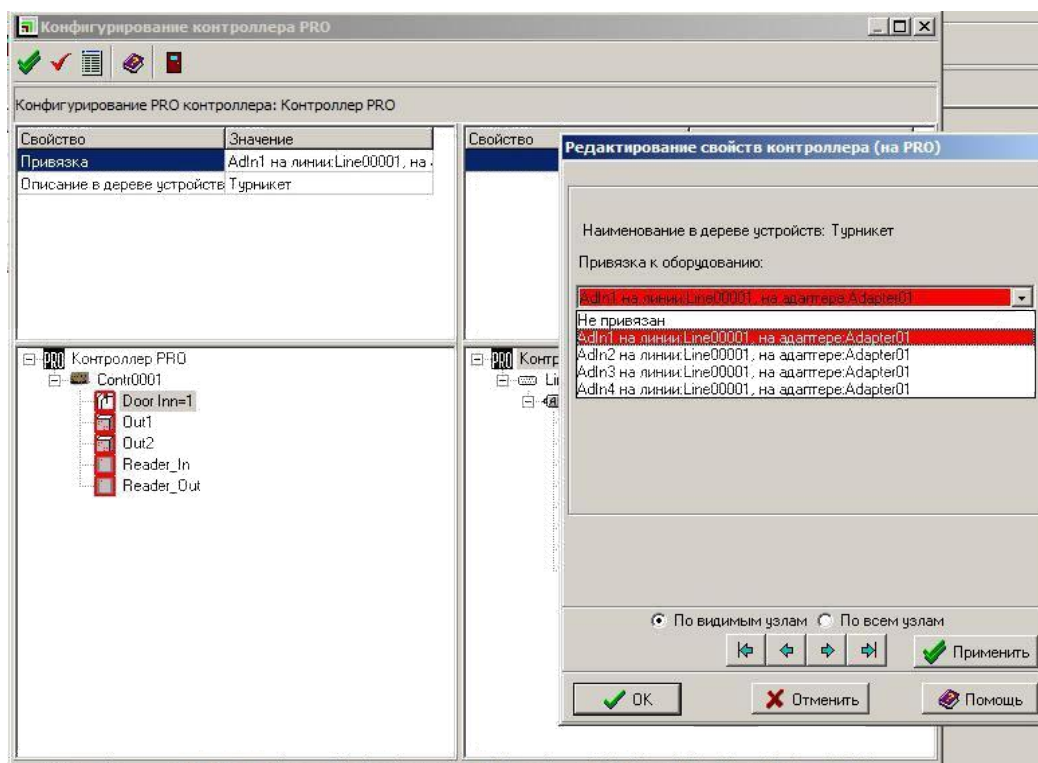


Рисунок 48 – Окно выбора линий для связывания датчиков и линий

Датчики In связываем с линиями In, датчики Out связываем с линиями Out, Reader – с Reader.

После нажатия Ok. Устанавливается связь выбранного датчика с выбранной линией, датчики которые привязаны к линиям. Установить два датчика на одну линию нельзя. Связывать линии и датчики надо по порядку.

После окончания связывания необходимо нажать кнопку применения конфигурации.

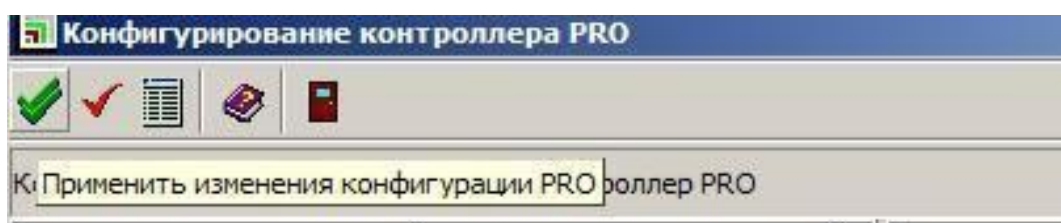
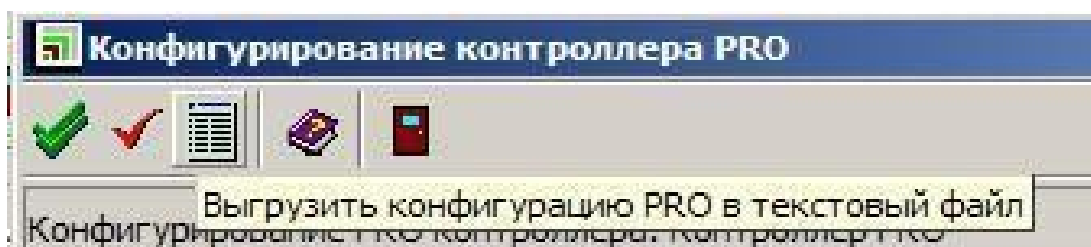
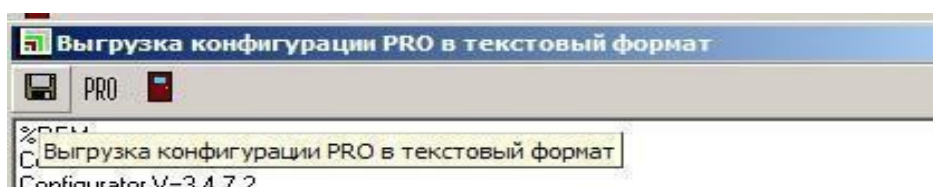


Рисунок 49 – Панель инструментов конфигурирования контроллера «КОДОС PRO»

Если конфигурация не содержит ошибок, то её можно записать в контроллер КОДОС PRO, для этого:нажимаем кнопку

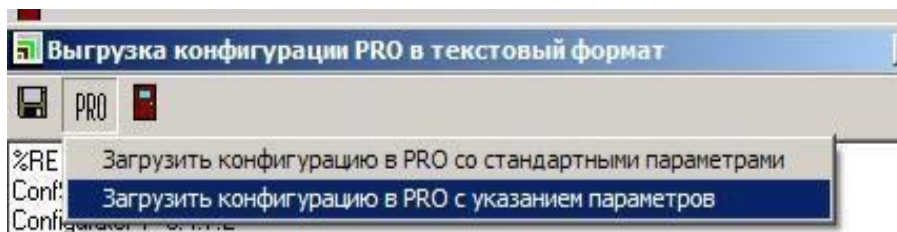


1) В открывшемся окне нажать «Выгрузить конфигурацию PRO в текстовый файл»



Далее сохраняем файл.

2) В открывшемся окне нажать «Загрузить конфигурацию в PRO с указанием параметров»



В открывшемся окне проверяем правильность указания IP-адреса и выбрать сохранённый файл на предыдущем этапе и нажимаем кнопку

«Загрузить».

3) Дождаться окончания загрузки конфигурации (для применения конфигурации контроллером возможно потребуется перезагрузка контроллера).Далее запускаем программу Сервер ИКБ и переходим на вкладку

«Пользователи» и добавляем нового пользователя. При вводе пользователя необходимо обязательно указать код карты и отметить слева, что разрешен доступ «Турникет». После чего нажать «Ок».

На вкладке «Управление» необходимо выбрать контроллер и нажать «Записать всех в дверь».



Дождавшись окончания записи можно произвести попытку входа и выхода через турникет, при правильном конфигурировании будет указано, что созданный пользователь вошёл или вышел через турникет.

Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомится с теоретической частью лабораторной работы.
2. С разрешения преподавателя включить стенд СКУД.
3. При помощи программы конфигуратор выполнить настройку контроллера «КОДОС PRO», настроив контроллер доступа типа «турникет».
4. При помощи программы сервер ИКБ выполнить открытие закрытие турникета.
5. При помощи программы Сервер ИКБ произвести добавление нового пользователя, разрешив проход через турникет.
6. Проверить работоспособность настроенного контроллера произведя вход и выход через контроллер.

Проверка настроенного стенда осуществляется по следующей методике:

- 1) При отключённом сервере ИКБ студент выполняет вход и выход через турникет.
- 2) При запущенной программе сервер ИКБ студент осуществляет вход и выход через турникет, при этом сервер ИКБ должен отображать входящего и выходящего пользователя.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполнения индивидуального задания лабораторной работы.

Контрольные вопросы

1. Для чего предназначена Система контроля и управления доступом на базе контроллера «КОДОС PRO»?
2. Какие функции выполняет СКУД «КОДОС PRO»?

3. Каково основное предназначение СКУД «КОДОС PRO»?
4. Какие элементы присутствуют в Адаптер «КОДОС АД-10»?
5. Для чего в контроллере реализована поддержка семейства протоколов ТСР/IP?

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

ТЕМА 2. ОРГАНИЗАЦИЯ СЛУЖБЫ БЕЗОПАСНОСТИ ОБЪЕКТА

Практическая работа №7-12

Цель: научиться настраивать СКУД на базе оборудования «КОДОС» и программного обеспечения «Сервер ИКБ».

Теоретическое обоснование

СКУД на базе оборудования «КОДОС» может работать без контроллеров-посредников, таких как «КОДОС PRO», но тогда для работы оборудования требуется использование программного обеспечения «Сервер ИКБ».

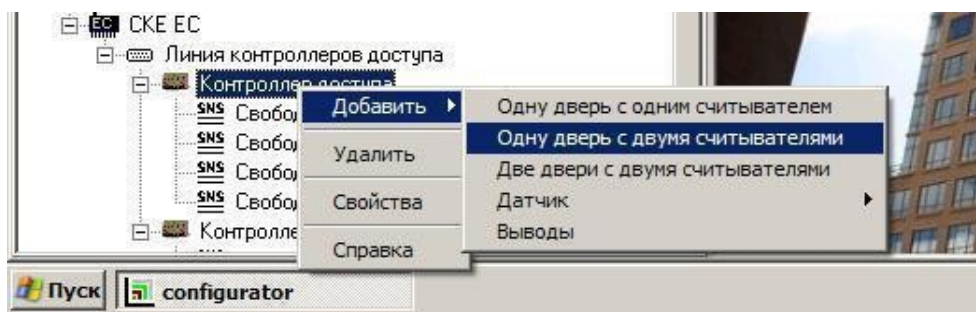
Конфигурирование оборудования происходит сходным образом с предыдущими лабораторными работами.

Для начала необходимо создать конфигурацию в программе «Конфигуратор».

К виртуальному ПК обозначающий рабочую станцию добавляем контроле «СКЕ ЕС». IP-адрес контроллера обозначен в файле hosts как ske2.

Далее к контроллеру добавляем «Линия контроллеров доступа». К линии добавляем два контроллера доступа. Первому контроллеру назначаем адрес 1 (dec). Второму адрес 2 (dec).

Далее к первому контроллеру необходимо выполнить добавление предустановленной конфигурации одной двери и двух считывателей.



После этого можно заполнить оставшиеся свободные выводы под датчики датчиками любого типа (на стенде присутствует эмуляция датчиков в виде кнопок, так что выбранный тип датчика не имеет ни какой роли).

Добавленную дверь переименуйте в «Дверь входная».

Второй контроллер для удобства переименуйте в RC102. Добавьте к нему также предустановленную конфигурацию одной двери и двух считывателей.

Добавлять какие либо датчики ко второму контроллеру не надо, т.к. к нему не подключено дополнительных датчиков.

Полученная конфигурации должна выглядеть подобно конфигурации на рисунке 5.1.

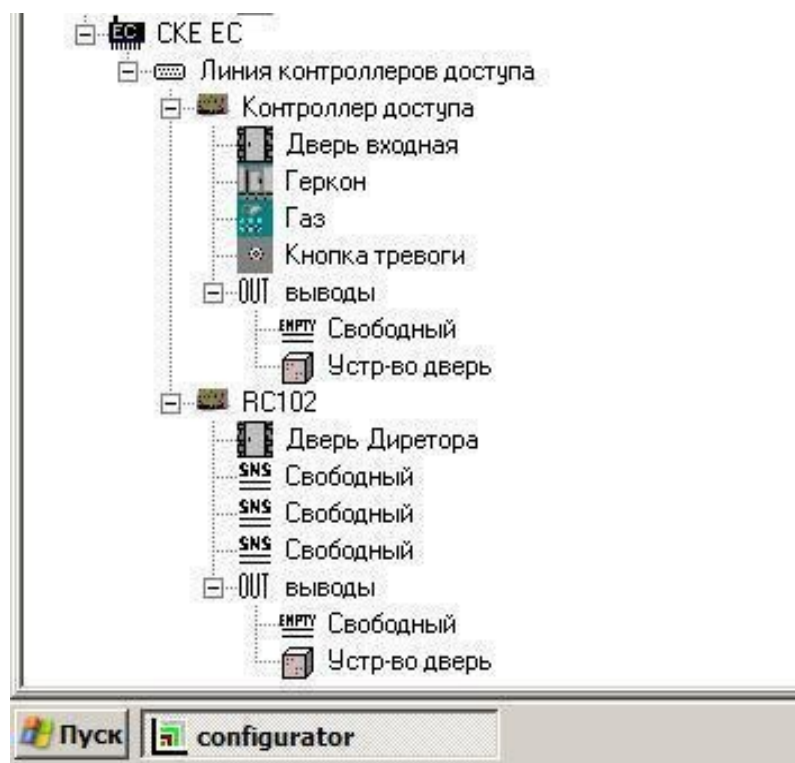


Рисунок 50 – Пример конфигурации

После сохранения и выхода из программы «Конфигуратор» необходимо запустить «Сервер ИКБ» и выполнить добавление нового пользователя с занесением информации о Proximity-карты.

После этих действий выполняется проверка возможности входа пользователя через двери.

Входная дверь в аудитории 322 соединена с электронным замком, который отпирается, если осуществляет вход или выход зарегистрированного пользователя системы.

Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомиться с теоретической частью лабораторной работы.
2. С разрешения преподавателя включить стенд «СКУД».
3. Создать конфигурацию в программе «Конфигуратор».
4. Выполнить добавление пользователя.
5. Проверить работоспособность настроенного стенда.
6. Проверка настроенного стенда осуществляется по следующей методике:

- 1) Проверяется реакция считывателей на вход/выход зарегистрированного пользователя.
- 2) Проверяется реакция считывателей на вход/выход незарегистрированного пользователя.
- 3) Проверяется открытие электронного замка при входе/выходе зарегистрированного пользователя.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполнения индивидуального задания лабораторной работы.
5. Вывод.

Контрольные вопросы

1. Каким образом происходит конфигурирование оборудования СКУД на базе оборудования «КОДОС»?
2. Для чего в Конфигураторе предназначены «Линии контроллеров доступа»?
3. Назовите характеристики контроллера RC-102.
4. Назовите стандарты пластиковых карт, которые могут быть использованы с данным стендом.
5. Назовите порядок добавление нового пользователя в систему.
6. Назовите порядок приписывания пользователей к считывателям.

