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

Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению лабораторных работ
по дисциплине «Комплексная система защиты информации на предприятии»
для студентов направления подготовки /специальности
10.03.01 Информационная безопасность
шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Комплексная система защиты информации на предприятии» является теоретическая и практическая подготовка студентов в области проектирования, создания и эксплуатации комплексных систем защиты информации на предприятии.

Задачи освоения дисциплины: сущность и задачи комплексной системы защиты информации (КСЗИ); принципы организации и этапы разработки КСЗИ; определение и нормативное закрепление объектов и субъектов защиты;анализ и оценка угроз безопасности информации; определение компонентов КСЗИ; построение моделей КСЗИ; принципы и методы планирования функционирования КСЗИ; состав методов и моделей оценки эффективности КСЗИ

2. Наименование лабораторных работ

№ темы	Наименование тем дисциплины, их краткое содержание
1	Тема 1. Защита баз данных на примере MS ACCESS Лабораторная работа 1. Защита баз данных на примере MS ACCESS Содержание: Изучение способов защиты информации в БД на примере СУБД MS Access.
2	Тема 2. Введение в систему MathCad Лабораторная работа 2. Введение в систему MathCad Содержание: ознакомление с системой MathCad, изучение ее интерфейса и произведение требуемых расчетов, а так же изучение встроенных функций MathCad.
3	Тема 3. Датчики случайных чисел Лабораторная работа 3. Датчики случайных чисел Содержание: Изучение датчиков случайных чисел, математическая реализация простого датчика случайных чисел в MathCad.
4	Тема 4. Система шифрования Цезаря Лабораторная работа 4. Система шифрования Цезаря Содержание: изучение простейших традиционных алгоритмов криптографической защиты информации и особенностей их практической реализации.
5	Тема 5. Алгоритм шифрования XOR Лабораторная работа 5. Алгоритм шифрования XOR Содержание: изучение алгоритма шифрования XOR при использовании открытого ключа и гаммы псевдослучайных чисел.
6	Тема 6. Изучение системы охранной сигнализации на базе оборудования «Болид». Настройка тактики работы системы охранной сигнализации при помощи программы «Pprog» Лабораторная работа 6. Изучение системы охранной сигнализации на базе оборудования «Болид». Настройка тактики работы системы охранной сигнализации при помощи программы «Pprog» Содержание: настраивать параметры и тактику работы интегрированной системы «Орион» для системы охранной сигнализации.

7	Тема 7. Изучение системы Орион Про на базе оборудования «Болид». Настройка уровней доступа для охранно-пожарной системы при помощи программы «Pprog» Лабораторная работа 7. Изучение системы Орион Про на базе оборудования «Болид». Настройка уровней доступа для охранно-пожарной системы при помощи программы «Pprog» Содержание: настраивать уровни доступа интегрированной системы «Орион» для системы охранно-пожарной сигнализации
8	Тема 8. Изучение системы охранной сигнализации на базе оборудования «Стрелец». Настройка паролей для охранно-пожарной системы при помощи Пульта управления Лабораторная работа 8. Изучение системы охранной сигнализации на базе оборудования «Стрелец». Настройка паролей для охранно-пожарной системы при помощи Пульта управления Содержание: настраивать уровни доступа интегрированной системы «Стрелец» для системы охранно-пожарной сигнализации.
9	Тема 9. Изучение системы пожарной сигнализации на базе оборудования «Стрелец» Лабораторная работа 9. Изучение системы пожарной сигнализации на базе оборудования «Стрелец» Содержание: настраивать параметры и тактику работы интегрированной системы «Стрелец» для системы пожарной сигнализации.

3. СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа №1
Защита баз данных на примере MS ACCESS.

Цель работы: Изучение способов защиты информации в БД на примере СУБД MS Access.

Краткие сведения из теории.

Система безопасности БД должна обеспечивать физическую целостность БД и защиту от несанкционированного вторжения с целью чтения содержимого и изменения данных.

Защита БД производится на двух уровнях:

- на уровне пароля;

-на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Для защиты БД Access использует файл рабочих групп system.mdw (рабочая группа - это группа пользователей, которые совместно используют ресурсы сети), к которому БД на рабочих станциях подключаются по умолчанию. Файл рабочих групп содержит учётные записи пользователей и групп, а также пароли пользователей. Учётным записям могут быть предоставлены права на доступ к БД и её объектам, при этом сами разрешения на доступ хранятся в БД.

Для обеспечения защиты БД Access необходимо создать рабочую группу, используя файл - администратор рабочих групп wrkgadm.exe. При создании уникальной рабочей группы задается имя пользователя, название организации и код рабочей группы.

Файл рабочей группы MS Access содержит следующие встроенные учётные записи:

1. Admins - стандартная учётная запись пользователя. Данные записи являются одинаковыми для всех экземпляров Ms Access;

2. Admin - учётная запись группы администратора - является уникальной в каждом файле рабочей группы;

3. Users - содержит учётные записи пользователей.

Для создания файла рабочих групп необходимо выйти из Access и в папке system или system32 в каталоге windows найти файл рабочей группы и создать новую рабочую группу (может быть до 20 цифровых или буквенных обозначений).

Группа Admins может содержать произвольное число пользователей, но владелец объекта всегда один (владельцем объекта может быть учётная запись, которая создавала объект или которой были переданы права на его использование).

Так как чтение записи Admin возможно для всех рабочих групп и данные учётные записи являются одинаковыми, то пользователя ADMIN необходимо удалить из группы администраторов, для чего следует создать новую учётную запись администратора и задать пароль на его учётные записи и на учетные записи владельца.

Зашифровать и дешифровать базу данных могут только её владелец и члены группы Admins. Для шифрования Jet использует алгоритм RSA (назван по первым буквам фамилий его изобретателей: Rivest, Shamir, Adelman) с ключом на основе идентификатора рабочей группы.

У шифрования базы данных имеется два негативных побочных эффекта. Во-первых, снижается её быстродействие - по оценкам Microsoft, процентов на 10-15. Во-вторых, зашифрованную базу данных нельзя сжимать такими программами, как PKZip, LHA, Stacker и DriveSpace. Точнее, сжимать можно, только в этом нет смысла - её размер уменьшится незначительно.

Разграничение прав доступа пользователей

Разрешения к доступу называются явными, если они принадлежат или присвоены учётной записи пользователя. Разрешения будут неявными, если они присвоены учётной записи группы, при этом пользователь, включённый в группу получает все её разрешения.

ТИПЫ РАЗРЕШЕНИЙ НА ДОСТУП К БД

Разрешения	Разрешённые действия	Объекты БД
Открытие и запуск	Открытие БД, формы или отчёта	БД, формы, отчёты, макросы
Монопольный доступ	Монопольное открытие БД	БД
Чтение макета	Просмотр объектов в режиме конструктора	Таблицы, запросы, формы, отчёты, макросы и модули
Изменение макетов	Просмотр и изменение макетов, удаление	Таблицы, запросы, формы, отчёты, макросы и модули
Разрешения администратора	Установка пароля в БД, репликация БД	Предоставление прав доступа другим пользователям
Чтение данных	Просмотр данных	Таблицы и запросы
Обновление данных	Просмотр и изменение данных без удаления и вставки	Таблицы и запросы
Вставка данных	Просмотр и вставка данных без удаления и изменения	Таблицы, запросы
Удаление данных	Просмотр и удаление данных без из изменения и вставки	Таблицы, макросы

Полномочия пользователя определяются по минимальным разрешениям доступа. Изменить разрешения для пользователей могут члены группы Admins, владелец объекта и пользователь, получивший на этот объект разрешения администратора.

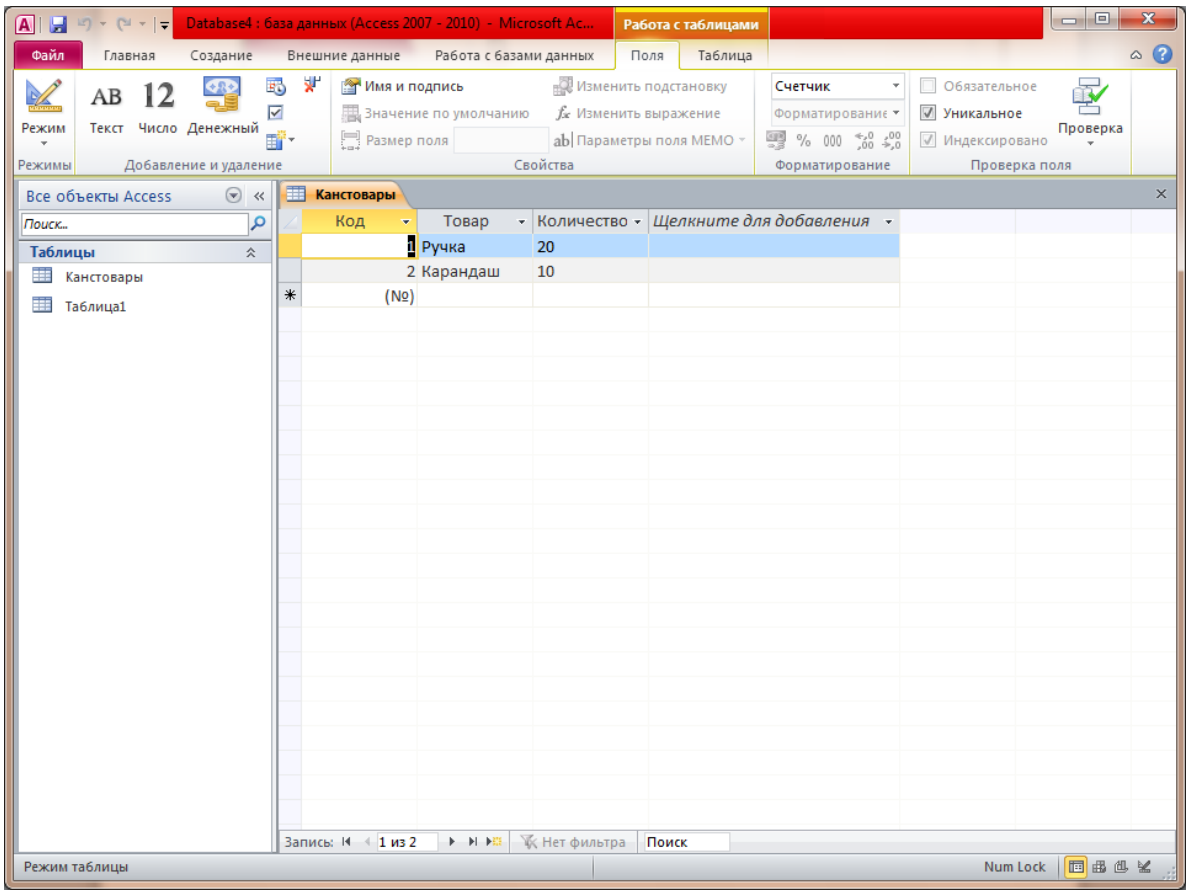
При подключении к БД пользователи получают права групп, которым они принадлежат.