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

ТЕМА 3. ОРГАНИЗАЦИЯ ВНУТРИОБЪЕКТНОГО РЕЖИМА

ТЕМА 4. ОХРАНА ОБЪЕКТОВ

Практическая работа №13-18

Цель: ознакомиться с современными системами видеонаблюдения, изучить их характеристики, функциональные возможности.

Теоретическое обоснование

Все видеосистемы объединяют понятием «цифровые системы видеонаблюдения» (ЦСВН) или зарубежной терминологии DVR (Digital Video Recorder – цифровое записывающее устройство).

В зависимости от типа сжатия видеопотока системы видеонаблюдения на базе ПК делятся на системы с аппаратным и программным сжатием. В

системах с программным сжатием компрессия видеосигнала осуществляется центральным процессором ПК. В системах с аппаратным сжатием сжатие видеопотока происходит на платах видеоввода средствами аппаратных кодеков.

Недостатком систем видеонаблюдения на основе плат с программным сжатием является высокая нагрузка шины ПК, к которой подключается плата видеоввода и, как следствие, - ограничение на скорости ввода и количество обрабатываемых видеоканалов.

Соответственно, преимущество систем видеонаблюдения на основе плат видеоввода с аппаратным сжатием состоит в возможности строить многоканальные системы видеонаблюдения, с высокими качеством

Преобразование аналогового сигнала в цифровой всегда производится АЦП, который является составной частью платы видеоввода. Далее цифровой сигнал «сжимается» кодером (то есть уменьшается его размер) и

записывается на жёсткий диск ПК. Цифровой сигнал «сжимается» либо программно - процессором ПК,

либо аппаратными средствами платы видеоввода.

В настоящее время в ПК используют 3 основных типа шин подключения плат видеоввода:

PCI;

PCI-X;

PCI Express.

Каждая из приведённых шин имеет ряд спецификаций и соответствующую пропускную способность:

PCI v.2.1-3.0 — имеет пиковую пропускную способность для тактовой частоты 33 МГц — 133 Мбайт/с, а для 66 МГц — 266 Мбайт/с;

PCI-X Версия 1.0 имеет пиковую пропускную способность — 1024 Мбайт/с, а версия 2.0 — до 4096 Мбайт/с;

PCI Express компьютерная шина, использует программную модель шины PCI и высокопроизводительный физический протокол, основанный на последовательной передаче данных. Кроме того, шиной PCI Express

поддерживается:

горячая замена карт;

гарантированная полоса пропускания (QoS); управление энергопотреблением;

контроль целостности передаваемых данных.

Значения пиковой (одно- и двухсторонней) пропускной способности различных спецификаций шины PCI Express приведены в таблице.

Таблица 1 – Пропускная способность шины PCI Express, Гбайт/с

Связей	X1	X2	X4	X8	X12	X16	X32
PCIe 1.0	0,25/0,5	0,5/1	1/2	2/4	3/6	4/8	8/16
PCIe 2.0	0,5/1		1/2	2/4	4/8	6/12	8/16
PCIe 3.0	1/2		2/4	4/8	6/12	8/16	16/32

DVR собираются из специализированных компьютерных комплектующих и представляют собой законченные решения, совмещающие функции цифрового видеомagniтофона и мультиплексора. Внешне и органами управления также напоминают видеомagniтофон.

Сравнивая DVR с системами видеонаблюдения на базе ПК, необходимо отметить большую надежность DVR, их простоту в установке, настройке и эксплуатации, простоту интерфейса. С пользовательской точки зрения цифровые видеорегистраторы являются развитием принципов, используемых в аналоговых системах обеспечения безопасности. Соответственно, DVR

часто становятся выбором заказчиков, не желающих коренным образом менять архитектуру системы безопасности и производить переподготовку обслуживающего персонала.

Недостатком DVR является низкий функционал, ограниченный, как правило, возможностью наблюдения, записи и минимальной сетевой работы,

и, зачастую, невозможность организации больших архивов.

Наиболее перспективной из всех реализуемых на практике технологий организации систем видеонаблюдения представляется IP-технология.

Архитектура IP-видеонаблюдения, как правило, выглядит так: в специальном устройстве совмещаются видеокамера, мини-компьютер и сетевой контроллер; передача данных производится с помощью Ethernet-интерфейса.

Встроенный веб-сервер позволяет получать доступ к просмотру видео и управлению устройством через обычный веб-браузер. Помимо этого пользователям систем видеонаблюдения на базе IP-технологии предлагается специализированное программное обеспечение, не применяемое для решения других, задач кроме управления устройством и просмотра видео через Интернет или по локальной сети.

Сохранение видеоматериалов в системах IP-видеонаблюдения производится на удаленные хранилища.

Основными достоинствами систем видеонаблюдения на базе IP-

технологии являются:

Простота установки, настройки и эксплуатации;

IP-системы не требуют прокладки дополнительных кабельных сетей;

Практически неограниченные возможности в организации распределенных систем.

К минусам данных систем следует отнести лишь низкую проработанность IP-технологии, естественно вытекающей из её молодости, и,

пока ещё, высокую стоимость.

Составим таблицу сравнения основных характеристик программно – аппаратных комплексов (Таблица 2).

Таблица 2 – Таблица характеристик систем видеонаблюдения

	Behold Uoffice101	TRASSIR ™Optima	ДОЗОР S -80200	AViaL Le 4.1	NUUO- PC2008	GLOB OSS
ЧИСЛО ВИДЕОВХОДОВ	4	до 16	8	4	8	до 32
ИНТЕРФЕЙС	BNC	BNC	BNC	BNC	BNC	BNC
ЧИСЛО ПЛАТ НА ОДНОМ ПК	1	2	до 4	1	до 4	до 4
ПОДДЕРЖКА WINDOWS	+	+	+	+	+	+
ПОДДЕРЖКА IP КАМЕР	-	-	-	-	+	+
ВОЗМОЖНОСТЬ ИНТЕГРАЦИИ	-	+	-	-	+	+
ПОДДЕРЖКА СЕТЕВЫХ ПРОТОКОЛОВ	-	+	+	-	+	+
ПОДДЕРЖКА PLUG & PLAY	+	+	+	-	+	+
ПОДДЕРЖКА АУДИОЗАПИСИ	+	+	-	-	+	+
ВОЗМОЖНОСТЬ УСТАНОВКИ ДАТЧИКОВ ДВИЖЕНИЯ	+	+	-	-	+	+
УДАЛЕННОЕ УПРАВЛЕНИЕ	+	+	+	-	+	+
		1570			1300	

Стоимость, руб.	8400	0	11200	7800	0	9000
-----------------	------	---	-------	------	---	------

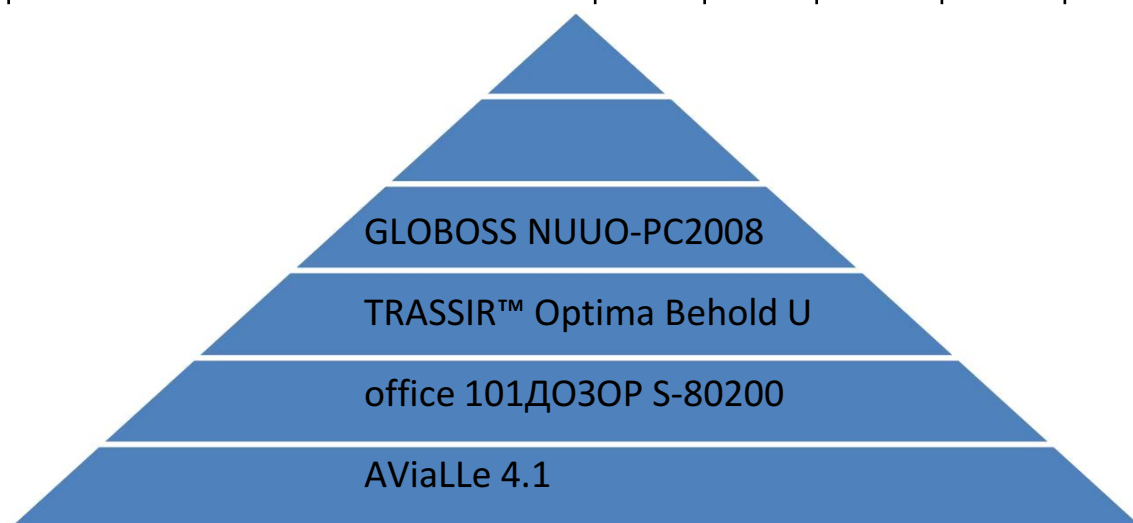


Рисунок 51 – Иерархия современных существующих СВН

Из таблицы 2 видно, что самой удобной и универсальной из рассмотренных систем является ПАК СВН «КОДОС – GLOBOSS».

СВН «GLOBOSS» представляет собой систему, построенную на базе ПК. Состоит из плат видеоввода и ПО, отвечающего за сжатие, запись и другую обработку видеосигнала и предоставляющего пользователю соответствующие инструменты управления.

В СВН «GLOBOSS» используются 2 типа плат видеоввода: с программным (компрессия видеопотока осуществляется центральным процессором ПК) и аппаратным сжатием (компрессия видеопотока производится средствами аппаратных кодеков плат видеоввода).

Кроме видеосигналов аналоговых видеокамер, СВН «GLOBOSS» может обрабатывать видеосигналы, поступающие от IP и USB-видеокамер.

Система видеонаблюдения «GLOBOSS» обеспечивает:

захват видеосигналов, поступающих от аналоговых, IP- и USB-
видеокамер;

захват аудиосигналов, поступающих от микрофонов; просмотр на мониторе

изображений с видеокамер; сжатие, запись в архив, передачу по сети изображения и звука, поступающих с соответствующих источников; объединение в единую Систему множества серверов «GLOBOSS» и клиентов; управление режимом записи в архив; просмотр и прослушивание архивных записей;

выведение кадров видеозаписи на печать; распределение между несколькими пользователями прав доступа к видеоданным, архивам, командам управления и настройкам СВН; управление поворотными устройствами видеокамер. Технологии цифровой видеорегистрации принадлежат к числу тех быстроразвивающихся областей, где находит применение самая современная элементная база и самые последние технические и программные решения.

Система «GLOBOSS» выполняет следующие функции:

Преобразование видеосигналов, поступающих с аналоговых видеокамер, в цифровой вид;

передачу видеоизображения с объекта по каналам передачи данных; просмотр изображения с видеокамер в многооконном режиме, в режиме последовательного просмотра, в полноэкранном формате, в режиме повышенной бдительности; архивация видеоизображения архивацию видеоизображений на диск ПК; запись архивов на сменные носители информации;

управление записью в архив: вручную, по детектору движения, по детектору звука, по сигналам внешних датчиков, по планировщику, осуществление претревожной записи событий с заданной длительностью;

удаленный просмотр видеоизображения в реальном времени, прослушивание звука, просмотр видеоархивов с множества серверов на рабочих местах администраторов и операторов системы видеонаблюдения;

управление исполнительными устройствами видеокамер (поворотными, управляющими оптическим приближением);

управление стандартными видеоустройствами (квадраторами, мультиплексорами); распечатку отдельных кадров на принтере.

взаимодействие с ИКБ, позволяя ИКБ принимать и передавать видео,

давать команды на запись, получать события от детектора движения. Обобщенная структурная схема цифровой системы видеонаблюдения «GLOBOSS» представлена на рисунке (Рисунок 2).

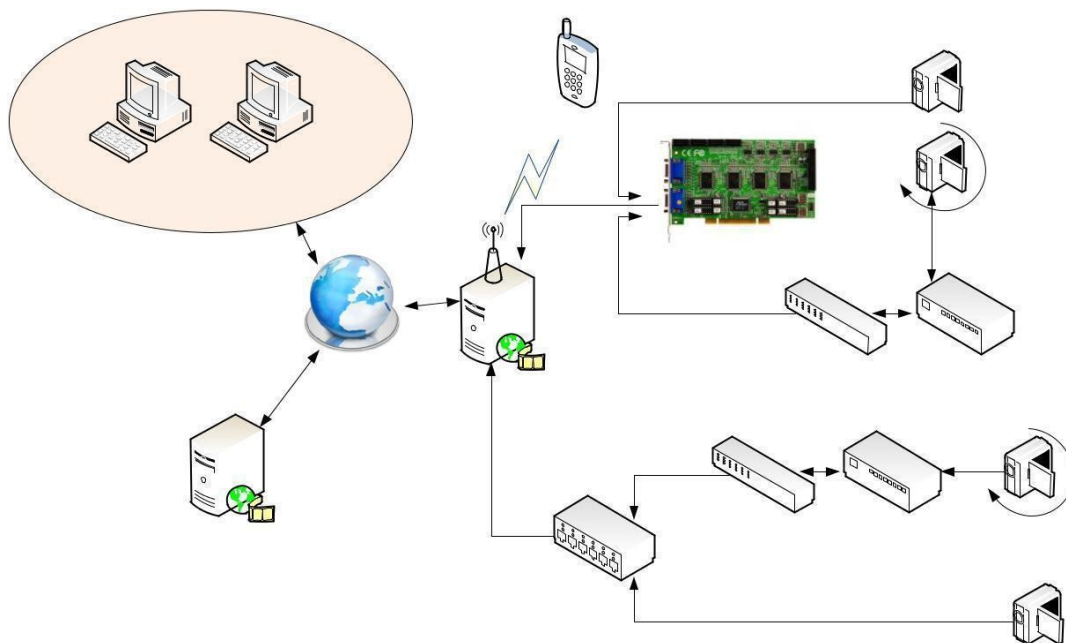


Рисунок 52 – Обобщенная структурная схема цифровой системы видеонаблюдения «GLOBOSS»

В состав системы «GLOBOSS» входят: аналоговые видеокамеры;

IP видеокамеры;

USB видеокамеры; платы видеоввода; микрофоны;

IP видеокоммутаторы.

контроллеры управления поворотными устройствами;
компьютеры с установленным специализированным ПО.

Особенности системы «GLOBOSS»:

транспортной средой для системы «GLOBOSS» является сеть TCP/IP;

экономное использование сетевого ресурса. Достигается путем использования специализированного высокоэффективного фирменного формата сжатия видеокadra;

простота конфигурирования системы; удобство работы с видеоархивом;

ежеквартальное бесплатное обновление ПО системы «GLOBOSS».

При выборе места установки видеокамер необходимо исходить из нескольких факторов: целей и задач видеонаблюдения конкретного объекта,

технической возможности прокладки до места установки камеры сигнального и питающего кабеля, эстетических соображений.

Идеальный способ выбора места установки – встать на точку установки видеокамеры и посмотреть, что вы сможете увидеть, применяя систему видеонаблюдения. При этом необходимо помнить, что стандартный объектив (2,8- 3,6 мм) имеет угол обзора около 90°.

Кабель от видеосервера до видеокамер желательно прокладывать в коробах или гофротрубе, даже в том случае если он идет под подвесным потолком. Поэтому при выборе места установки продумайте как вы проложите короба, или скроете кабель каким-либо другим способом.

При установке видеокамер на подвесной потолок рекомендуем использовать купольные камеры, как наиболее удобные по установке и идеально подходящие по дизайну.

Для установки скрытой камеры можно использовать датчик детектора движения охранно-пожарной сигнализации. Потенциальный объект наблюдения не заподозрит в установленном приборе видеокамеру.

Для выбора видеокамеры и формирования технического задания необходимо учитывать:

1. Какой участок охраняемой территории необходимо наблюдать. Это может быть строение, контрольно-следовая полоса, крыша или фасад здания,

коридор, холл, кабинет, склад и т.д. Для наблюдения узких и длинных участков (контрольно-следовая полоса, коридор, фасад здания) потребуется объектив с АРД и углом обзора от 15° до 30°. Объектив с ручной/фиксированной диафрагмой не позволит получить необходимую глубину резкости. Для наблюдения за обширной территорией (крыша, холл, кабинет, склад и т.д.) необходимо установить объектив (можно и с

фиксированной диафрагмой) с углом обзора от 60° до 90°. При углах обзора более 90° на изображении появляются сильные геометрические бокообразные искажения.

2. Особенности территории наблюдения, такие, как большая площадь, ограниченные возможности прокладки телекоммуникационных линий, сложность рельефа, удаленность от центрального пункта наблюдения и т.п. 3.

На каком расстоянии от центра мониторинга необходимо установить видеокамеру. Это определяет способ передачи видеосигнала и качество полученного изображения Составим принципиальную схему системы видеонаблюдения объекта

(рисунок 3). Определяем точки, в которых будет произведена установка камер

На основании требований того, что должно быть видно, выбираются соответствующие зоны видеонаблюдения (используя план помещений).

Желательно, чтобы в поле зрения видеокамер попадало максимальное количество дверей, коридоров, лестниц, с тем, чтобы злоумышленник был бы обнаружен при любой траектории его движения. Особенно важными с точки зрения безопасности являются въезды и выезды, ворота и прилегающие к ним территории, заборы, дворы, стоянки автомобилей.

Сервер ИКБ

Аналоговая «КОДОС» IP видеокамера видеокамера

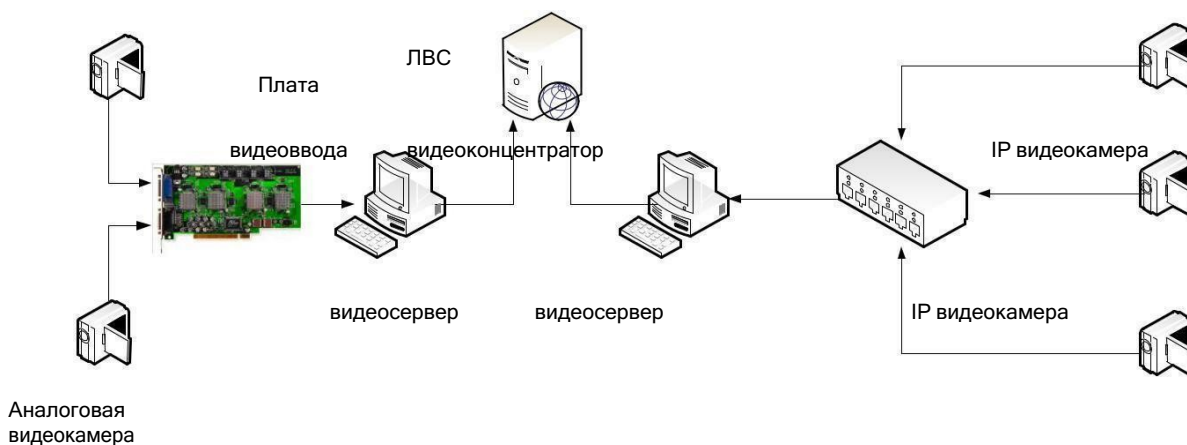


Рисунок 53 – Принципиальная схема видеонаблюдения

Для мониторинга обстановки в контролируемой зоне размер изображения человека по вертикали должен составлять порядка 5% от высоты экрана (непонятно, человек или собака, но что-то движется), для четкого обнаружения человека размер должен составлять 10%, для узнавания человека размер должен быть 50%, для идентификации, для опознавания размер должен быть 120% от высоты экрана .

Далее выбираются наиболее удобные места крепления видеокамер. Это определяет ракурсы наблюдения (например, можно повесить видеокамеру прямо перед входом, но тогда будут видны одни лишь макушки голов,

которые для опознавания не всегда пригодны). При выборе мест размещения видеокамер следует прогнозировать влияние возможных препятствий -

деревьев, кустов, распахивающихся дверей. Следует исключить попадание в поле зрения видеокамеры источников света (прямые солнечные лучи, огни рекламы, осветительные фонари, фары автомобилей), а также отражений от создающих блики поверхностей (вода, стекла и пр.). При этом должен обеспечиваться необходимый для нормальной работы видеокамеры уровень освещенности. Предлагаемые технические решения должны быть комплексными: если предлагаете использовать видеокамеру с питанием от источника постоянного тока или инфракрасный осветитель, сразу же следует решать вопрос о необходимом блоке питания, не забыть выбрать кронштейн, термокожух и т.д.

Видеокамера, как и любой прибор системы безопасности, может стать объектом диверсии. Борьба с вандализмом происходит в следующих направлениях: используют специальные кожухи и кронштейны, затрудняющие повреждение или похищение видеокамеры, применяют специальные схемотехнические решения (тревога при попытке снять кронштейн или приблизиться к нему, при пропадании видеосигнала), используют пассивную форму защиты (видеоглазки, скрыто установленные

видеокамеры) - приборы как бы мимикрируют в окружающей среде и эффективны до тех пор, пока не обнаружены злоумышленниками.

Точка расположения видеокамеры и подлежащие наблюдению объекты образуют сектор наблюдения. Определение оптимального количества таких секторов является многовариантной задачей. Недостаточное количество видеокамер приводит к наличию в пространстве так называемых –мертвых зон. Чрезмерное количество видеокамер приводит к неоправданному повторению схожих изображений. Естественно, что это ведет к росту стоимости оборудования (видеокамеры, объективы, кронштейны, кожухи,

кабели), усложнению оборудования обработки видеосигналов, а значит, и к удорожанию видеосистемы. С другой стороны, увеличение числа каналов приводит к уменьшению времени наблюдения по каждой зоне, к уменьшению размеров изображения при мультисценовом отображении на видеомониторе – вместо ожидаемого повышения информативности видеосистемы происходит ее уменьшение. Выбранные секторы наблюдения однозначно определяют углы обзора видеокамер (либо расстояния до объекта и поля зрения). На основании этих параметров и знания форматов видеокамер определяются фокусные расстояния объективов.

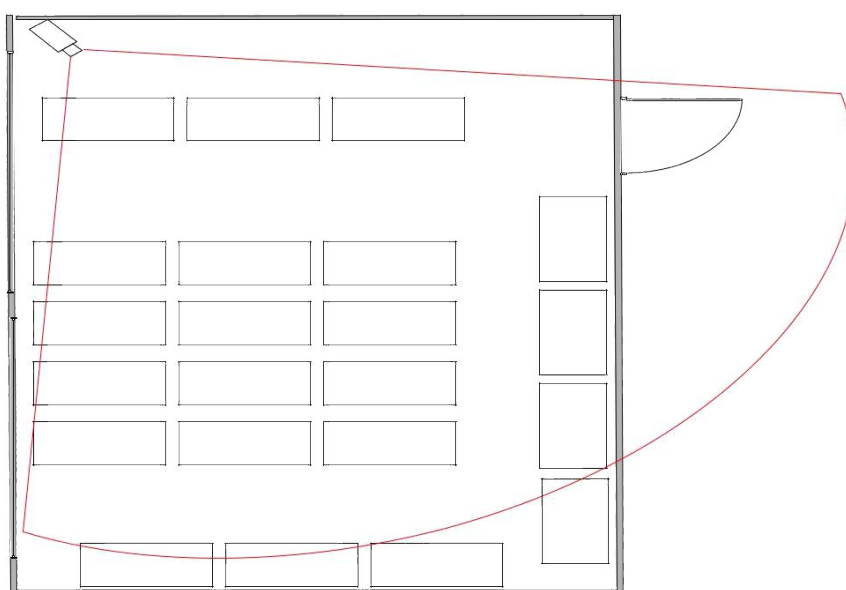


Рисунок 54 – Вариант размещения видеокамер на кафедре защиты информации

Все силовые линии должны быть скрыты во избежание диверсии.

Монтаж (установка) видеонаблюдения как и монтаж любых слаботочных систем, предполагает точное соблюдение основных руководящих и нормативных документов, с учетом специфики, связанной с техническими особенностями систем видеонаблюдения - высокой зависимостью от влияния различных помех, сложной настройкой оборудования, зависимости от погодных условий. Особенно много "подводных камней" при монтаже

(установке) и настройке уличных систем видеонаблюдения. Основные технические особенности, характеристики объекта влияющие на процесс подготовки к монтажным работам должны быть учтены на этапе обследования объекта и использованы при подготовке технического предложения по монтажу системы видеонаблюдения.

Полученная система видеонаблюдения предназначена для определения факта несанкционированного проникновения на охраняемый объект, факта присутствия персонала на объекте, факта кражи и порчи имущества, а также при интеграции в ИКБ «КОДОС» выдачи сигнала тревоги и включения исполнительных устройств (световых и звуковых оповещателей, реле и т. п.).

Оборудование и материалы

4. Стенд охранно-пожарной сигнализации КОДОС
5. Стенд системы контроля и управления доступом КОДОС
6. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

5. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
6. Запрещается включать любое оборудование при снятом защитном кожухе.
7. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
8. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Сравнительный анализ аналоговых и цифровых систем видеонаблюдения. Вывод в краткой форме о преимуществах и недостатках каждой из них, целесообразности применения каждой из них.
2. Изучение характеристик выбранной системы аналогового видеонаблюдения.
3. Изучения характеристик выбранной системы цифрового видеонаблюдение.
4. Изучение типовой схемы использования выбранной системы аналогового видеонаблюдения.

5. Изучения типовой схемы использования выбранной системы цифрового видеонаблюдения.

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполнения индивидуального задания лабораторной работы.
5. Вывод.

Контрольные вопросы

- 1) Перечислите достоинства и недостатки аналоговых систем видеонаблюдения?
- 2) Перечислите достоинства и недостатки цифровых систем видеонаблюдения?
- 3) Какие разъёмы в ПК используются для подключения цифровых систем видеонаблюдения?
- 4) Назовите основные компоненты аналоговой системы видеонаблюдения?
- 5) Назовите основные компоненты цифровой системы видеонаблюдения?

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»

3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.:Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с.

ТЕМА 5. ПОДБОР СОТРУДНИКОВ И РАБОТА С КАДРАМИ
ТЕМА 6. ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ РЕЖИМА СЕКРЕТНОСТИ НА ОБЪЕКТЕ
Практическая работа №19-20

Цель: получить практические навыки по установке и настройке системы видеонаблюдения на примере системы видеонаблюдения «GLOBOSS».

Теоретическое обоснование



GLOBOSS - система видеонаблюдения. В бесплатном варианте поддерживает 4 подключения. Возможно использование обычных веб-камер.

Бесплатная версия системы видеонаблюдения GLOBOSS является полнофункциональной!

Ограничения:

Максимум 2 канала захвата и суммарно 4 канала отображения (то есть,

могут быть такие конфигурации: 2 канала захвата + 2 канала отображения из сети, 4 канала отображения из сети и т.п.).

Бесплатная 2-канальная версия GLOBOSS не работает совместно с коммерческой версией. Нельзя поставить несколько бесплатных систем и вывести на ПО администратора коммерческой версии. Бесплатная версия работает только с бесплатной, а коммерческая – с коммерческой.

Функции:

Поддержка аналоговых и ip-камер, поворотных устройств

Мощный детектор движения (технология ScanMove)

Детектор звука

Интеллектуальный алгоритм сжатия для охранного видеонаблюдения
(кодэк Morsa)

Обработка до 800 кадров/сек на одном сервере

Удаленный просмотр и управление по сети и через интернет

Разрешение 768x576 для аналоговых камер без эффекта "гребёнки"
(алгоритм Improve-S)

Отправка тревожных сообщений на e-mail и мобильный телефон

Система прав доступа для пользователей

Эффективный анализатор событий

Удобная работа с архивом

Автоматический поиск подключенных камер

Планировщик заданий

Вывод изображения на несколько мониторов

Трансляция в интернет

Передача изображений на КПК

Выбор цветности выводимого изображения Система функционирует
самостоятельно или с интегрированным

комплексом безопасности «ИКБ КОДОС», а также поддерживает
дополнительно устанавливаемый модуль web-трансляции «GLOBOSS WEB».

Состав ПО системы «GLOBOSS» :

Видео ИКБ/4 (Поддержка любой платы «КОДОС». Количество каналов видео-4. Количество кадров в секунду на канал определяется конфигурацией системы).

Видео ИКБ/8 (Поддержка любой платы «КОДОС». Количество каналов видео-4. Количество кадров в секунду на канал определяется конфигурацией системы).

«GLOBOSS»-ЗВУК (используется для подключения звуковых каналов к системе «GLOBOSS»).

ПО для сетевой интегрированной системы охранного видеонаблюдения (используется только совместно с программной оболочкой ИКБ «КОДОС».

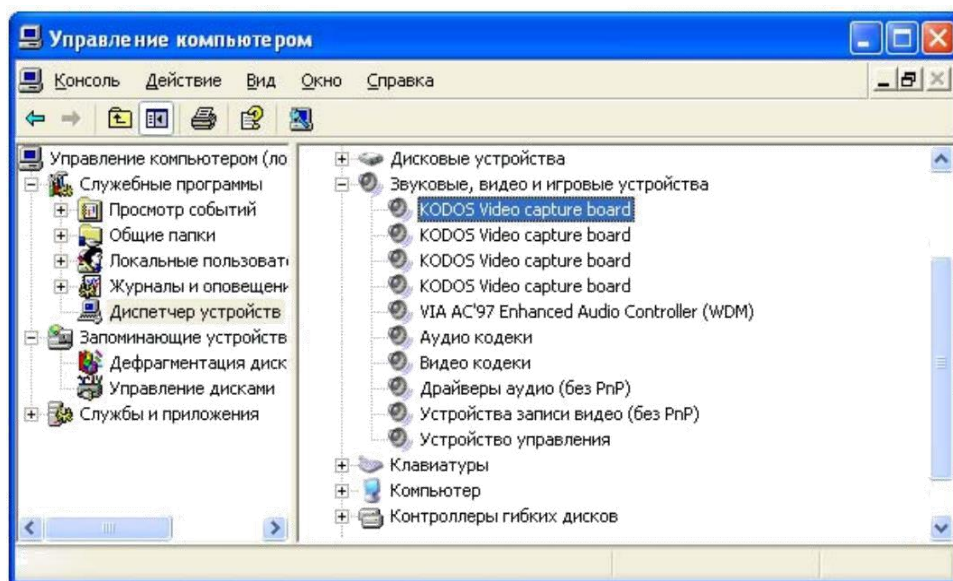
Дает возможность настраивать параметры записи видеоизображения. При конфигурировании системы на планах охраняемых помещений размещаются изображения подключенных видеокамер. Просмотр изображения с видеокамеры производится щелчком мыши по пиктограмме камеры.).