Задание к работе.

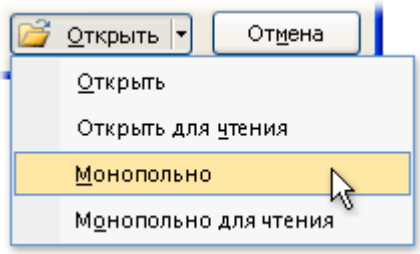
1. Создать новую базу данных MS Access
2. Зашифровать базу данных паролем
3. Расшифровать базу данных.

В Access 2010 не поддерживается защита на уровне пользователя для баз данных, созданных в новом формате (ACCDB и ACCDE-файлы). Однако при открытии базы данных из более ранней версии Access, имеющей защиту на уровне пользователя, в Access 2010 эти параметры будут продолжать действовать. Поэтому рассмотрим алгоритм защиты на уровне пароля.

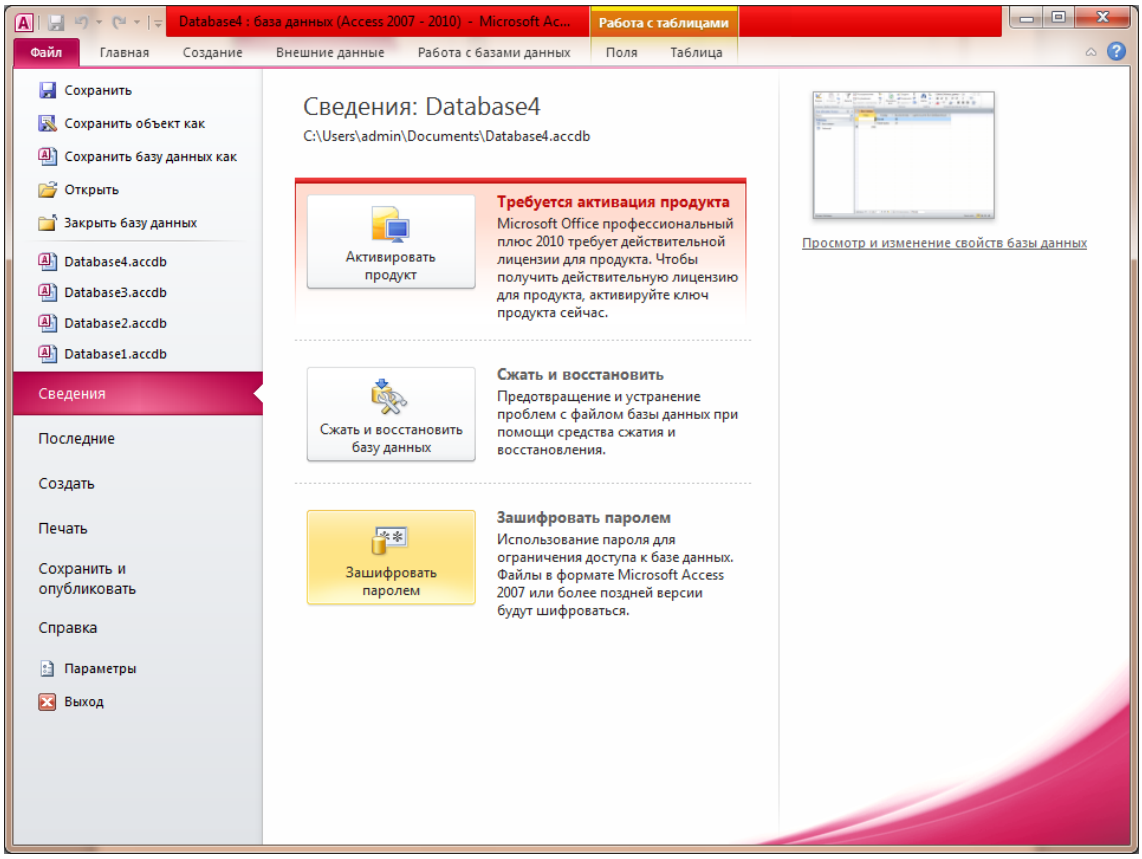
1. Открываем СУБД MS Access и создаем новую базу данных MS Access



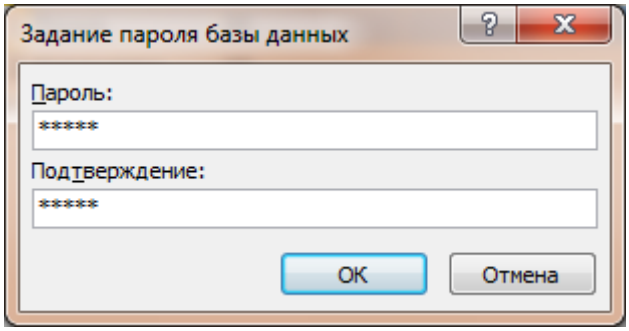
2. Сохраняем созданную БД и закрываем эту БД.
3. Вновь открываем БД но уже в монопольном режиме.
4. На вкладке Файл нажмите кнопку Открыть.
5. В диалоговом окне Открыть найдите файл, который нужно открыть, и выделите его.
6. Щелкните стрелку рядом с кнопкой Открыть и выберите команду Монопольно.



7. На вкладке Файл нажмите кнопку Сведения и выберите пункт Зашифровать паролем.

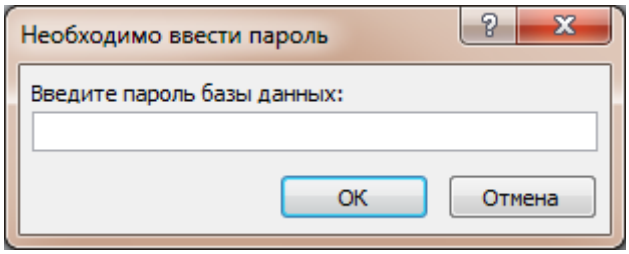


Откроется диалоговое окно Задание пароля базы данных. Введите пароль в поле Пароль, а затем повторите его в поле Проверить.

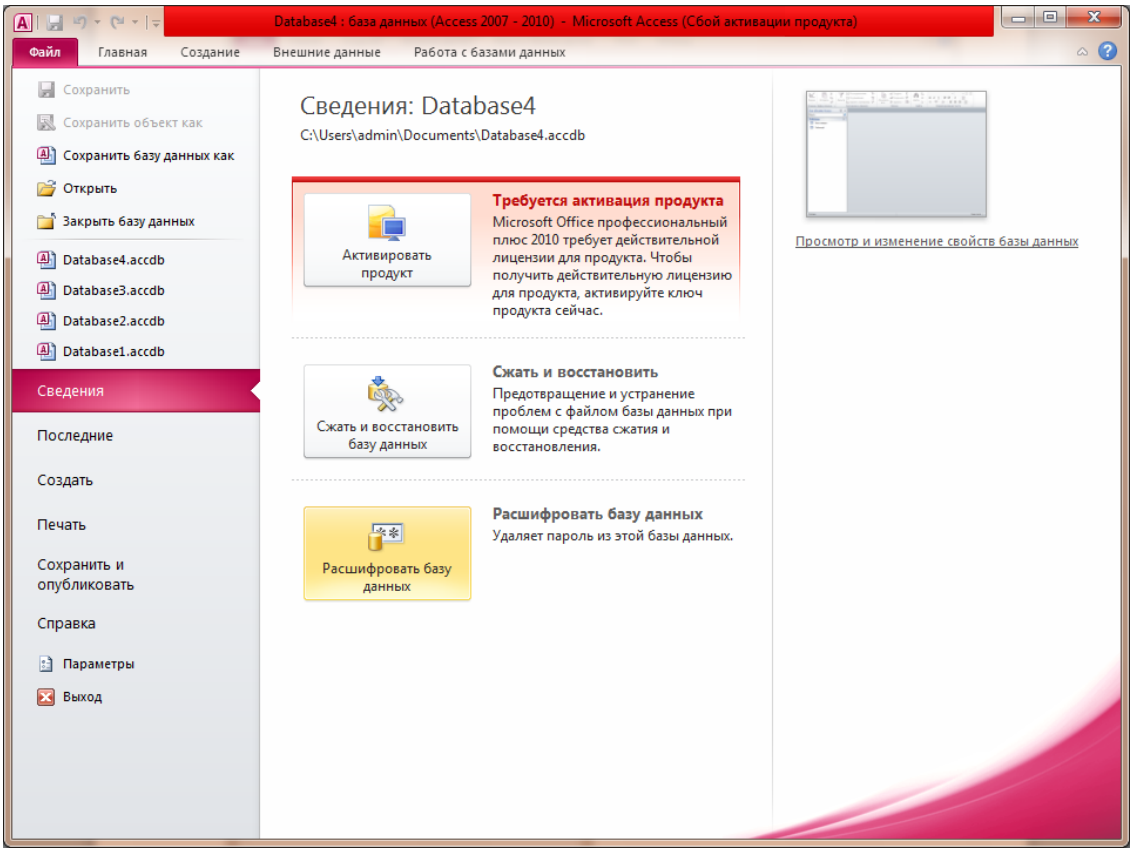


Закрыть БД.