ПО «GLOBOSS» (ПО «GLOBOSS» с сетевыми возможностями для оцифрованного видеосигнала аналоговых IP-, USB-и web-камер).

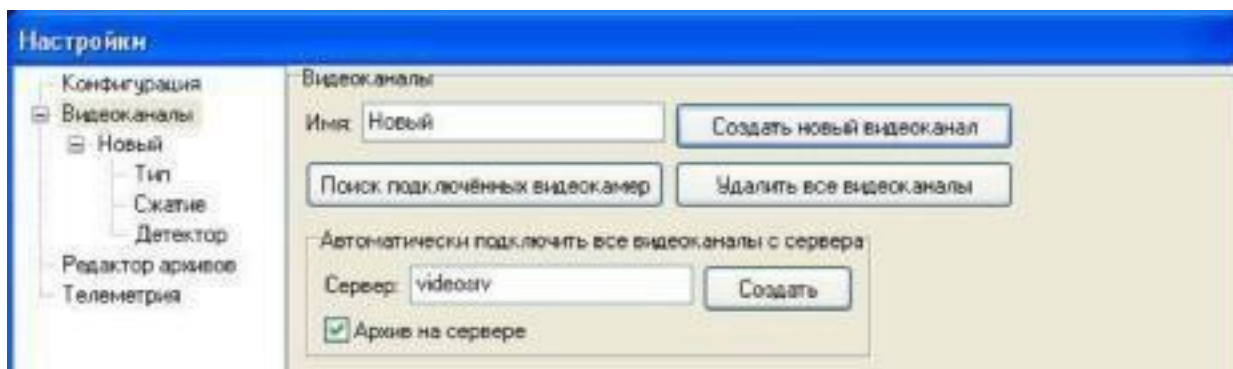
Программа удалённого администрирования «GLOBOSS» (Рабочее место оператора или администратора системы. Используется для удалённого администрирования и просмотра архива видеозаписей системы видеонаблюдения).

После установки и ввода лицензии программа запускается нажатием на пиктограмму файла «KodosVideo.exe» или командой: «Пуск»>«Все программы»>«GLOBOSS»>«GLOBOSS» .

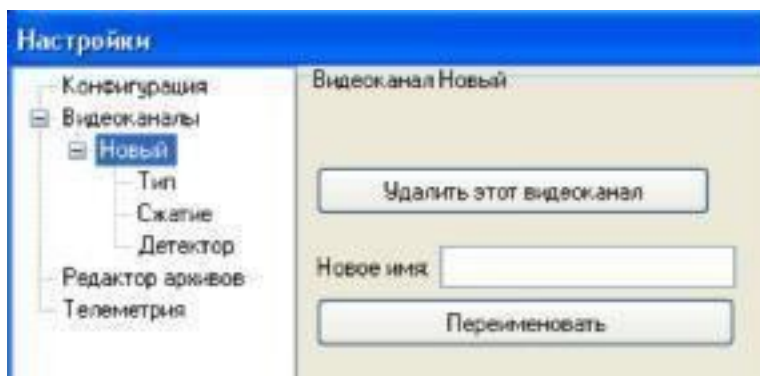
При первом запуске программы откроется основное окно программы. Из него подаются все команды по управлению системой видеонаблюдения.



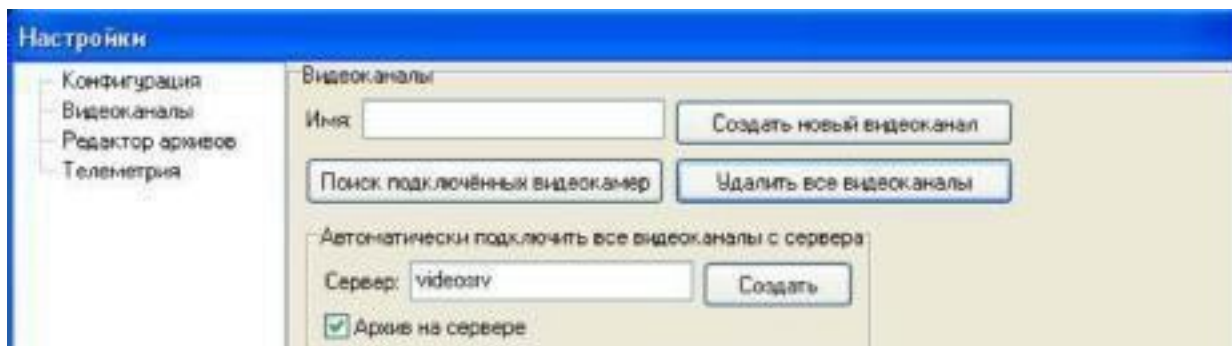
Для добавления нового видеоканала необходимо ввести имя видеоканала в строке «Имя» и нажать кнопку «**Создать новый видеоканал**»



Новый видеоканал будет добавлен в поле слева. Для удаления видеоканала следует выбрать его в левом поле и нажать кнопку «**Удалить этот видеоканал**»

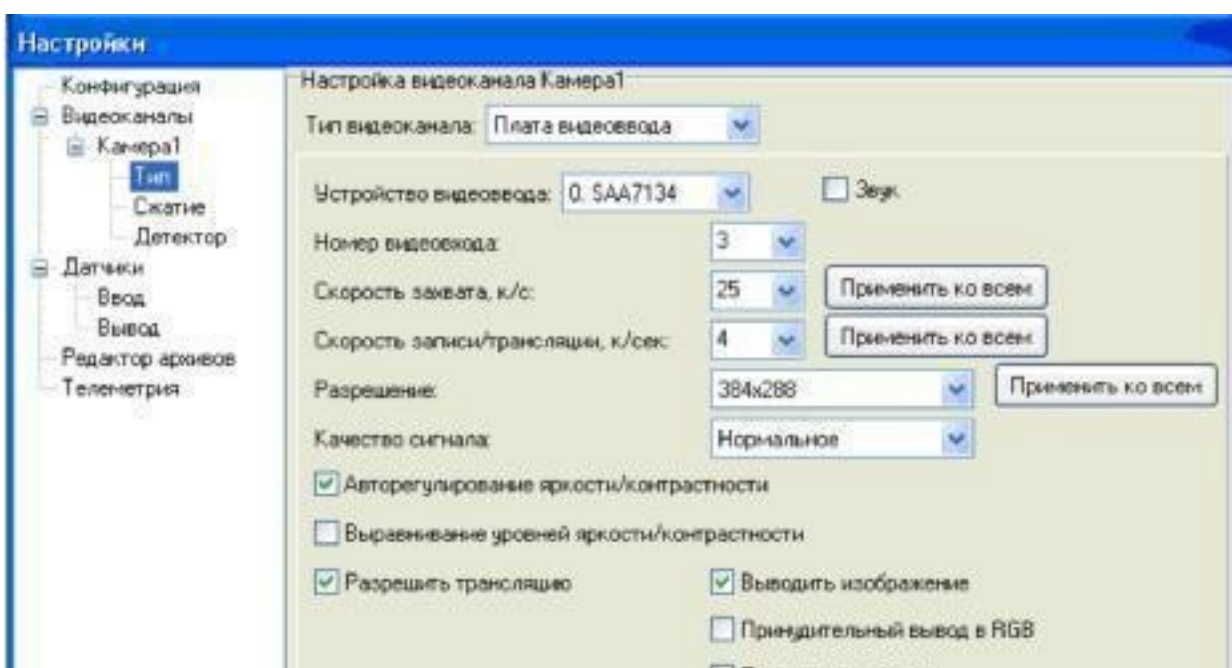


Для переименования ввести новое имя в строке «**Новое имя**» и нажать кнопку «**Переименовать**». Для удаления всех видеоканалов нажать кнопку «**Удалить все видеоканалы**»

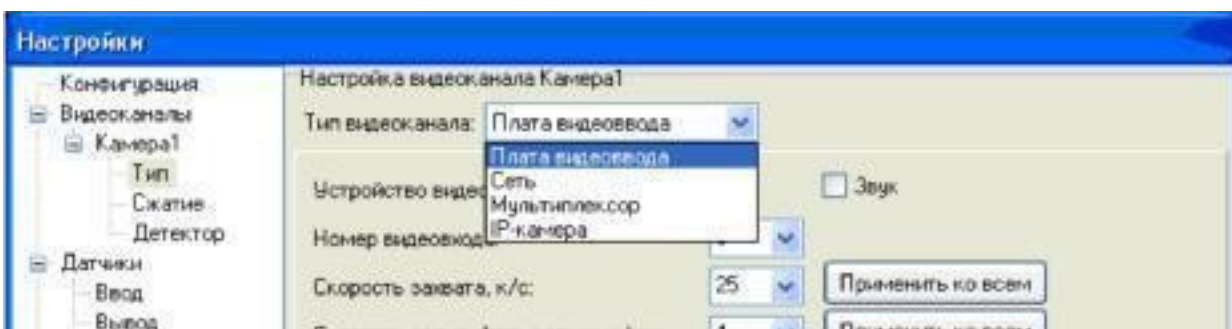


По окончании нажать кнопку «**ОК**».

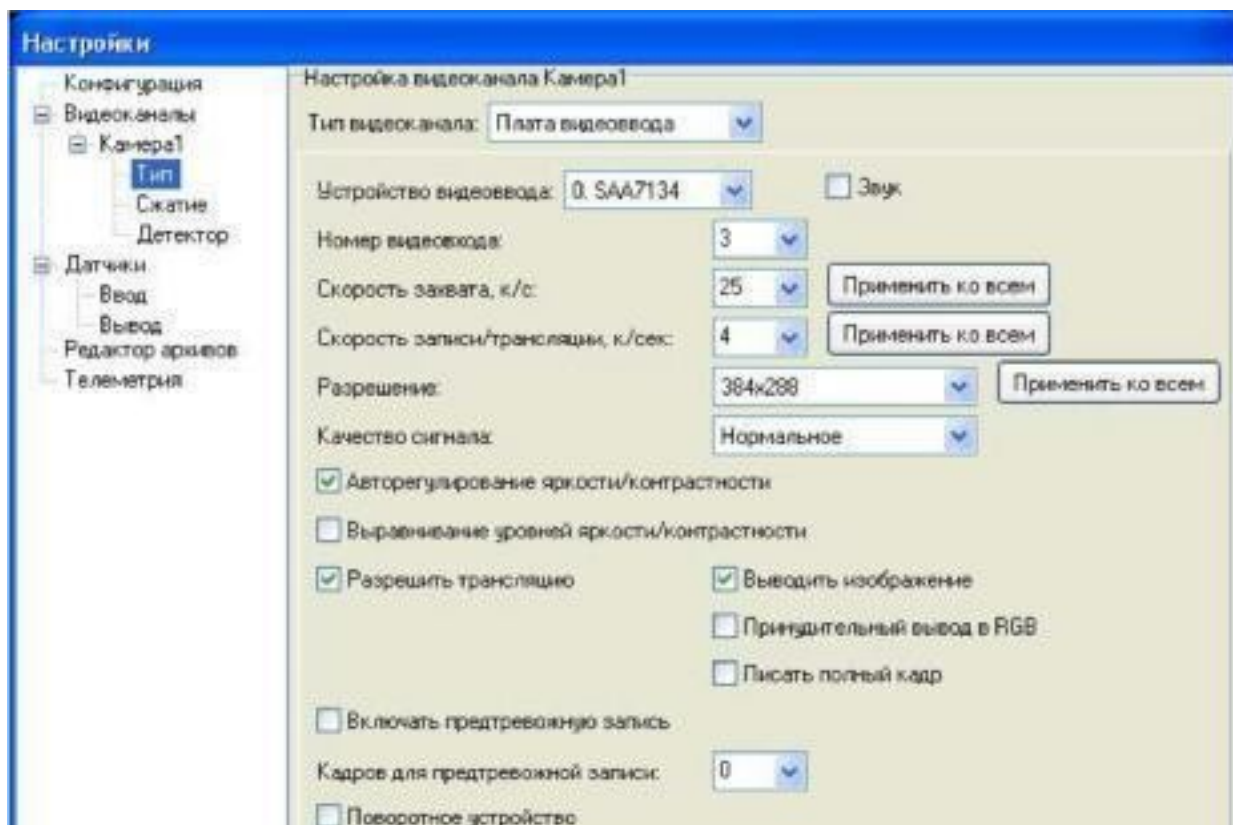
Для настройки типа видеоканала выбрать «**Тип**» в левом поле. Правое поле изменится



В строке со списком «**Тип видеоканала**» выбрать тип



Настройка типа видеоканала «Плата видеоввода»



«**Устройство видеоввода**» – выбрать плату из списка.

«**Звук**» - при установленном флажке появится кнопка «**Настройка звука...**».

«**Номер видеовхода**» – выбрать номер входа из списка, куда подключена камера.

«**Скорость захвата**» – выбрать из списка скорость захвата. При нажатии

«**Применить ко всем**» параметр будет установлен для всех видеовходов платы.

«**Скорость записи/трансляции, к/сек**» – выбрать из списка скорость записи.

При этой же скорости будет транслироваться видео в сеть. При нажатии

«**Применить ко всем**» параметр будет установлен для всех видеовходов платы.

«**Разрешение**» - выбирается разрешение изображения на данном канале.

При нажатии «**Применить ко всем**» параметр будет установлен для всех

ВИДЕОВХОДОВ ПЛАТЫ.

«**Качество сигнала**» - выбирается качество изображения на данном канале.

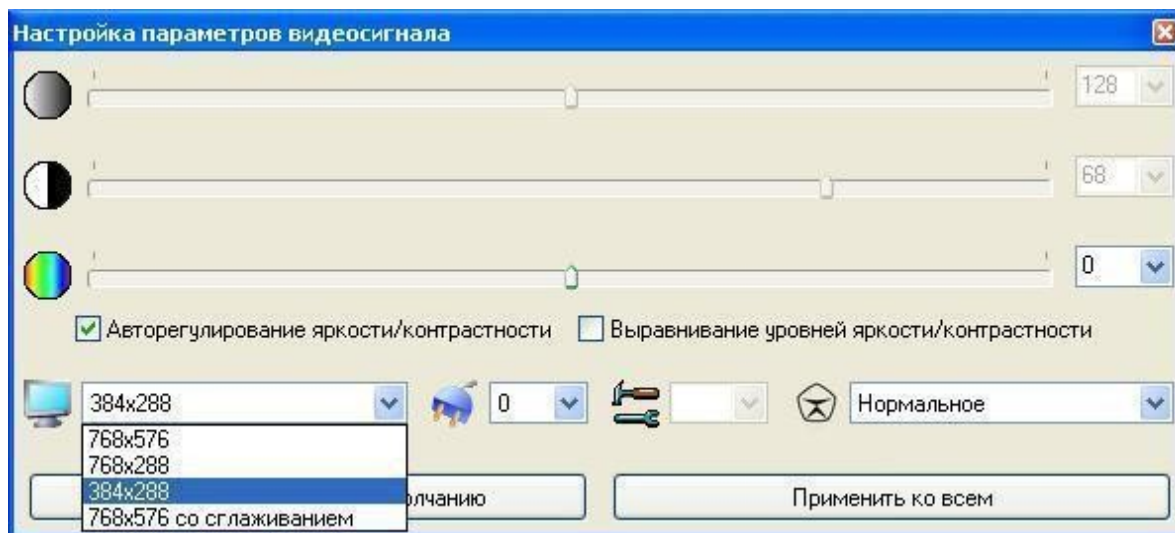
«**Авторегулирование яркости/контрастности**» - при включенной опции авторегулирование яркости/контрастности выполняется анализ изображения на предмет его "засвеченности" или "затемненности". На основе этого анализа значения яркости и контрастности автоматически меняются на оптимальные.

«**Выравнивание уровней яркости/контрастности**» - при включенной этой опции изображение обрабатывается по специальному алгоритму, чтобы при сильной «засвеченности» или «затемненности» скорректировать изображение для оптимального просмотра.

«**Разрешить трансляцию**» – при установленном флажке к каналу можно подключиться по сети.

«**Выводить изображение**» – при установленном флажке изображение будет выводиться.

«**Принудительный вывод в RGB**» – режим используется на слабых видеокартах.

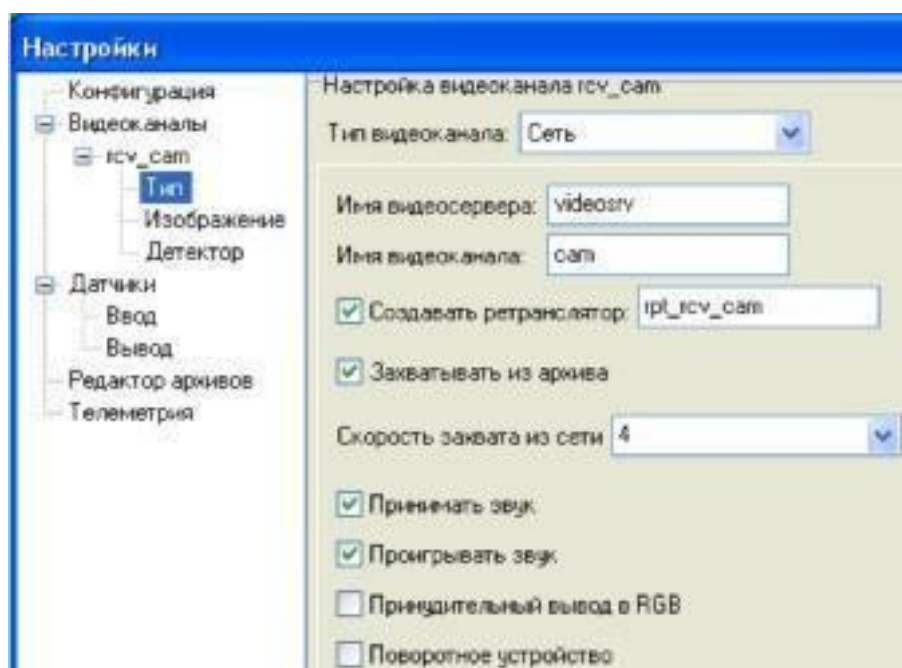


«**Включать предтревожную запись**» – при установленном флажке предтревожная запись будет активна. Предтревожная запись – это запись установленного количества кадров предшествующих наступлению события.

«**Кадров предтревожной записи**» – выбрать из списка количество кадров предтревожной записи.

«**Поворотное устройство**» – при установленном флажке будут доступны настройки поворотных устройств.

Настройка типа видеоканала «**Сеть**»



сервера, откуда передается видео.

«**Имя видеоканала**» - имя канала, откуда передается видео. «**Создавать ретранслятор**» - при установленном флажке будет создан

передатчик, который сможет ретранслировать принимаемое видео.

«**Захватывать из архива**» - при установленном флажке на сервере

будет создан передатчик, берущий видео из архива по пути, указанном в параметре «**Имя видеоканала**».

«**Скорость захвата из сети**» - максимальная скорость приема данных от передатчика.

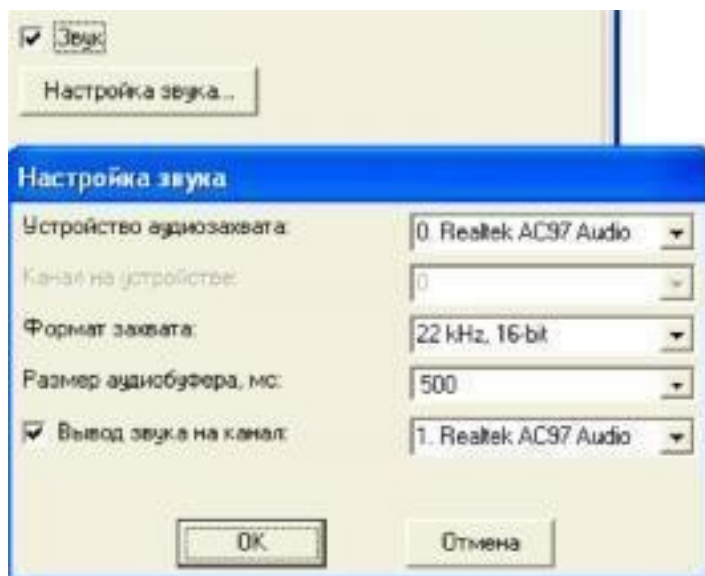
«**Принимать звук**» - при установленном флажке будет принимать звук от передатчика.

«**Проигрывать звук**» - при установленном флажке будет проигрываться полученный звук от передатчика.

По окончании настроек нажать кнопку «**ОК**».

Настройка устройств вывода звука

Нажать кнопку «**Настройка звука**», появится соответствующее окно.



«**Устройство аудиозахвата**» – указать плату аудиозахвата из списка.

Если это многоканальная плата, то будет доступна строка «**Канал на устройстве**».

«**Формат захвата**» – указать формат захвата аудиопотока из списка. «**Размер аудиобуфера**» – выбрать значение буфера из списка.

«**Вывод звука на канал**» - при установленном флажке будет доступен выбор канала вывода звука.

По окончании настроек нажать кнопку «**ОК**».

Настройка поворотного устройства

Подробно подключение и настройка поворотных устройств описана в



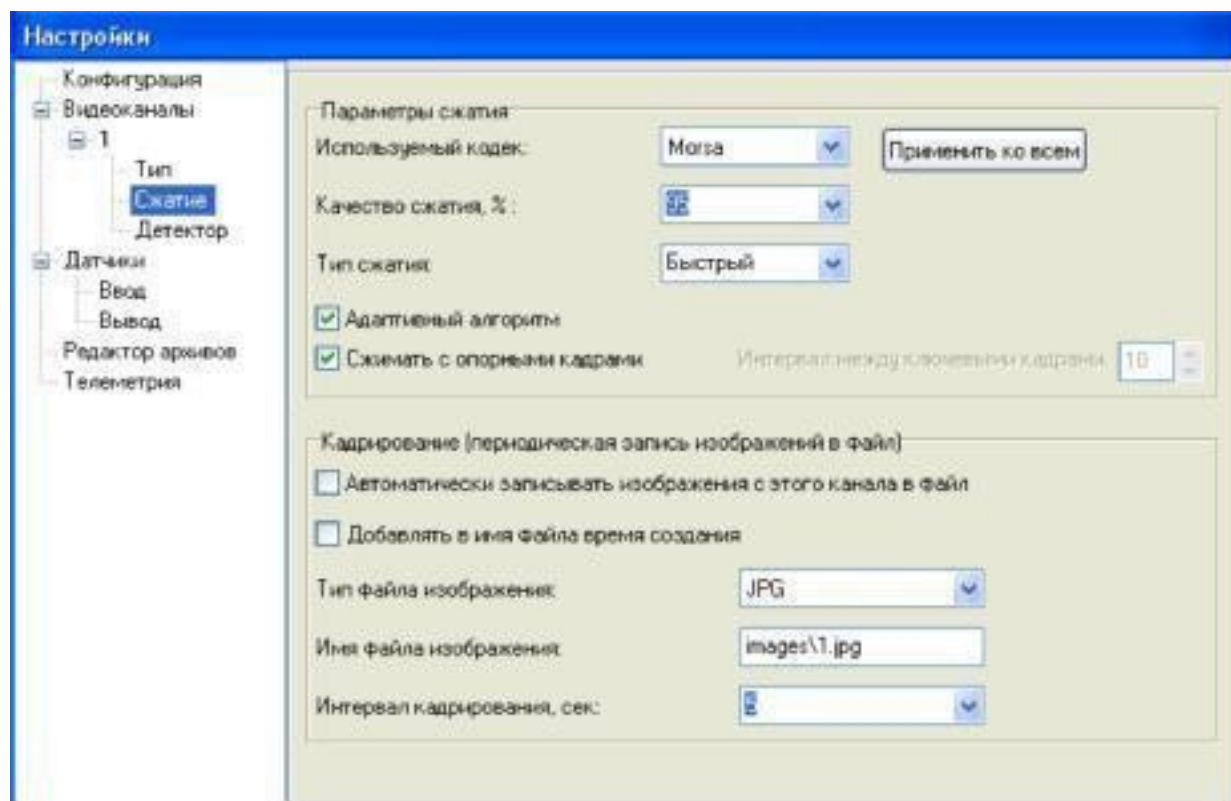
«**Тип поворотного устройства**» – выбрать из списка тип устройства. У разных типов устройств настраиваются разные параметры. «**IP адрес**» – IP адрес устройства.

«**Номер устройства**» – идентификационный номер устройства.

«**Логин**» – логин для доступа к управлению поворотником. «**Пароль**» – пароль для доступа к управлению поворотником.

По окончании настроек нажать кнопку «**ОК**».

Для настройки сжатия выбрать «**Сжатие**» в левом поле. Правое поле изменится



Параметры сжатия.

«**Используемый кодек**» – выбрать кодек из списка, по умолчанию используется кодек «**Morsa**». Для плат SecTORR 8EDV, кодек по умолчанию HDWC.

«**Качество сжатия**» – выбрать качество сжатия из списка. Чем выше значение, тем выше процент соответствия оригиналу.

«**Тип сжатия**» – выбрать тип сжатия из списка. «**Быстрый**» - высокая

скорость сжатия, с опорными кадрами или без. **«Медленный»** - все кадры опорные. **«Смешанный»** - низкая скорость сжатия, кадры меньшего размера, чем на быстром, работает по схеме с опорными кадрами.

«Адаптивный алгоритм» – кодек сжатия подстраивается под конкретное изображение. Время сжатия возрастает на **5-10%**, размер картинки падает на **10%**.

«Сжимать с опорными кадрами» – берётся один опорный кадр, следующие несколько кадров - относительные, в них остаётся только та часть, которая изменилась по сравнению с опорным. За счёт этого снижается средний размер кадров в видеопотоке. Если эта опция не выставлена - все кадры опорные.

Запись статичных изображений.

«Автоматически записывать изображения с этого канала в файл» –

при выставленном флажке изображение будет записываться в файл автоматически.

«Добавлять в имя файла время создания» – при выставленном флажке в имя файла будет добавлено время создания файла.

«Тип файла изображения» – выбрать из списка тип сохраняемого файла.

«Имя файла изображения» – задать имя сохраняемых файлов изображения.

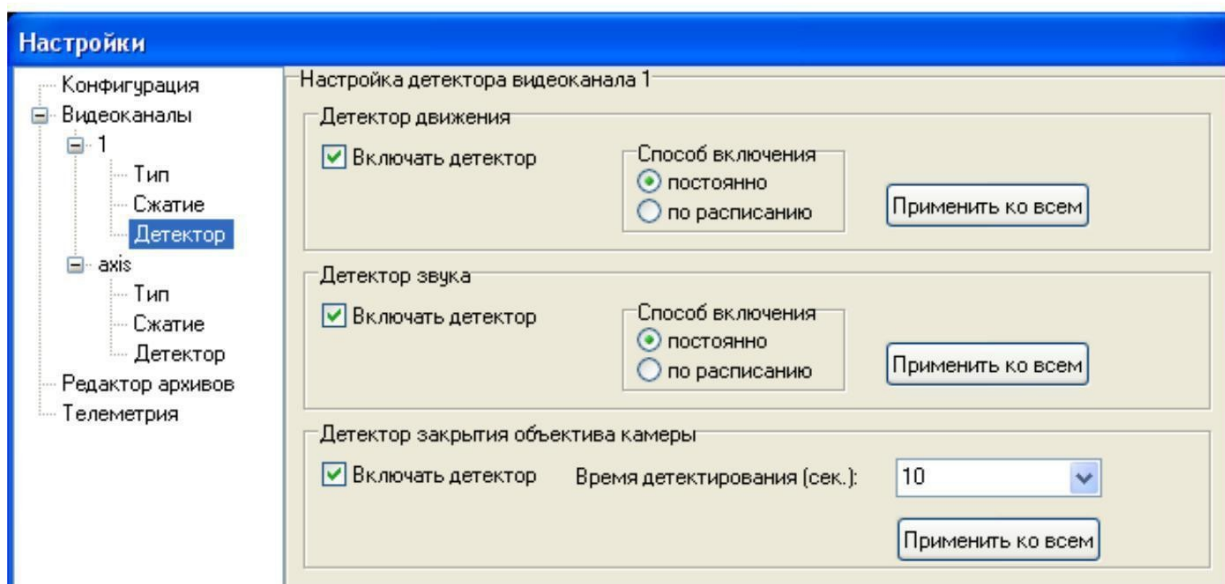
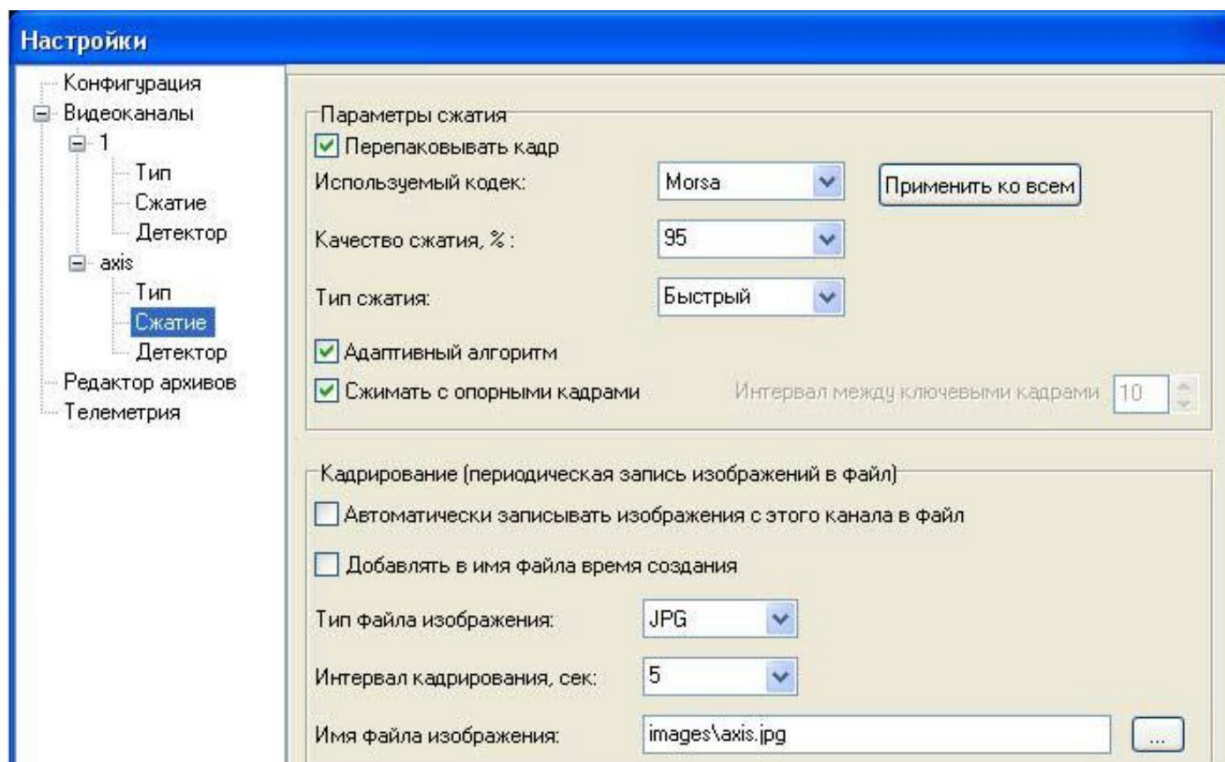
«Период записи изображения» – выбрать из списка период записи файла. По