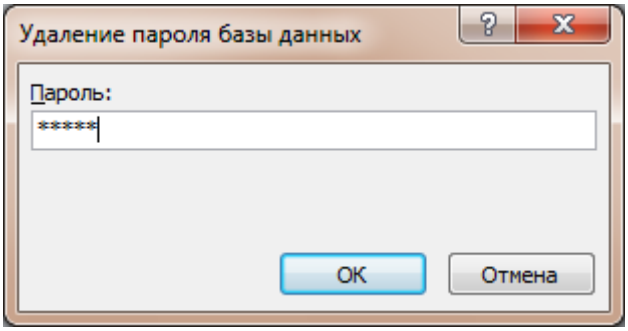
Открыть защищенную паролем БД в монопольном режиме. Появиться окно «Необходимо ввести пароль».



Для удаления созданного пароля необходимо зайти во вкладке Файл нажать кнопку Сведения и выбрать пункт Расшифровать базу данных.



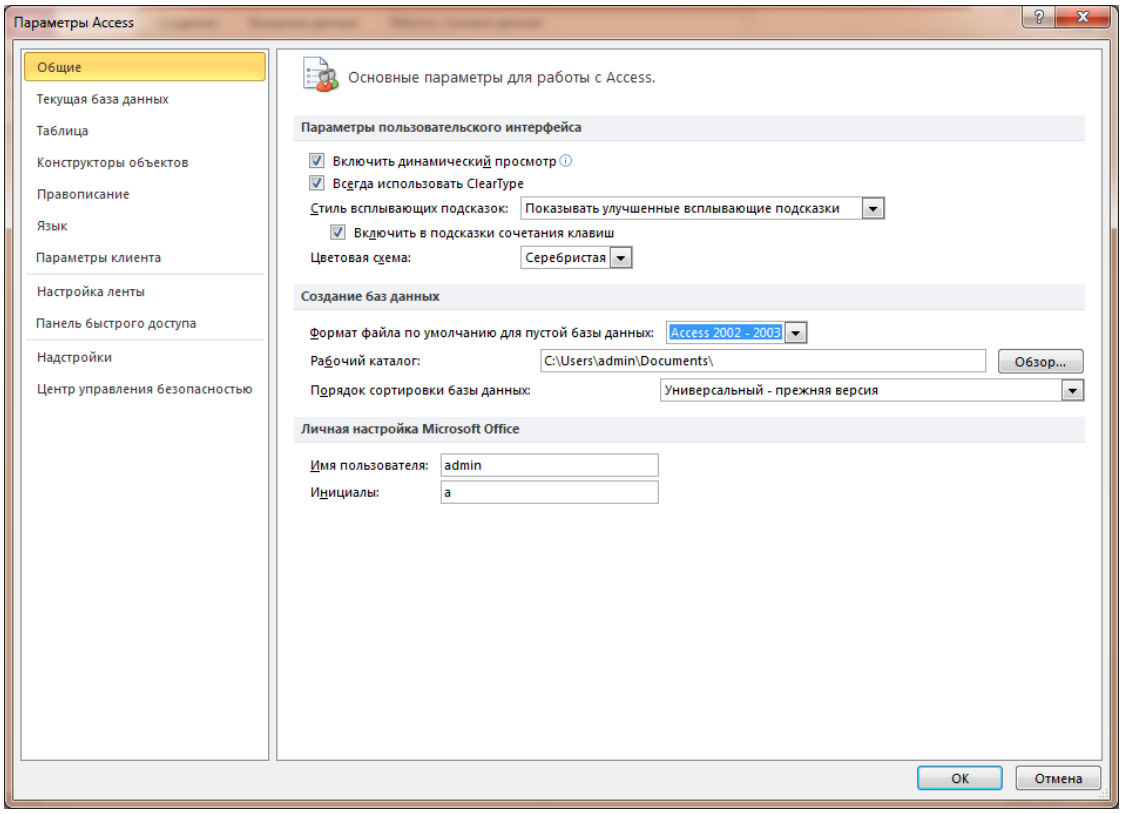
Появиться окно Удаления пароля баз данных.



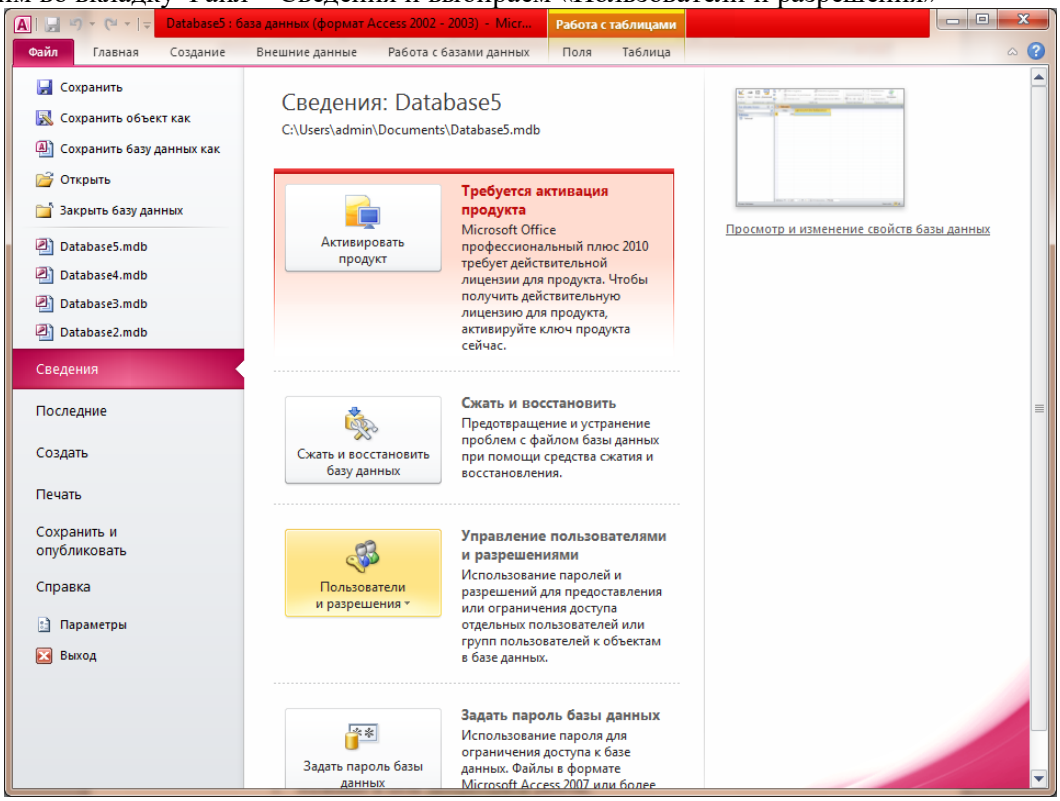
Алгоритм на уровне пользователя

Так как в Access 2007-2010 не поддерживается защита на уровне пользователя для баз данных, созданных в новом формате (ACCDB и ACCDE-файлы). Необходимо сохранить БД в Access 2003.

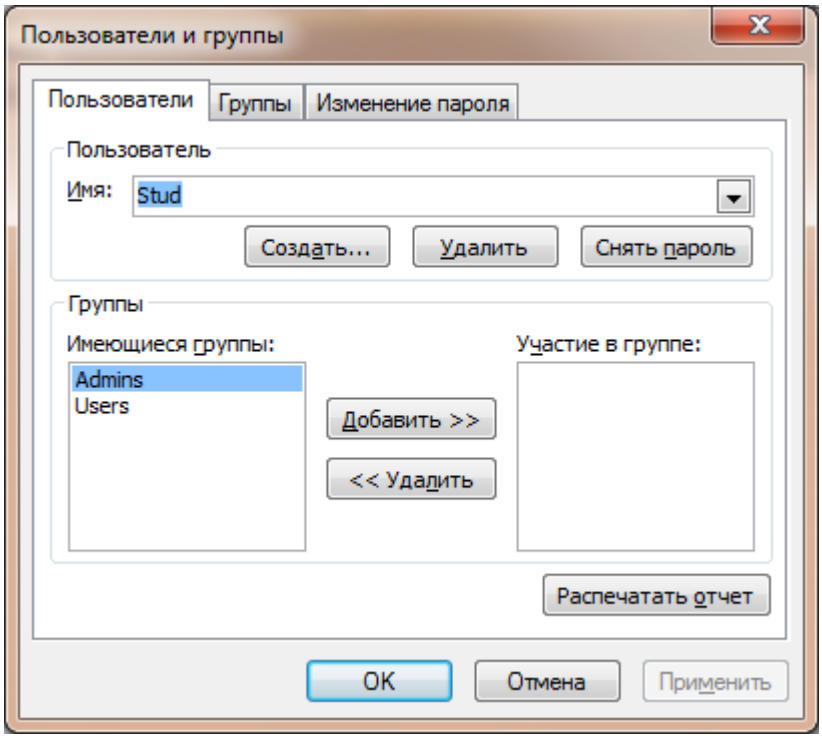
Задаем параметр для открытия пустой базы данных в формате Access 2003.