окончании настроек нажать кнопку **«ОК»**. Кодек XViD

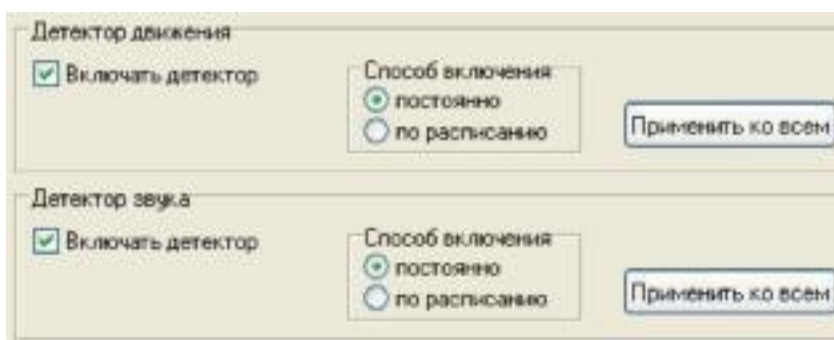
оптимизирован под слабые процессоры прошлого поколения. Использование данного кодека снижает скорость записи в архив и передачи в сеть, но при этом существенно снижается нагрузка на процессор. Настоятельно не рекомендуется использовать данный кодек на новых процессорах – Intel Core 2 Quad и Intel Core 2 Duo, а также на других многоядерных CPU, в связи с несовместимостью оптимизационного алгоритма с многоядерными процессорами. В текущей версии для IP камер **AXIS** и **DLink** по умолчанию видео пишется без перепаковки, т.е. если сигнал приходит в MPEG4 или

MJPEG, то в таком же виде он записывается в архив и транслируется по сети.

При желании можно поставить в этой вкладке применять перепакровку. В этом случае для сжатия будет использоваться выбранный кодек и его параметры. Изображение будет записываться в архив и транслироваться по сети в этом формате сжатия.



Детектор движения и звука

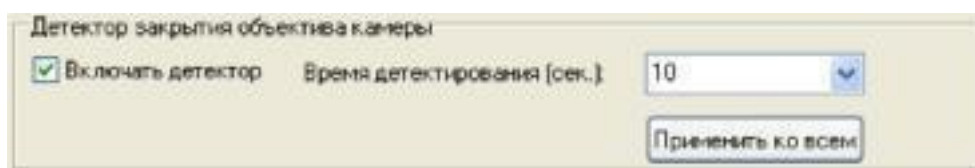


«**Включать детектор**» – при установленном флажке детектор будет включен.

«**Способ включения**» – переключателем установить, «**постоянно**» включенный или включение «**по расписанию**».

«**Применить ко всем**» – назначенные параметры будут применены ко всем видеоканалам.

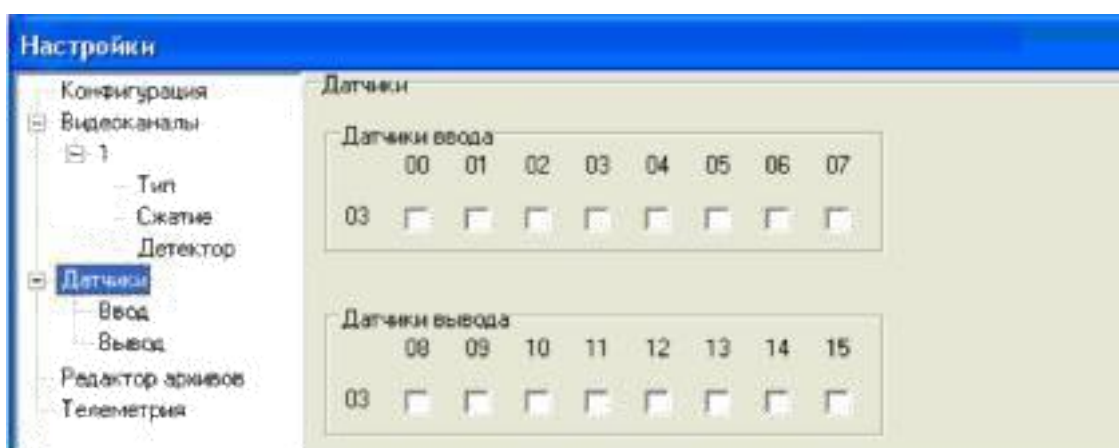
Детектор закрытия объектива камеры (рис. 3.36в).



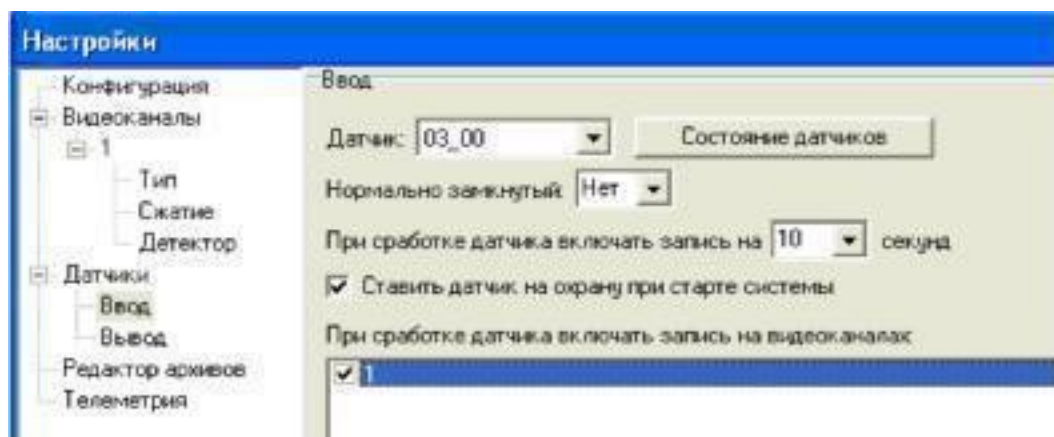
«**Включать детектор**» – при установленном флажке детектор будет включен.

«**Время детектирования (сек.)**» – время, сколько будет закрыта/засвечена камера и после завершения которого сработает детектор .

«**Применить ко всем**» – назначенные параметры будут применены ко всем видеоканалам.



Для настройки датчиков ввода выбрать «**Ввод**» в левом поле. Правое поле изменится



«**Датчик**» - выбрать настраиваемый датчик ввода из списка. «**Нормально замкнутый**» - выбрать состояние, которое будет считаться

нормальным для данного датчика. Другое состояние будет считаться сработкой датчика.

«**При сработке датчика включать запись на ... секунд**» - выбрать из списка продолжительность записи.

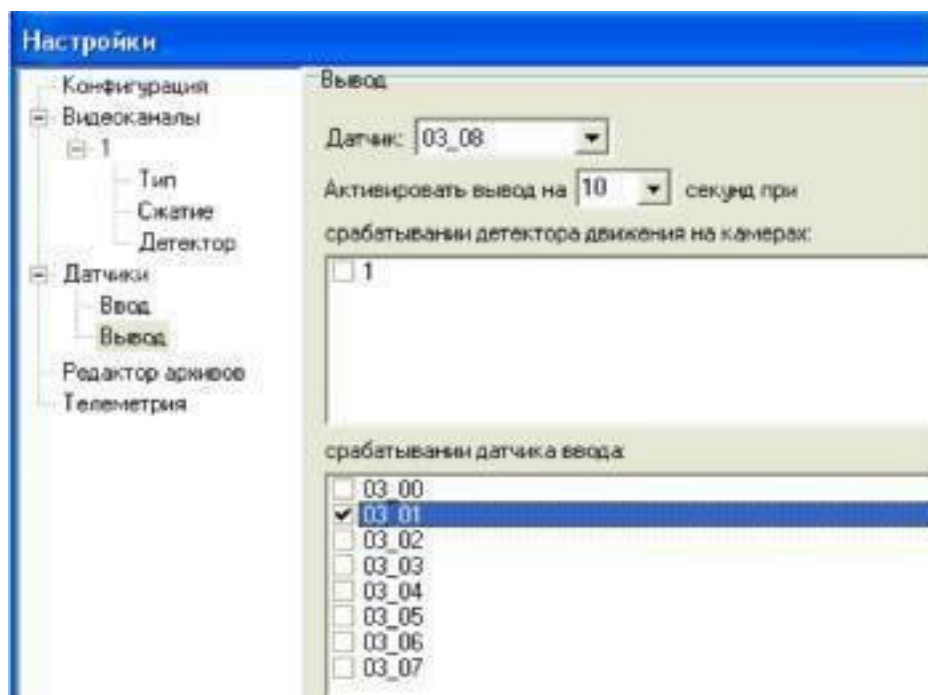
«**Ставить датчик на охрану при старте системы**» - при установленном флажке датчик будет ставиться на охрану при старте системы.

«**При сработке датчика включать запись на видеоканалах**» - установить флажки у тех видеоканалов, на которых необходимо включать запись при срабатывании датчика.

Для просмотра состояния датчиков – нажать «**Состояние датчиков**».

Для принятия изменений нажать «ОК».

Для настройки датчиков вывода выбрать «**Вывод**» в левом поле. Правое поле изменится



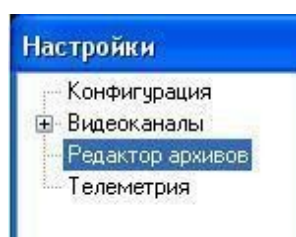
«**Датчик**» - выбрать настраиваемый датчик ввода из списка.

«**Активировать вывод на ... секунд**» - выбрать из списка продолжительность активации вывода.

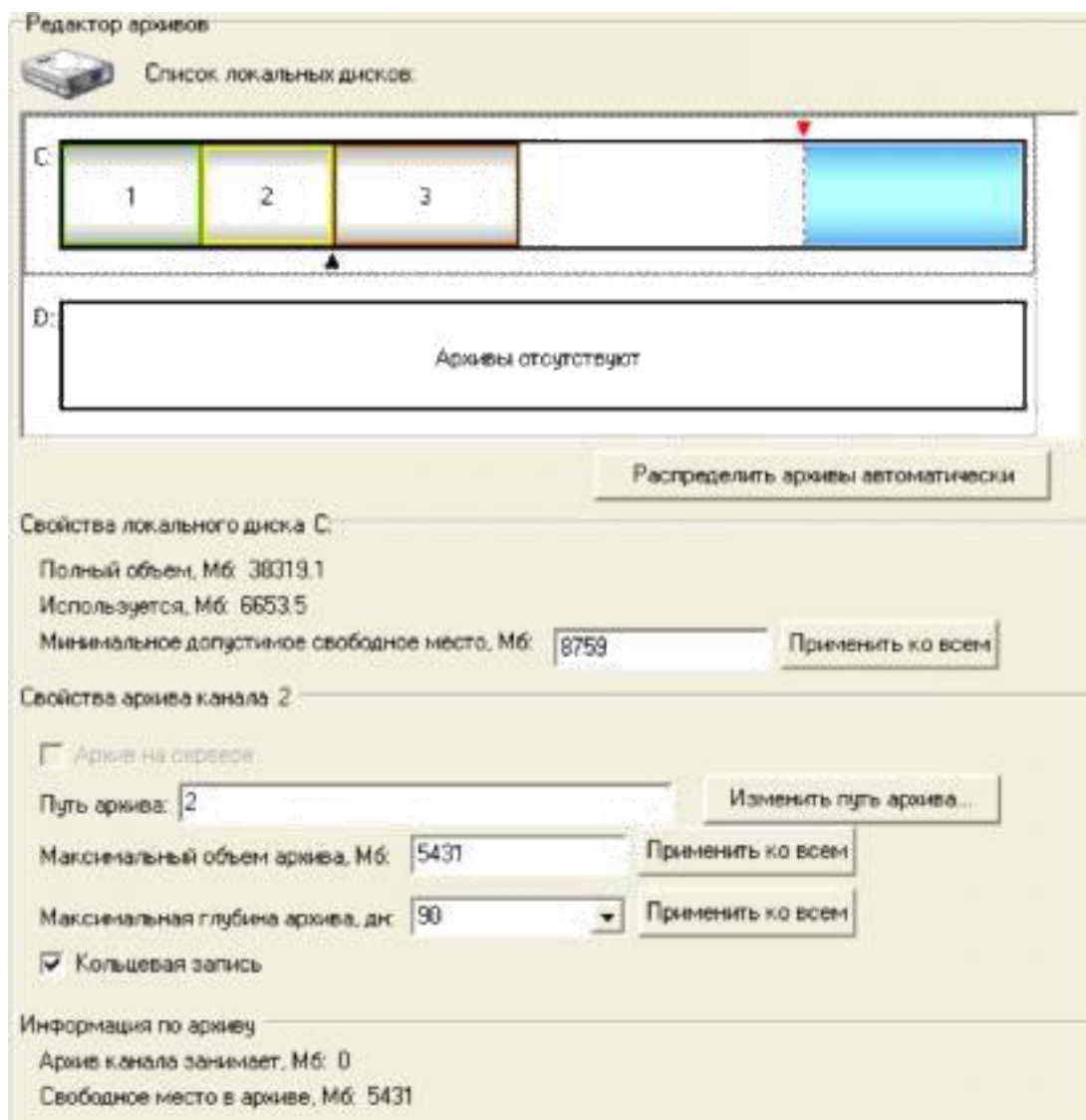
«**... при срабатывании детектоа движения на камерах**» - установить флажки у тех камер, при срабатывании детектора движения которых будет активирован вывод.

«**... при срабатывании датчика ввода**» - установить флажки у тех датчиков ввода, при срабатывании которых будет активирован вывод.

Для принятия изменений нажать «ОК».



Правое поле изменится



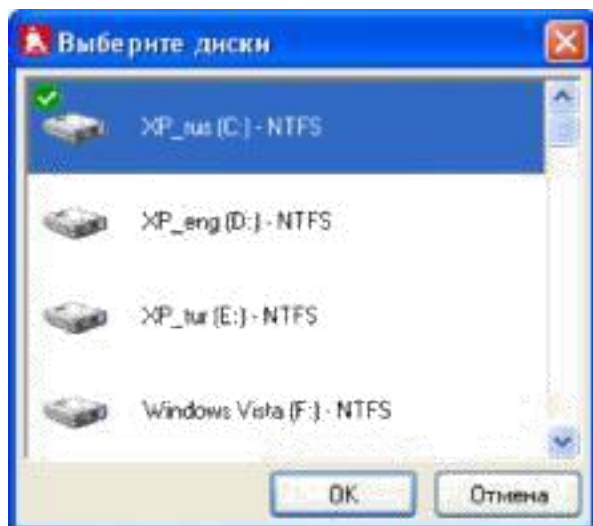
Архивы отображаются в виде прямоугольников. Слева указаны имена дисков, где хранятся архивы – диск «C:», диск «D:» и т.д.

Белый цвет архива обозначает свободное место на диске.

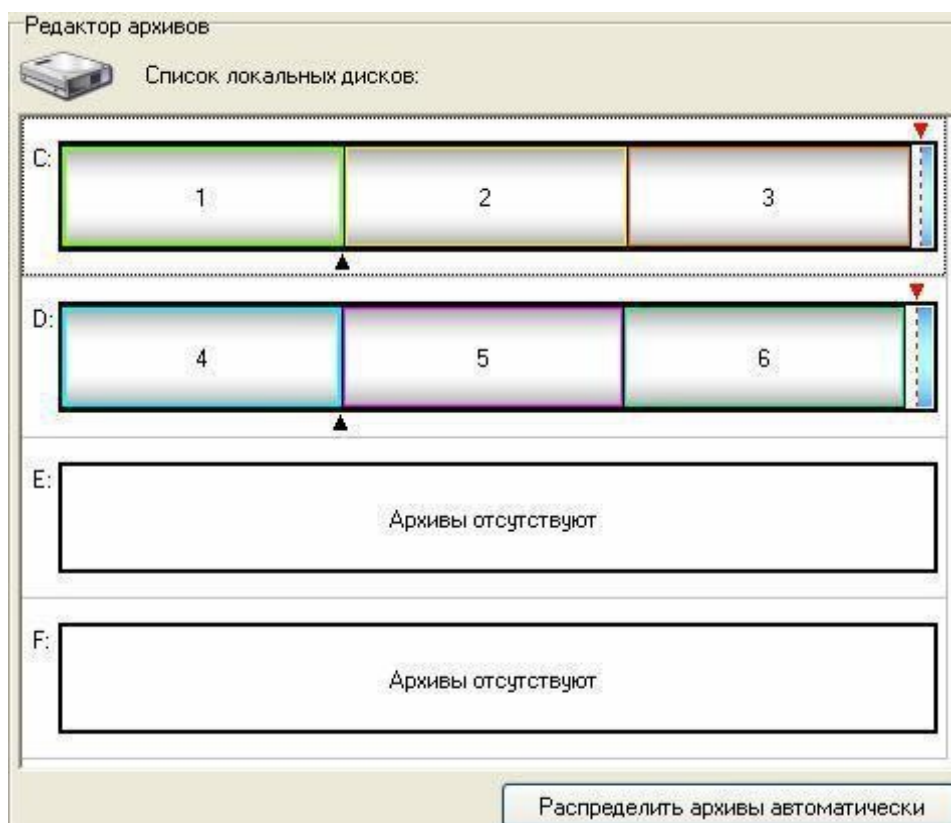
Голубой цвет обозначает зарезервированное место на диске, запись туда производиться не будет. Изменение размеров зарезервированного места производится перемещением красного бегунка над архивом.

Архивы выделены цветными рамками и пронумерованы. Изменить размер архива можно перемещением черного бегунка снизу архива.

«Распределить архивы автоматически» - автоматическое распределение архивов по выделенным дискам



Архивы будут распределены автоматически, равномерно, с учетом всех жестких дисков. Зарезервированное место будет оставлено на каждом диске (по умолчанию **1000 Мб**). Если диск системный и меньше **20 Гб**, то архивы на него распределены не будут.



ВНИМАНИЕ! При распределении архивов на системном диске выставить зарезервированное место размером 4 Гб. Это необходимо для правильной работы ОС.

Свойства локального диска C:



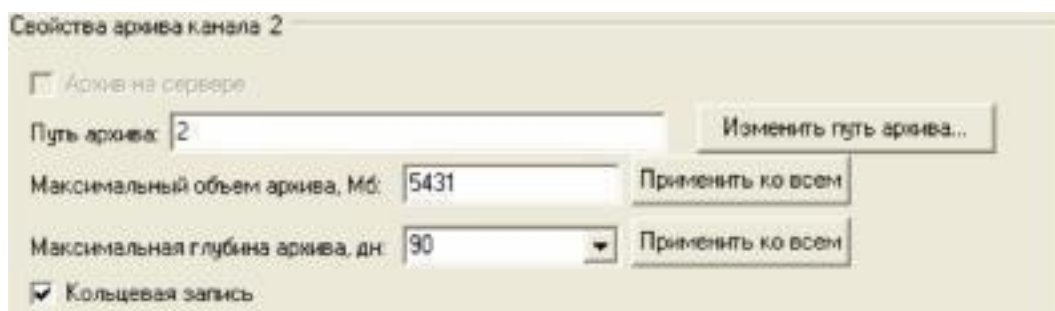
Свойства выделенного локального диска отображаются в строках: **«Полный объем»** - показывает полный объем диска.

«Используется» - показывает используемый объем для записи архива.

«Минимальное допустимое свободное место» - задается значение зарезервированного места на локальном диске.

«Применить ко всем» - применяет выставленные параметры локального диска для всех имеющихся дисков.

Свойства архива канала.



Свойства выделенного архива настраиваются в следующих параметрах: **«Архив на сервере»** - поле доступно, если есть возможность сохранить архив на сервере или на клиенте.

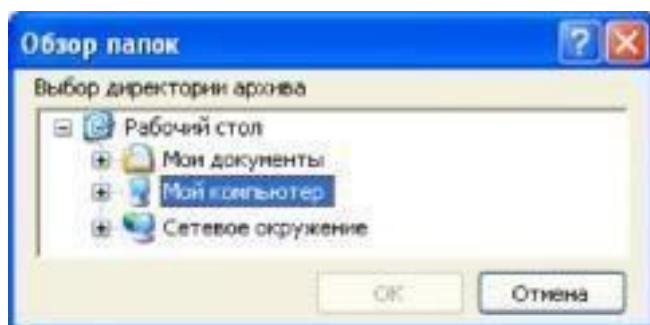
«Путь архива» - указывается место, куда сохраняется изображение. При необходимости задать другой путь – нажать **«Изменить путь архива»** и в появившемся окне указать новый путь.

«Максимальный объем архива» - задается максимальный объем архива.

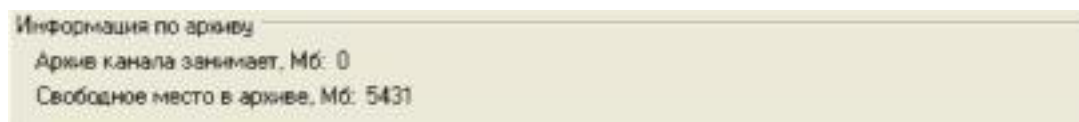
«Максимальная глубина архива» - задается максимальное количество дней, на которые может быть записан архив.

«Применить ко всем» - применяет выставленные параметры архива для всех имеющихся архивов.

«Кольцевая запись» - установленный флажок позволяет при заполнении архива производить постоянную, кольцевую запись архива. При снятом флажке при заполнении архива запись останавливается.



Информация по архиву.



Здесь выводится информация о выбранном архиве – сколько места занимает архив, сколько места осталось.

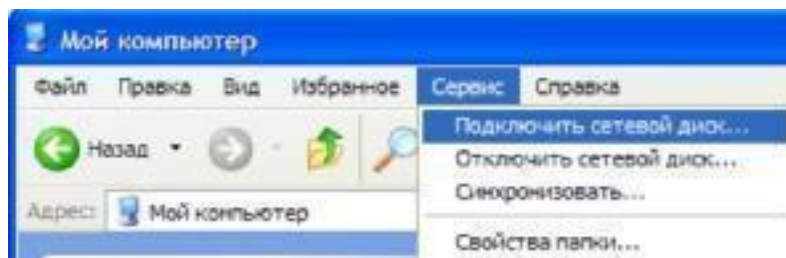
По окончании настройки архивов нажать «**ОК**».

Запись на сетевые диски.

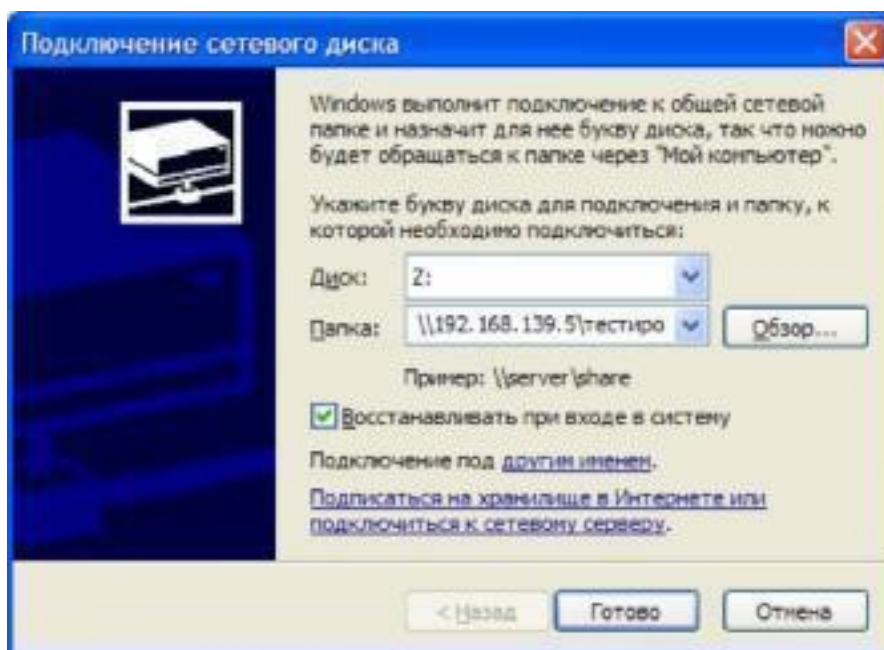
В **GLOBOSS** есть возможность записывать архив видео на сетевые диски.

Для настройки записи на сетевые диски нужно первоначально подключиться к сетевому диску.

Подключение сетевого диска



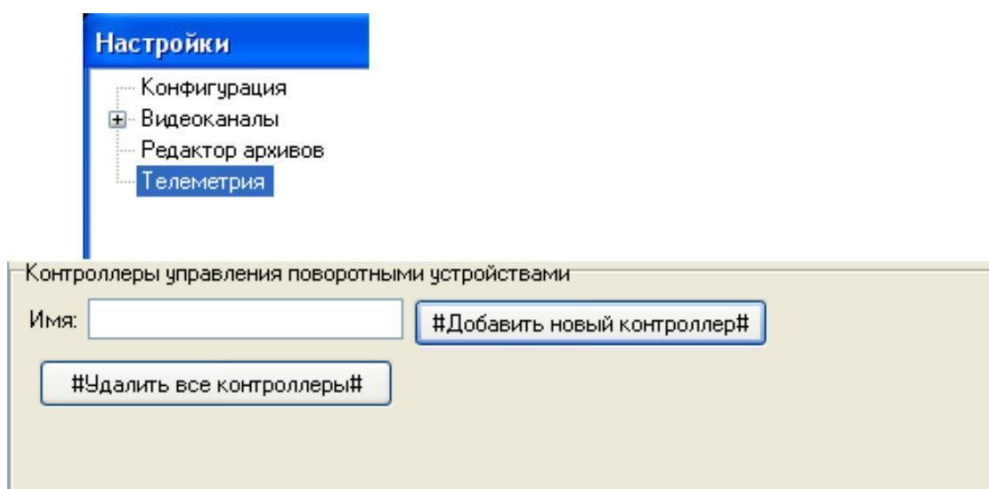
В параметре «Папка» нужно указать сетевой адрес и имя общей сетевой папки (у папки должно быть разрешение на изменение по сети)



Далее настройка записи на этот диск аналогична описанной выше.

При пропадании или отключении сетевого диска запись архивов продолжается в папку, где располагается **GLOBOSS**.

ВНИМАНИЕ! Если сетевой диск будет не доступен, то запись осуществляться не будет.



Телеметрия подразумевает управление поворотными устройствами и камерами с помощью джойстиков. Также есть возможность настроить переход на след камеру и включение/выключение патруля - это выполняется через файл `telemetry.ini`, который находится в папке, куда была установлена

программа. Содержимое файла создается автоматически, при настройке необходимо указать номер кнопки на джойстике.