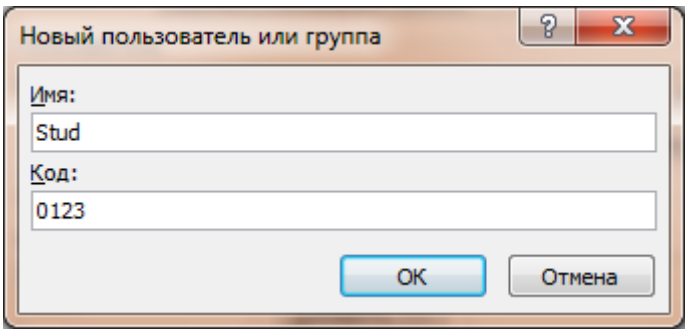
Создаем новую базу данных.
Заходим во вкладку Файл – Сведения и выбираем «Пользователи и разрешения»



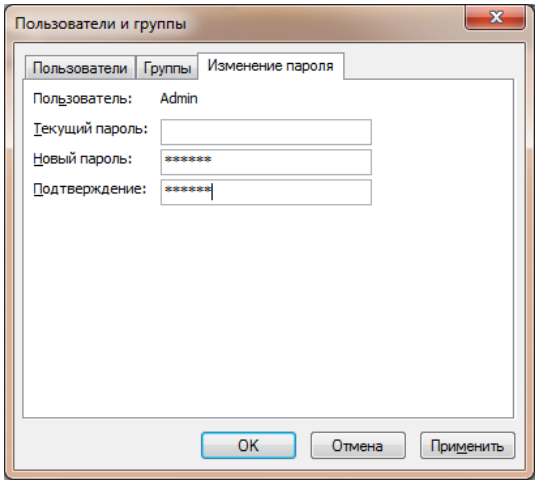
В открывшемся списке выбираем Пользователи и группы
Открывшемся окне задаем имя нового пользователя и нажимаем кнопку «Создать»



В открывшемся окне задаем код, который должен состоять не менее 4 символов и нажимаем «Ок».

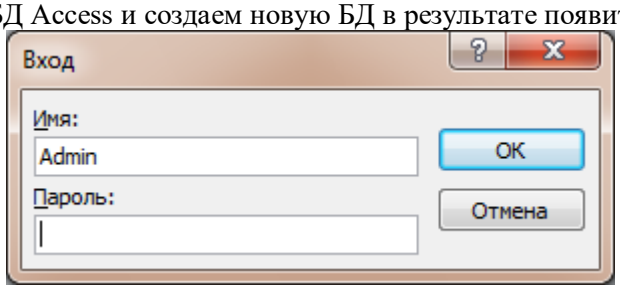


Далее заходим во вкладку «Изменение паролей» и задаем новый пароль и подтверждение пароля.

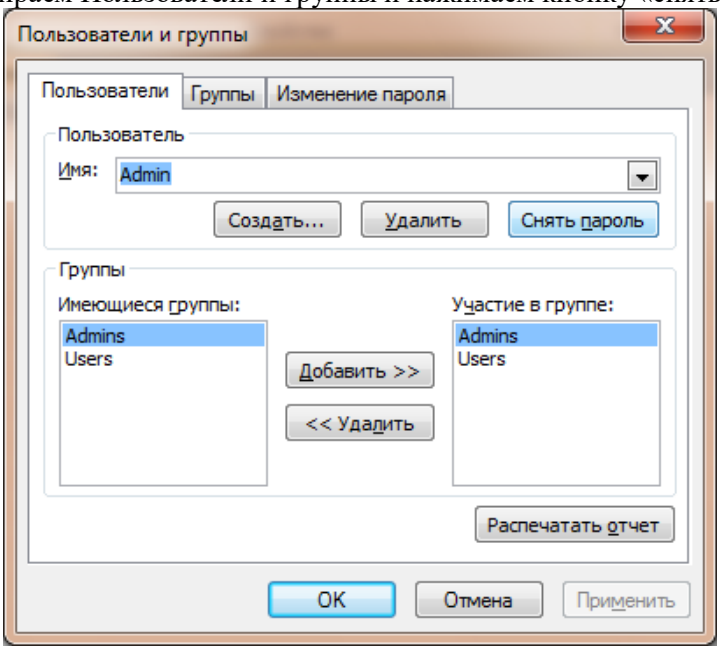


Закрываем программу БД Access

Запускаем программу БД Access и создаем новую БД в результате появиться «Вход».



Заходим во вкладку Файл – Сведения и выбираем «Пользователи и разрешения». В открывшемся списке выбираем Пользователи и группы и нажимаем кнопку «снять пароль».



Оформление отчета:

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

Отчет должен содержать:

1. Название и цель лабораторной работы;
2. Скриншоты о проделанной работе;
3. Заключения и выводы.

Вопросы для самопроверки:

1. Способы защиты информации в БД Access.
2. Группы и пользователи БД Access . Файл рабочей группы.
3. Объекты БД Access и права доступа к объектам. Понятие владельца объекта.
4. Алгоритм защиты БД Access.

Лабораторная работа №2
Введение в систему MathCad.

Цель работы: является ознакомление с системой MathCad, изучение ее интерфейса и произведение требуемых расчетов, а так же изучение встроенных функций MathCad.

Краткая теория.

Система MathCad является мощным средством для решения практических расчетных задач, обладающая удобным пользовательским интерфейсом удобным для работы.

MathCad являются математически ориентированными универсальными системами. Помимо собственно вычислений они позволяют с блеском решать оформительские задачи, которые с трудом даются популярным текстовым редакторам или электронным таблицам. Так, они позволяют готовить статьи, книги, диссертации, научные отчеты, дипломные и курсовые проекты не только с качественными текстами, но и с доступным набором самых сложных математических формул и изысканным графическим представлением результатов.

Начиная с версии Mathcad 3.0 для Windows, в Mathcad были реализованы возможности символьной (аналитической) математики. Для этого в систему было включено ядро символьной математики от одной из лучших систем компьютерной алгебры Maple V. Это превратило системы Mathcad в подлинно универсальные математические системы для всех. К важным средствам новых версий Mathcad относятся настройка под любой мало-мальски известный тип печатающих устройств, богатый набор шрифтов, возможность использования всех инструментов Windows, прекрасная графика и современный многооконный интерфейс. В новейшую версию Mathcad 2000 Professional включены эффективные средства оформления документов в цвете, возможность создания анимационных (движущихся) графиков и звукового сопровождения. Тут же текстовый, формульный и графический редакторы, объединенные с мощным вычислительным потенциалом. Предусмотрена и возможность объединения с другими математическими и графическими системами для решения особо сложных задач. Отсюда и название таких систем — интегрированные системы.

Интерфейс системы MatCad.

Интерфейс системы MatCad представляет собой типовое окно Windows и имеет стандартные строки:

Строка Меню – строка с пунктами меню, открывающая доступ к подменю с различными командами;

Панель инструментов - панель с кнопками, обеспечивающими быстрое выполнение наиболее важных команд при работе с системой;

Панель форматирования – панель с кнопками, обеспечивающими быстрое форматирование текстовых и формульных блоков в документах;

Панель инструментов для ввода математических объектов – панель с кнопками открывающими палитры специальных математических знаков и греческих букв(если этой панели нет на основном окне, то ее можно включить, поставив галочку с строке меню ВИД подменю ПАНЕЛЬ ИНСТРУМЕНТОВ в строке МАТЕМАТИКА);

Все эти панели можно перемещать по окну, зажав панель левой кнопкой мыши саму панель и прилепить ее к любой стороне окна.

Для более наглядного представления приведен рисунок общего вида окна MathCad с пояснениями.

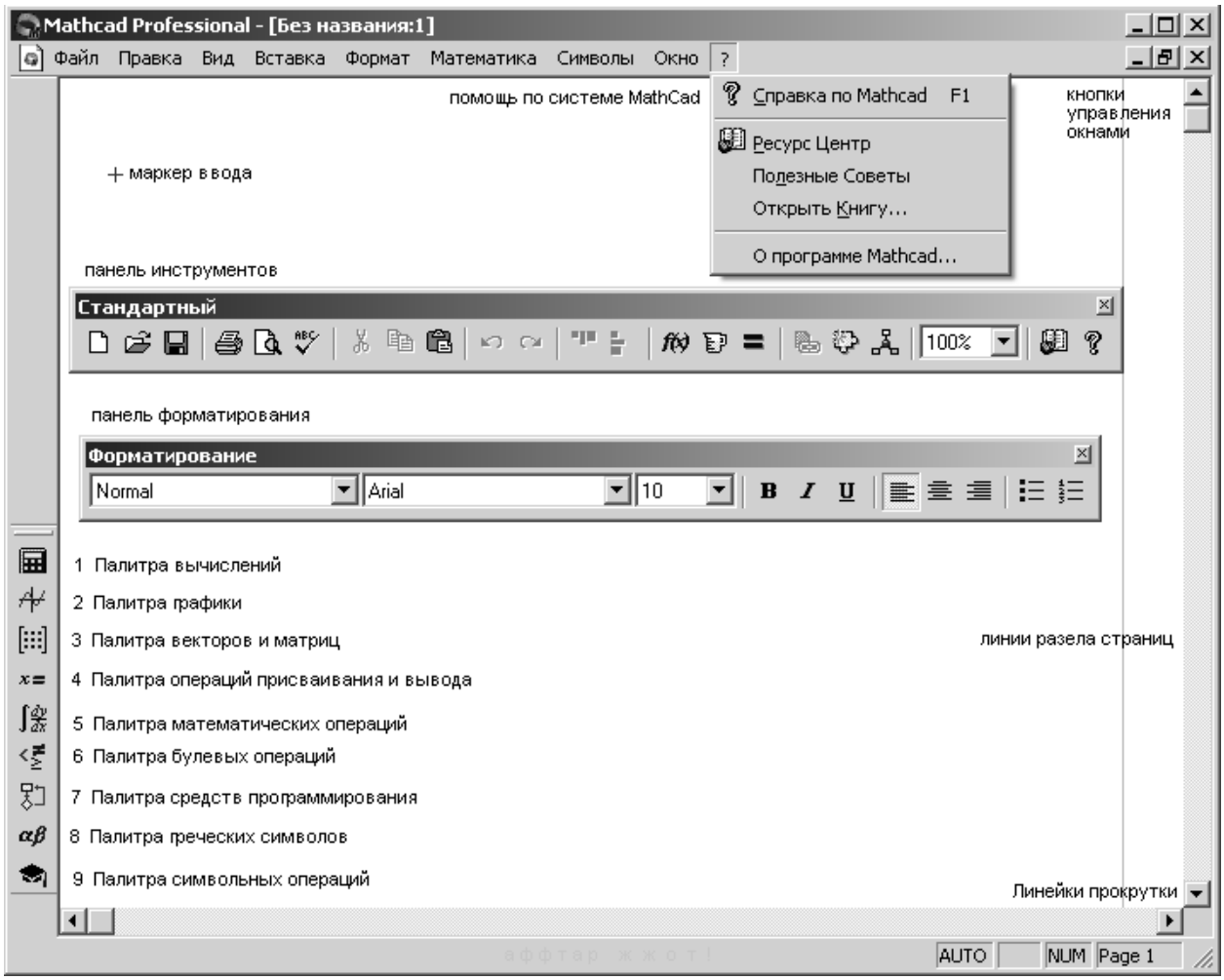


Рис.1 Основные элементы интерфейса системы MathCad.

Задание для работы.

Произвести простейшие вычисления в системе MathCad при помощи формульного редактора.

Простейшие вычисления выполняются посимвольным набором левой части вычисляемого выражения и установкой после него оператора вывода — знака = (равно). Например:

Ввод	На экране дисплея
2+3=	2+3=5

Оператор «равно» обычно используется как оператор вывода. Однако в версиях Mathcad 8 и Mathcad 2000 его можно использовать и как оператор первого присваивания.

Ввод	На экране дисплея
a=2	a := 2
b=3	b := 3
a+b=	a + b:=5

Если теперь попытаться придать переменным a и b новые значения, то ничего из этого не выйдет. Как только после имени переменной, мы попытаемся поставить знак =, появится старое значение переменной.

Ввод	На экране дисплея
a=	a = 2
_b=	b = 3

Чтобы все же присвоить переменным новые значения, придется использовать стандартный оператор присваивания : =, для которого сначала вводится символ : (двоеточие).

Ввод	На экране дисплея
a:1	a := 1
b:1	b := 1
a+b=	a + b = 2

Приведем еще несколько примеров простых вычислений. Для ввода десятичных чисел в качестве разделителя целой и дробной части используется точка, а не запятая.

Ввод	На экране дисплея
1.234*2.345=	1234 • 2.345 = 2.894
1/7=	7 = 0-143
cos(0.5)=	cos(0.5) = 0.878
e 2=	e2 = 7.389

В этих примерах можно заметить некоторые особенности работы Mathcad при выполнении простых вычислений:

•некоторые комбинированные операторы (например, : =) вводятся одним символом;

•Mathcad вставляет пробелы до и после арифметических операторов;

•оператор умножения вводится как звездочка, но представляется точкой в середине строки;

•оператор деления вводится как косая черта, но заменяется горизонтальной чертой;

•оператор возведения в степень вводится знаком ", но число в степени представляется в обычном виде (степень как верхний индекс);

•по умолчанию десятичные числа имеют представление с тремя знаками после разделительной точки;

•Mathcad понимает наиболее распространенные константы, например e — основание натурального логарифма (проверьте, что он поймет и pi или л).

Способы решения уравнений в MathCAD

Для решений уравнения с одним неизвестным вида F(x) = 0 существует специальная функция root(f(x),x), Эта функция возвращает с заданной точностью значение переменной, при котором выражение f(x) равно 0.

Для одновременного нахождения всех корней полинома используют функцию Polyroots(v), где v — вектор коэффициентов полинома, начиная со свободного члена. Нулевые коэффициенты опускать нельзя. В отличие от функции root функция Polyroots не требует начального приближения.

Функция Find (Найти) работает в ключевой связке с ключевым словом Given (Дано). Конструкция Given – Find использует расчетную методику, основанную на поиске корня вблизи точки начального приближения, заданной пользователем.

Задание для лабораторной работы.

Для нечетных номеров в списке преподавателя:

произвести расчет шаблона определенного интеграла e^x при условии, что x изменяется от 0 до 1; найти решение уравнения (2*x1+6*x2-3=10) при помощи функций Given и Find.

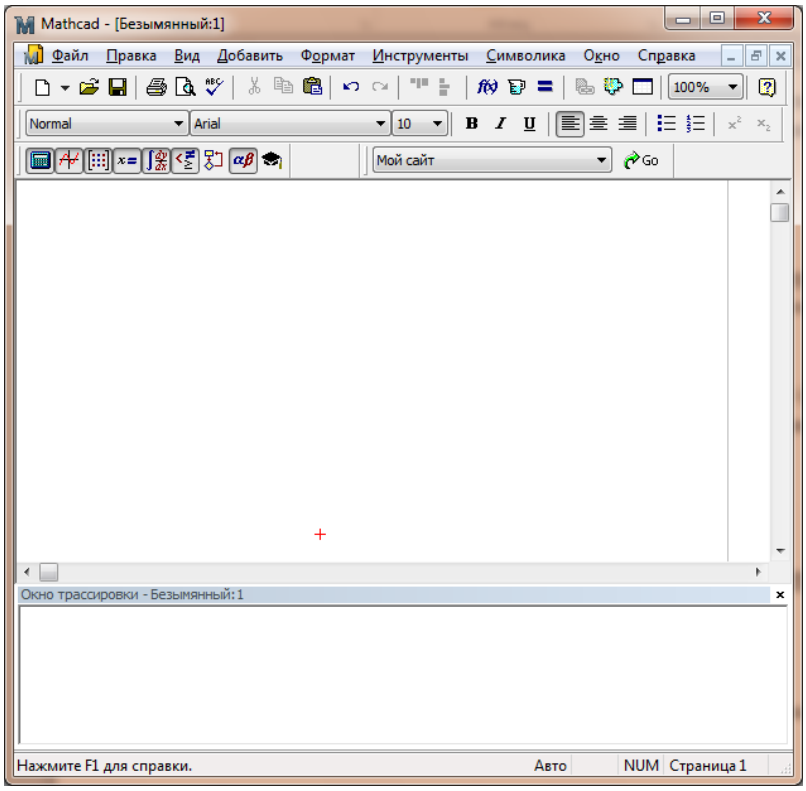
Для четных номеров в списке преподавателя:

произвести символьное вычисление шаблона производной функции ((ln(x)+5*x)/(x^2)) ; произвести расчет корней полинома(3*x^3+2*X^2+6=0) при помощи функции polyroot.

Для открытия меню функций MathCad необходимо нажать на кнопку  или ввести название функции вручную.

Порядок выполнения работы:

Запускаем программу Matcad.



Для выполнения задания на лабораторную работу необходимо на вкладке Вид – Панель инструментов выбрать панели Калькулятор, Исчисление, Вычисление, Логический.

Для второй части лабораторной работы нечетных номеров необходимо воспользоваться функцией Given и Find для этого необходимо задать значение x.