Пример заполнения файла telemetry.ini: /> TO_LEFT_CHANNEL=6

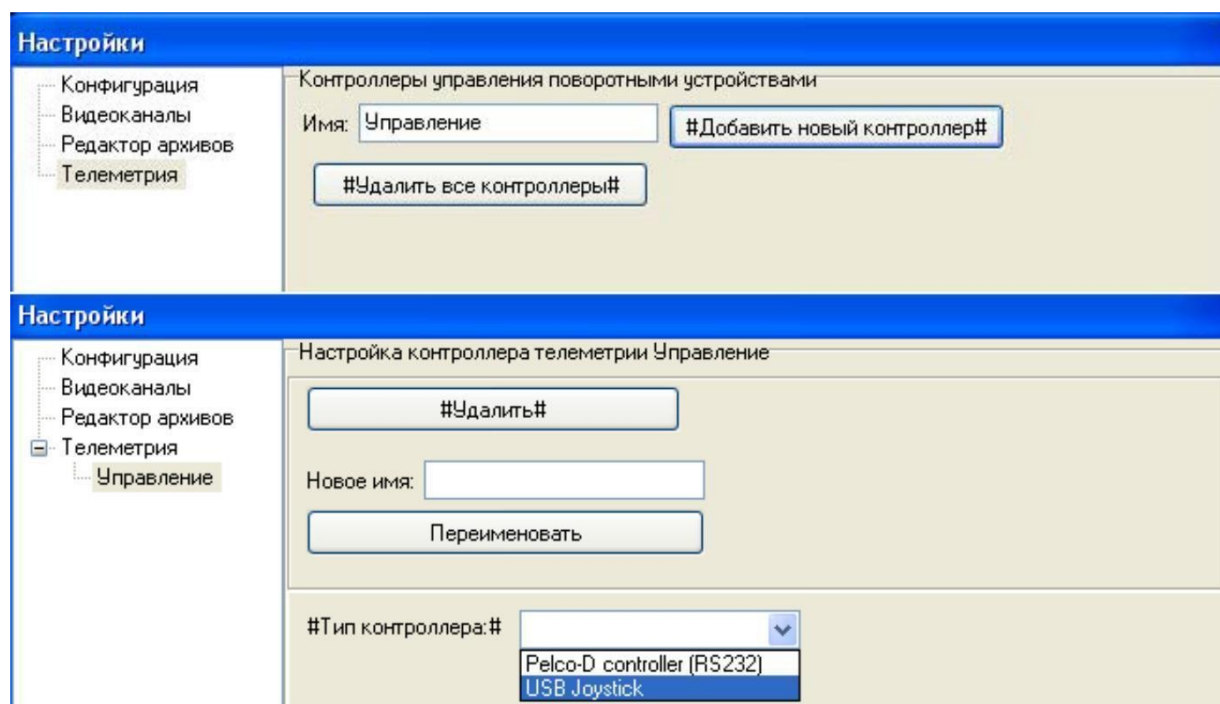
TO_RIGHT_CHANNEL=7 TLM_CMD_START_PATROL=8

TLM_CMD_STOP_PATROL=9

/> TLM_PATROL_TIME=1B Globoss управление может осуществляться при помощи двух интерфейсов: USB и Pelco.

1. USB.

В разделе «Телеметрия» добавить новый контроллер



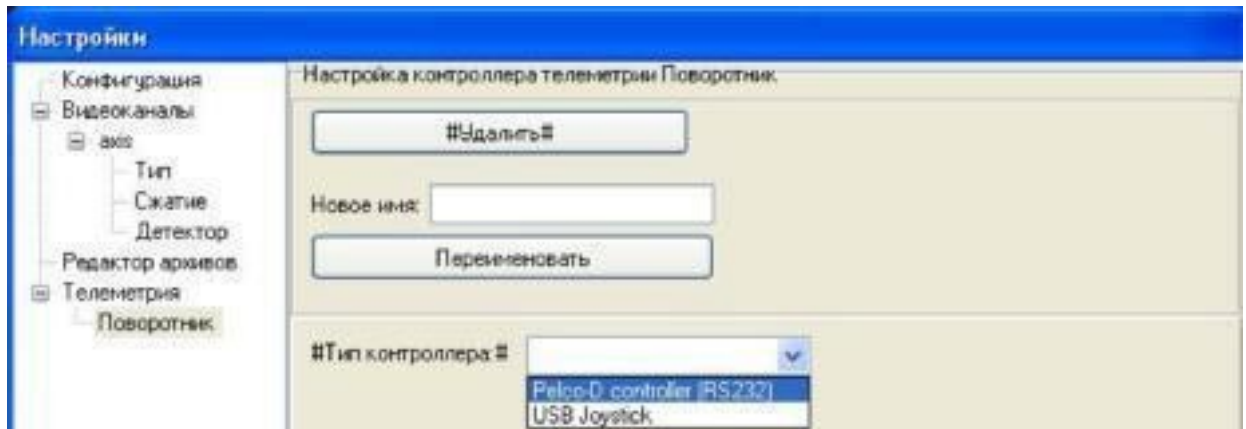
После этого выбрать модель джойстика из списка «Device model»



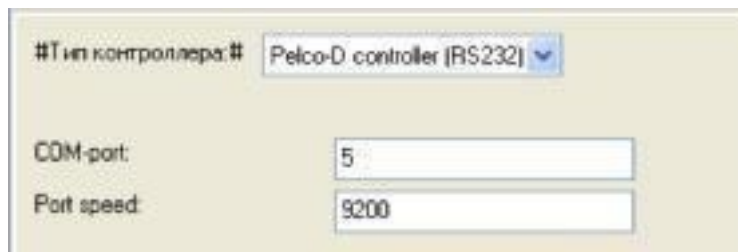
Если необходимо настроить переход на следующую камеру или включение/выключение патруля – внести соответствующую нумерацию кнопок в конфигурационный файл telemetry.ini.

2. Pelco. В разделе «Телеметрия» добавить новый контроллер

Далее в типе контроллера выбрать «Pelco – D controller»



После этого необходимо указать номер и скорость COM порта, по которому будет происходить подключение



Мультиплексор – это плата видеозахвата, где каждый чип обрабатывает несколько видеопотоков.

Функция мультиплексирования - автоматическое создание нескольких каналов, распределённых по входам мультиплексирующего устройства.

Применение мультиплексоров позволяет увеличить количество контролируемых видеоканалов за счет снижения количества отображаемых кадров в секунду по каждому видеоканалу.

Обычно параметры этих каналов практически идентичны, что позволяет осуществлять их групповую настройку. С этой целью используется

«Автоматическое создание мультиплексора»: «Операции»
«Настройки...» «Видеоканалы»

Автоматическое создание мультиплексора

Тип мультиплексора: CvCap1x4

Количество видеоканалов: 4

Номер платы видеоввода: 0

Префикс: Мультиплексор

COM-порт (для EC802): COM1

Номер EC802: 3

Создать

«**Тип мультиплексора**» следует выбрать из раскрывающегося списка.

При использовании в качестве мультиплексора платы видеоввода «**КОДОС V16**» – выбрать «**CvCap1x4**».

Поля «**Номер EC802**» и «**COM-порт (для EC802)**» относятся только к мультиплексору **EC802**.

В поле «**Префикс:** » указывают имя, которое будет в названии видеоканалов перед их порядковыми номерами, начиная с нулевого,

например: «**Мультипл_0÷ Мультипл_3**».

Специфика настройки платы видеоввода «**КОДОС V16**» обусловлена особенностями формирования каналов ввода информации.

После установки драйверов платы видеоввода «**КОДОС V16**» в свойствах компьютера, будут отображаться четыре устройства видеоввода и четыре устройства аудиоввода. Устройства видеоввода в списке пронумерованы от «**0.FV-KODOS**» до «**3.FV-KODOS**». Каждое из устройств поддерживает обработку сигналов по четырем каналам.

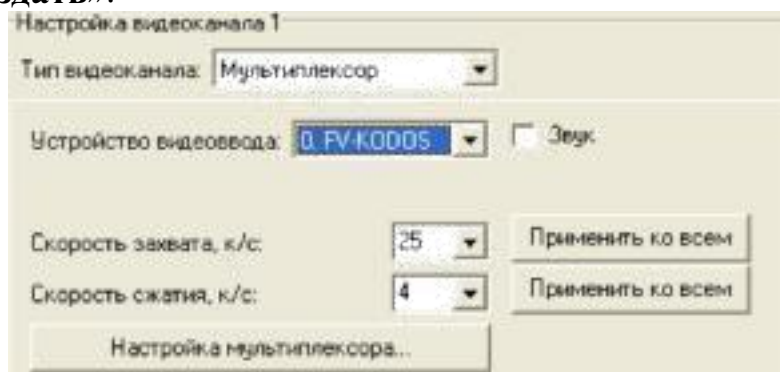
Применение функции «**Автоматическое создание мультиплексора**»

при использовании платы видеоввода «**КОДОС V16**» позволяет сократить количество манипуляций при настройке.

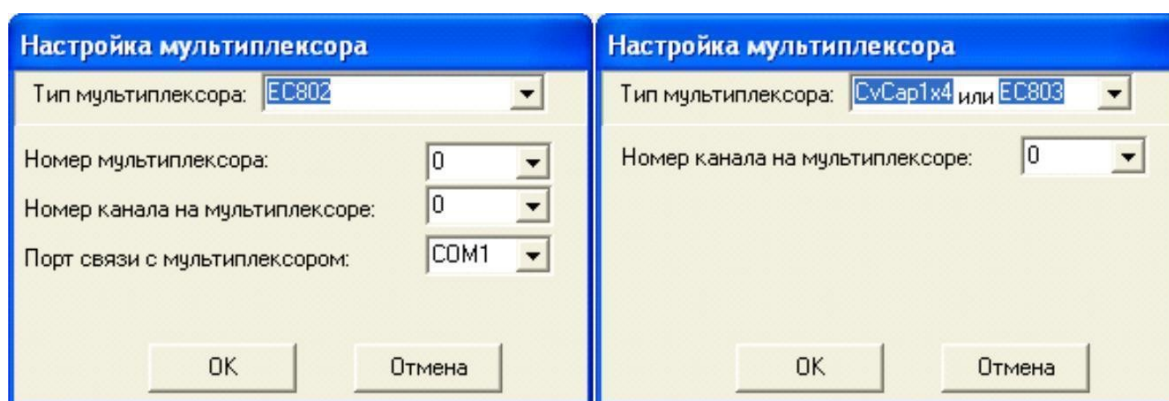
Изменяя последовательно значения «**Номер платы видеоввода:**» (**0 – 3**)

и «**Префикс**», можно получить **16** видеоканалов, сгруппированных по именам, лишь за четыре цикла операций, завершающихся нажатием кнопки

«Создать».



Для каждого мультиплексора свой набор настраиваемых параметров.



Автоматическое создание приёмников позволяет настраивать несколько видеоканалов одновременно.

Открыть: «Операции» «Настройки...» «Видеоканалы».

В поле «Сервер:» ввести с клавиатуры сетевое имя удаленного компьютера (на котором настроены видеоканалы-источники) или его IP-

адрес. Нажать кнопку «Создать» для создания дерева видеоканалов-приемников.

ВНИМАНИЕ! Для видеоканалов на сервере, изображение с которых предполагается передавать по сети, должны быть установлены флажки

«Создавать передатчик». Флажок «Архив на сервере» означает, что для всех автоматически создаваемых на клиентском компьютере видеоканалов-

приемников программа «GLOBOSS» будет использовать архивы



видеоканалов-источников сервера.

При снятом флажке «**Архив на сервере**» информация будет архивироваться на клиентском компьютере: для каждого видеоканала в папке, имя которой указано в поле ввода «**Путь архива:** ».



Оборудование и материалы

1. Стенд охранно-пожарной сигнализации КОДОС
2. Стенд системы контроля и управления доступом КОДОС
3. ПК с установленным программным обеспечением: Windows XP, Firebird 2.5, драйвер аппаратного ключа защиты, Сервер ИКБ, Конфигуратор.

Указания по технике безопасности

1. Порядок подключения оборудования определяется инструкцией по эксплуатации данного оборудования.
2. Запрещается включать любое оборудование при снятом защитном кожухе.
3. Запрещается включать оборудование при наличии повреждения изоляции соединительных проводов.
4. Запрещается самостоятельная замена или попытка ремонта любых вышедших из строя компонентов системы. В случае выхода из строя компонентов системы необходимо сообщить об этом преподавателю.

Задания

1. Ознакомиться с теоретическим материалом.

2. Добавление и удаление видеоканалов.
3. Настройка детекторов и датчиков.
4. Настройка архива.
5. Создание мультиплексора и приемника.

Вариант	Задание
1	1 канал/3датчик/4архив/2приемник
2	2 канала/4датчика/2архива/3приемника
3	3 канала/3датчика/2архива/1приемника
4	1 канал/3датчик/архив/1приемник
5	2 канала/3датчика/2архива/2приемника
6	3 канала/3датчика/3архива/3приемника
7	1 канал/2датчик/1архив/2приемник
8	2 канала/2датчика/2архива/1приемника
9	3 канала/2датчика/архива/приемника

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполнения индивидуального задания лабораторной работы.
5. Вывод.

Контрольные вопросы

1. Назовите порядок добавления и удаления видеоканалов
2. Назовите порядок настройки детекторов.
3. Назовите порядок настройки датчиков.

4. Назовите разницу между детектором и датчиком.
5. Назовите минимально необходимую конфигурацию для развертывание системы видеонаблюдения «GLOBOSS».

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
6 семестр					
ОПК-6 ИД-2 ОПК-6 ИД-3 ОПК-9 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3	Подготовка к лабораторной работе	Собеседование	6.00	6.00	23.00
ОПК-6 ИД-2 ОПК-6 ИД-3 ОПК-9 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3	Подготовка к лекции	Конспект	6.00	6.00	22.00
Итого за семестр			12.00	12.00	44.00
7 семестр					
ОПК-6 ИД-2 ОПК-6 ИД-3 ОПК-9 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3	Самостоятельное изучение литературы	Конспект	6.00	2.00	18.00
ОПК-6 ИД-2 ОПК-6 ИД-3 ОПК-9 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3	Подготовка к практическому занятию	Письменный отчет	6.00	2.00	18.00
Итого за семестр			18.00	6.00	36.00
Итого			30.00	18.00	80.00

Список литературы

1. Методическое пособие к базовому практическому курсу «Интегрированный Комплекс Безопасности КОДОС». – Москва, 2012.
2. Руководство по эксплуатации «Программное обеспечение «КОДОС» Программа настройки систем «КОДОС» («Конфигуратор»))»
3. Руководство по инсталляции «СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ КОНТРОЛЛЕРА «КОДОС PRO».
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб.заведений/ А.А. Стрельцов [и др.]: под ред. А.А. Стрельцова. - М.: Академия, 2008. – 256 с.
5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие.- СПб.: Питер, 2008.- 272 с.
6. Романов О.А. Организационное обеспечение информационной безопасности: Учебник для студентов высш. учеб.заведений/ О.А. Романов, С.А. Бабин, С.Г. Жданов.- М.: Академия, 2008. – 192 с.
7. Обеспечение информационной безопасности бизнеса/ Курило А.П., Андрианов В.В., Алексеев В.М. и др. – М.: БДЦ-пресс, 2005.- 512 с.
8. Семкин С.Н., Беляков Э.Н., Гребенев С.Н., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие.- М.: Гелиос АРВ, 2005.-192 с