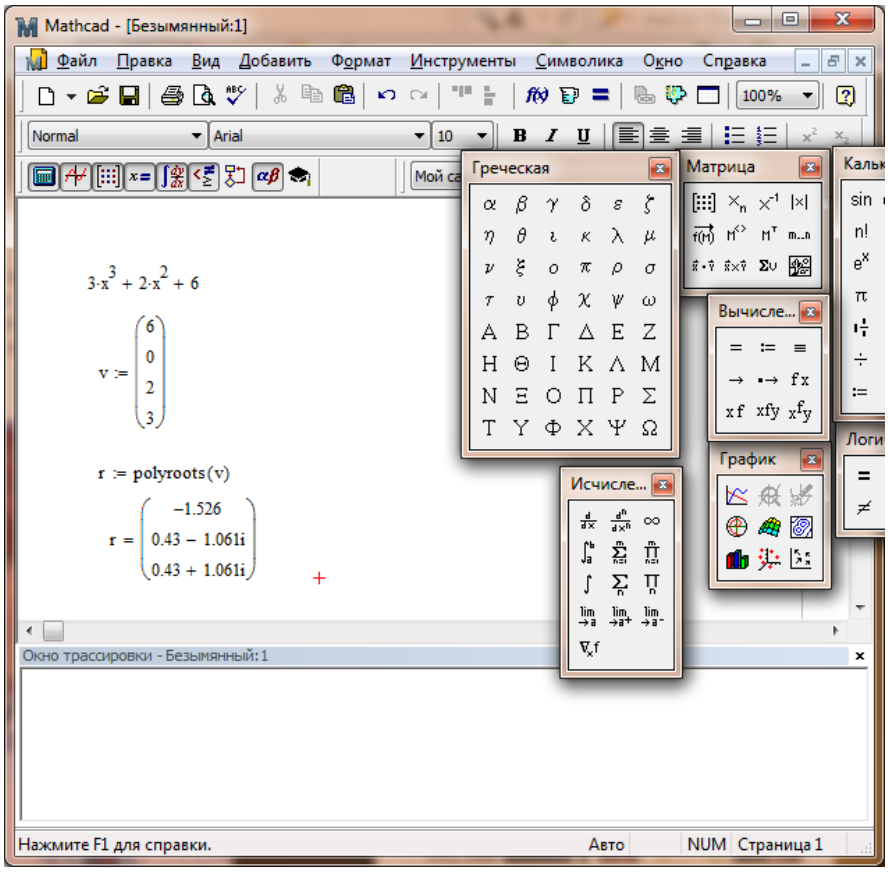
$$x_1 := 85 \quad x_2 := 50$$

Given

$$2 \cdot x_1 + 6 \cdot x_2 - 3 = 10$$

$$\text{Find}(x) = \begin{pmatrix} 0 \\ 85 \\ -26.167 \end{pmatrix}$$

Для второй части лабораторной работы четных номеров необходимо воспользоваться функцией Polyroot для этого необходимо задать значение x.



Контрольные вопросы:

1. Способы решений уравнений в MathCad.
2. Стандартные шаблоны для математического анализа MathCad.
3. Способ получение ответа в виде числа с плавающей запятой, с требуемой точностью.
4. Интерфейс системы MatCad представляет собой.

Содержание отчета.

1. Отчет должен быть выполнен на бумаге формата А4.
2. Отчет должен содержать краткую теорию по теме работы.
3. Отчет должен содержать текст программ MathCad с комментариями.
4. Отчет должен содержать выводы о проделанной лабораторной работе.

Лабораторная работа №3
Датчики случайных чисел.

Цель работы: Изучение датчиков случайных чисел, математическая реализация простого датчика случайных чисел в MathCad.

Краткая теория.

В ряде шифровальных алгоритмов используется бесконечная гамма случайных чисел, обладающих рядом качеств и параметров (диапазон изменений, максимальное и минимальное значение, частотность и другие).

В основе этих методов получения случайных чисел, распределенных по любым законам, так же лежит использование генератора случайных чисел в интервале 0…1. Наибольшее распространение получили следующие методы генерирования:

квадратов;

произведений;

мультипликативный конгруэнтный;

смешанный конгруэнтный.

Метод квадратов. В квадрат возведено текущее случайное число и из результатов средних разрядов выделяется следующее число.
Метод произведений. Два следующих друг за другом случайных числа умножают а из произведения

средних разрядов выделяют следующее случайное число. Мультипликативный конгруэнтный метод. В качестве текущего значения случайного числа выделяют остаток от деления произведения предыдущего случайного числа и постоянного множителя a на постоянное число m:

yi=a*yi-1*(mod m),

где a, m -постоянные числа; yi - случайное число. Смешанный конгруэнтный метод. Этот метод отличается от предыдущего прибавлением к остатку от деления постоянного числа m:

yi=a*yi-1+m*(mod m),

Перечисленные методы также обладают своими недостатками, поэтому датчики случайных чисел, реализованные на их основе проверяют. Различают три типа проверки:

на периодичность;

на случайность;

на равномерность.

Для определения длины периода генерируют случайные числа и сравнивают их с зарегистрированным числом, подсчитывая количество случайных чисел, полученных до совпадения с зарегистрированным числом.

При проверке на случайность используют совокупность тестов проверки: частот; пар; комбинаций; серий; корреляции.

В первых четырех тестах осуществляется разбиение диапазона распределения на t интервалов и выполняется подсчет количества попаданий случайных чисел в выделенные интервалы. Полученное эмпирическое распределение сравнивается с теоретическим. Для сравнения используются критерии согласия Колмогорова и c2.

Тест проверки корреляции заключается в определении коэффициента корреляции. При этом выполняются следующие действия: запускают два генератора случайных чисел на отрезке апериодичности с некоторой разницей между собой, затем подсчитывают коэффициент корреляции между собой.

При поверке на равномерность используется тест проверки частот, так как гистограмма хорошо отражает равномерность распределения.

В данной лабораторной работе необходимо ознакомиться с двумя датчиками случайных чисел, один из которых – встроенный датчик случайных чисел RND в системе MathCad, а второй датчик реализующий мультипликативный конгруэнтный датчик.

Так называемый мультипликативный конгруэнтный датчик задается двумя параметрами: модулем m и множителем k. Обычно это достаточно большие целые числа.

При заданных m, k числа z1, z2, ..., вычисляются по рекуррентной формуле:

Ai = (kAi -1) mod m, i = 1, 2,...,

zi = Ai / m,

где m - модуль, k - множитель, A0 - начальное значение, mod - операция вычисления остатка от деления kAi -1 на m.

Таким образом, A1 определяется как остаток от деления kA0 на m; A2 - как остаток от деления kA1 на m и т.д. Поскольку все числа Ai - это остатки от деления на m, то 0 J Ai < m. Разделив последнее неравенство на m, видим, что 0 J Ai / m< 1, т. е. 0 J zi <1.

Из неравенства 0 J Ai < m вытекает также, что датчик дает периодическую последовательность Ai. Действительно, число всех возможных остатков от 0 до m - 1 равно m и, рано или поздно, на каком-то шаге i обязательно появится значение Ai, уже встречавшееся ранее. С этого момента последовательность Ai “зациклится".

Длина периода T будет не больше m - 1. Например, если встретится остаток Ai= 0, то далее, согласно рекуррентной формуле , будет Ai+ 1 = 0, Ai+ 2 = 0, ... , т.е. длина периода T = 1. Ненулевых же остатков в интервале 0J Ai < m всего m - 1, и, если все они войдут в период, будет T = m - 1. Это имеет место, например, при m = 13, k = 7; в этом случае ряд Ai выглядит так:

1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, 7,... .

_____/

T = m - 1 = 12

Поскольку в качестве случайной можно использовать лишь подпоследовательность Ai внутри одного периода, то параметры датчика выбирают так, чтобы длина периода T была максимальной. С учетом ограничения TJ m - 1 модуль m берут максимально возможным. Чтобы упростить вычисление остатков по (2.5), для двоичных ЭВМ часто берут m = 2n. Рекомендуется также брать достаточно большой множитель k, причем взаимно простой с m.

В [30] можно найти подробные рекомендации по выбору параметров m, k и начального значения A0 . Заметим, однако, что в настоящее время не известны правила, которые гарантировали бы высокое качество датчика без его специального статистического тестирования.

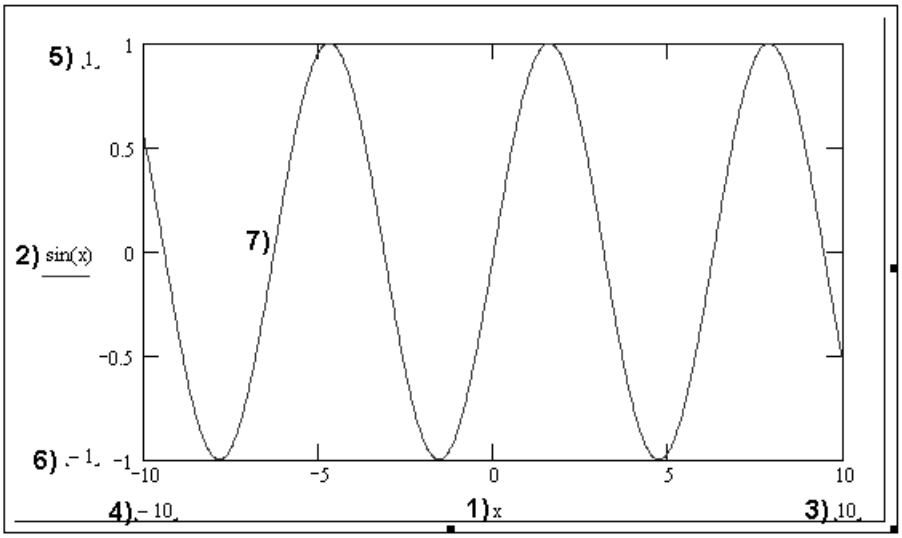
Датчик называют мультипликативно-конгруэнтным потому, что он использует две основные операции - умножение (англ. multiplication) и вычисление остатка (в теории чисел - получение конгруэнтного числа). Можно было бы поэтому перевести его название и как "множительно-остатковый датчик".

Обратим внимание также и на то, что операция вычисления остатка воплощает здесь неймановский принцип вытаскивания цифр. Это становится очевидным, если записывать числа в системе счисления с основанием m. Тогда операция X mod m означает выбор последней цифры из числа X. Для m = 2n операция X mod m означает также выделение последних n цифр из двоичной записи числа X.

Функцию выполняющую роль датчика случайных чисел в системе MathCad, является функция rnd(x), где x максимальное значение случайного числа. Для получения характеристик гаммы так же понадобятся функции: mean(x), max(x), stdev(x), var(x), min(x).

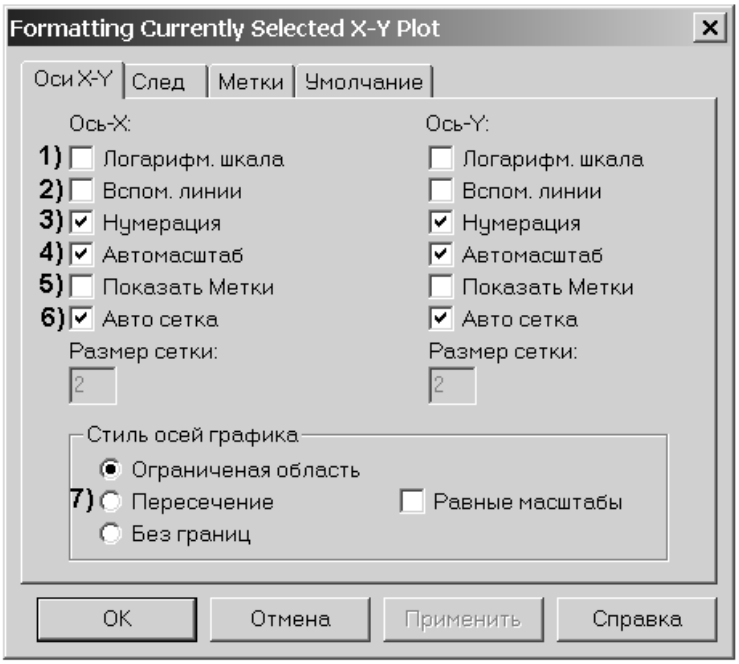
Для наглядной иллюстрации равномерности распределения, а так же гистограммы распределения необходимо применить графический аппарат MathCad.

В математической системе MathCad есть возможность построение 2х и 3х мерных графиков.



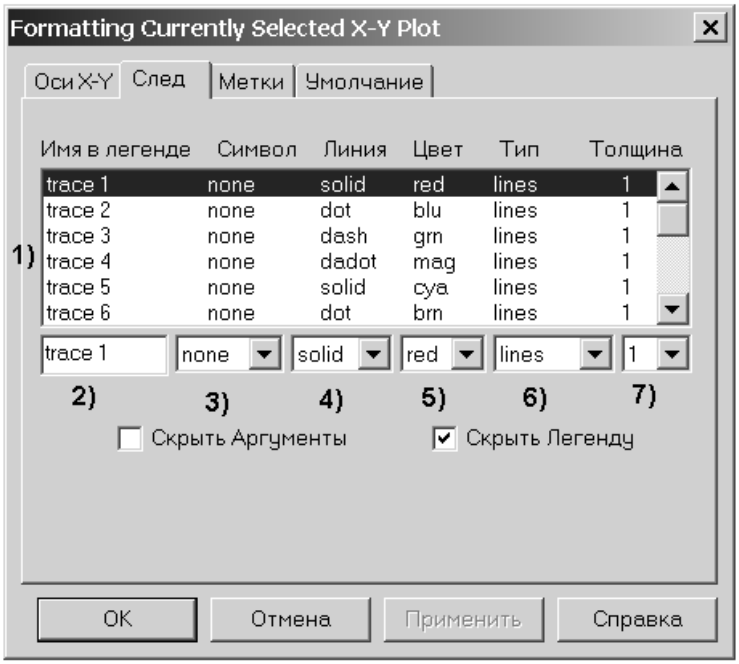
1) аргумент
2) функция
3) максимальный предел рисования графика по аргументу
4) минимальный предел рисования графика по аргументу
5) максимальный предел рисования графика по функции
6) минимальный предел рисования графика по функции
7) график функции

Рис.1 Общий вид графика функции



1) установка логарифмического счета значения по оси
2) Вспомогательные линии
3) нумерация шкал
4) автомаштаб
5) включение 2х меток по оси
6) автоматическая сетка
7) выбор типа координатной оси

Рис.2 меню форматирования графика



1) список графиков
2) выбор текущего графика для редактирования
3) символ обозначения точки расчета
4) тип линии
5) цвет линии
6) стиль рисования графика
7) толщина линии

Рис.3 меню управления графиками функций

Задание для лабораторной работы.

1)Используя датчик случайных чисел системы MathCad, получить последовательность из 1000 чисел, в диапазоне от 0 до 10, и построить гистограмму распределения случайных чисел, при помощи встроенной функции hist(int,x).

2)Реализовать мультипликативный конгруэнтный датчик, выдающий последовательность из 1000 случайных чисел, по заданному числу A, и фиксированных m=2^36, k=5^15, при условии, что случайные числа должны находится в диапазоне от 0 до 10.

Порядок выполнения работ.

1-ое задание:

1. Согласно заданию необходимо задать диапазон последовательности от 0 до 1000.
2. При помощи функции “rnd” задаем диапазон от 0 до 10.
3. Вывести последовательность из 1000 чисел.

$y_i =$

2.07
0.576
1.194
7.275
2.164
7.238
8.63
7.89
8.615
2.442
9.914
0.924
1.827
8.34
1.061
...

4. Задать диапазон от 0 до 10 и присвоить его значению int_j.
5. Присваиваем переменной (например f) функцию hist(int,x)
6. Строим гистограмму распределения случайных чисел.

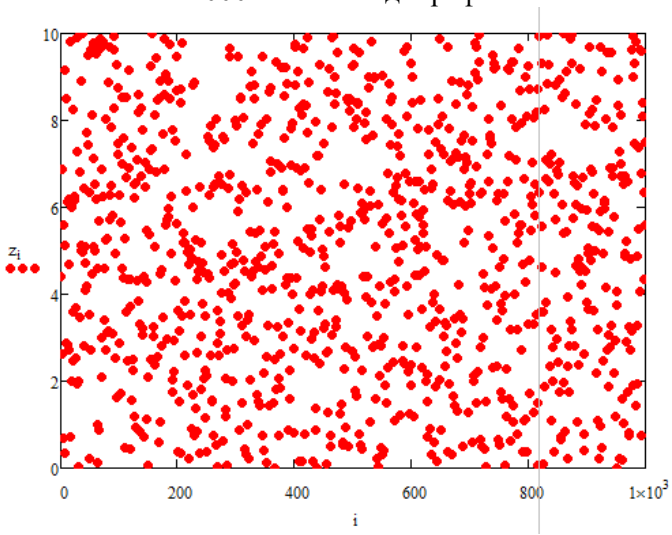
2-ое задание:

1. Задать согласно заданию на лабораторную работу модуль - m, множитель - k, начальное значение – A0 (любое число 1-20).
2. Согласно заданию необходимо задать диапазон последовательности от 1 до 1000.
3. Записать рекуррентную формулу (Ai, zi).
4. Вывести zi последовательность из 1000 чисел.

z_i =

4.409
6.881
2.633
0.697
5.598
0.336
5.136
9.166
2.886
8.513
6.115
2.83
2.713
4.697
6.195
...

5. Вывести zi последовательность из 1000 чисел в виде графика.



6. Задать диапазон от 0 до 10 и присвоить его значению int_j.
7. Присваиваем переменной (например f) функцию hist(int,x)
8. Строим гистограмму распределения случайных чисел.

Контрольные вопросы:

1. Где применяются датчики случайных чисел?
2. Четыре методы генерирования случайных чисел?
3. Построение декартова графика в системе MathCad, форматирование графика, реализация нескольких графиков функций от одного аргумента на одном графике?
4. Три типа проверки с генерированных датчиков случайных чисел?
5. Реализация мультипликативного конгруэнтного метода?

Содержание отчета.

1. Отчет должен быть выполнен на бумаге формата А4.
2. Отчет должен содержать краткую теорию по теме работы.
3. Отчет должен содержать текст программ MathCad с комментариями.
4. Отчет должен содержать выводы о проделанной лабораторной работе.

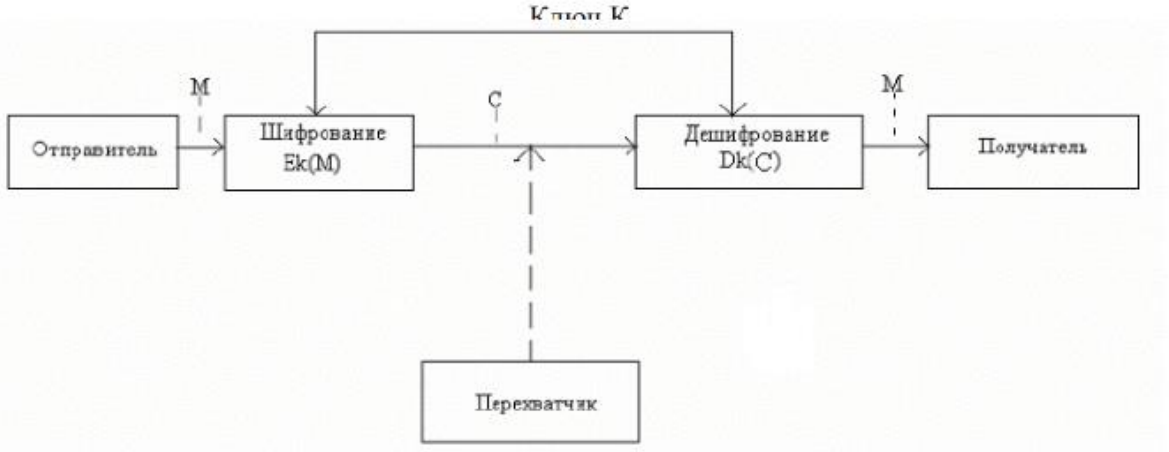
Лабораторная работа №4
Тема: Система шифрования Цезаря

Цель работы: изучение простейших традиционных алгоритмов криптографической защиты информации и особенностей их практической реализации.

Краткая теория.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблему обеспечения конфиденциальности (путем лишения противника возможности извлечь информацию из канала связи) и проблему целостности (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи).

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, изображена на следующем рисунке:



Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того, чтобы перехватчик не смог узнать содержание сообщения M, отправитель шифрует его с помощью обратимого преобразования Ek и получает шифротекст C=Ek*(M), который отправляет получателю .Законный получатель приняв

шифротекст C, расшифровывает его с помощью обратного преобразования Dk =Ek-1 (C) и получает исходное сообщение в виде открытого текста M.

Преобразование Ek называется криптоалгоритмом.

Под криптографическим ключом K понимается конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Данный ключ, либо его часть, является закрытой информацией, которая должна быть известна только законным участникам криптографического обмена. Утеря секретной части ключа ведет к раскрытию всего защищенного обмена.

Любая попытка со стороны перехватчика расшифровать шифротекст C для получения открытого текста M или зашифровать свой собственный текст M* для получения правдоподобного шифротекста C*, не имея подлинного ключа, называется криптоаналитической атакой. Если предпринятые криптоаналитические атаки не достигают поставленной цели и криптоаналитик не может, не имея подлинного ключа, вывести M из C или C* из M*, то систему называют криптостойкой.

Криптоанализ – это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу. Успешный криптоанализ может раскрыть исходный текст или ключ.

Традиционные симметричные алгоритмы шифрования

Среди наиболее распространенных простейших алгоритмов шифрования информации можно выделить шифры перестановок и шифры замены(подстановки).

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Примерами шифров перестановки являются шифр «скитала»,шифрующие таблицы.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены.

Примерами шифров замены являются моноалфавитная замена, многоалфавитная замена, шифр Цезаря, шифр Гросфельда, шифр Вижинера.

Система шифрования Цезаря

Шифр Цезаря является частным случаем шифра простой замены. Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около50 г. до н.э.). При шифровании исходного текста методом Цезаря, каждая буква открытого текста заменяется на букву того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту от исходной буквы на K букв (позиций). При достижении конца алфавита выполняется циклический переход к его началу. Смещение K в данном случае определяет ключ шифрования. Совокупность возможных подстановок для больших букв английского алфавита и K=3 представлена в таблице 1.

Таблица 1. Таблица подстановок A

A	→	D		H	→	K		O	→	R		V	→	Y
B	→	E		I	→	L		P	→	S		W	→	Z
C	→	F		J	→	M		Q	→	T		X	→	A
D	→	G		K	→	N		R	→	U		Y	→	B
E	→	H		L	→	O		S	→	V		Z	→	C
F	→	I		M	→	P		T	→	W				
G	→	J		N	→	Q		U	→	X				

Математическая модель шифра Цезаря записывается в виде (1)

$$C=(P+K) \bmod M \quad (1)$$

C – код символа шифротекста, P – код символа открытого текста, K – коэффициент сдвига, M – размер алфавита, mod – операция нахождения остатка от деления на M.

Например, результатом шифрования открытого текста RED APPLE по методу Цезаря с ключом K =3 будет являться последовательность UHGASSOH

Задание к лабораторной работе:

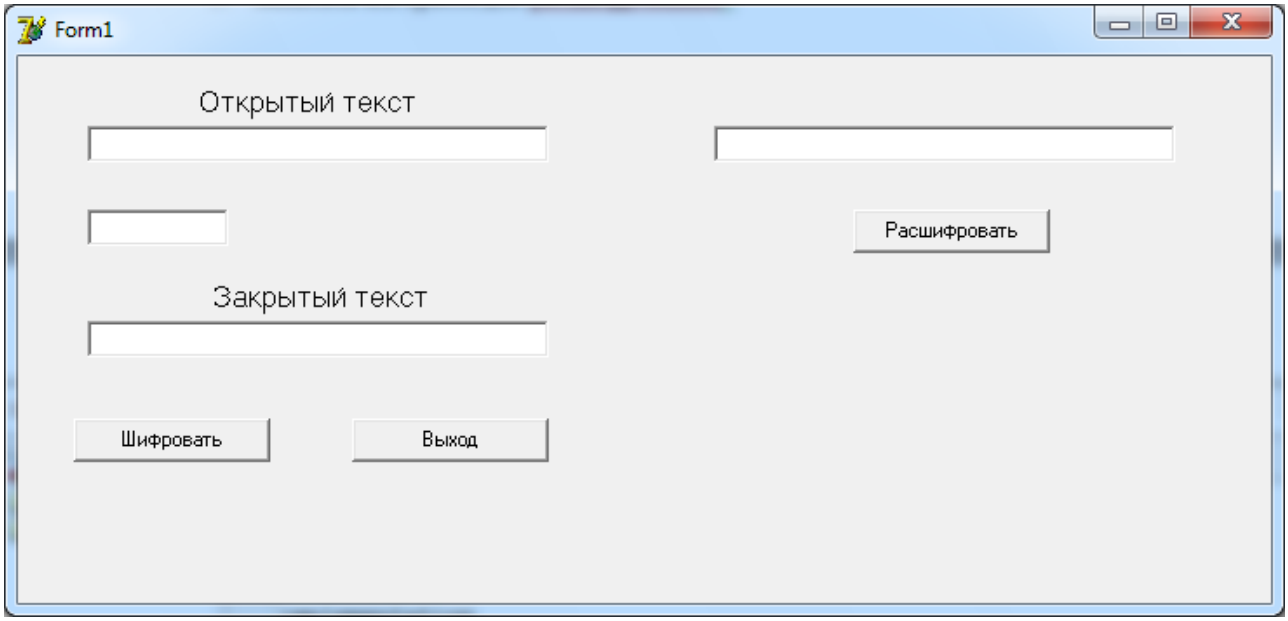
Реализовать систему шифрования Цезаря в программной оболочке Delphi.

Порядок выполнения работы:

1. Запустить программу «Delphi.exe»
2. Создать новую форму и добавить на нее Edit1, Edit2, Edit3, Edit4, Button1, Button2, Button3 ,Label1, Label2.
3. Для Button1 задаем две переменные типа string и две переменные типа integer.
4. Записываем алгоритм для шифрования.

```
begin
st:=Edit1.Text;
x:=StrToInt(Edit2.Text);
Edit3.Text:=' ';
for i:=1 to length(st) do
if (st[i]<>' ') and (st[i]<>'.') then
begin
s:=chr((ord(st[i])+x) mod 255);
Edit3.Text:=Edit3.Text+s;
end;
end;
```

5. Записать алгоритм для расшифрования..



Оформление отчета:

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

Отчет должен содержать:

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

Контрольные вопросы:

1. Определение криптографии?
2. Определение криптоанализа?
3. Два простейших способа шифрования?
4. Описать шифр Цезаря ?

Лабораторная работа №5
Алгоритм шифрования XOR.

Цель работы: является изучение алгоритма шифрования XOR при использовании открытого ключа и гаммы псевдослучайных чисел.

Краткая теория.

XOR – это функция булевой алгебры, носящей название «исключающее или», данная функция используется для работы с данными представленными в двоичной системе исчисления. Основным достоинством, позволяющим использовать эту функцию в шифровальных алгоритмах является ее обратимость, при отсутствии потери информации.

Как ни странно, но самым простым и одним из самых эффективных (при правильном использовании) алгоритмов шифрования является так называемое XOR-шифрование. Как известно из булевой алгебры, операция логического сложения «$\oplus$» по модулю 2 (или логического исключающего ИЛИ — XOR, eXclusive OR) имеет следующую семантику:

таблица истинности для OR:

x_i	y_i	$x_i \wedge y_i$
0	0	0
0	1	1
1	1	1
1	1	0

, но для XOR:

x_i	y_i	$x_i \oplus y_i$
0	0	0
0	1	1
1	0	1
1	1	0

, то есть:

$$x = 10011101$$
$$\oplus$$
$$\underline{y = 01001100}$$
$$z = 11010001$$

То есть, операция z = x $\oplus$ y по сути поразрядная (побитовая — результат не зависит от соседних битов). Если только один из соответствующих битов равен 1, то результат 1. А если оба 0 или оба 1, то результат 0. Если внимательно посмотреть на результат применения XOR к двум двоичным числам, то можно заметить, что мы можем восстановить одно из слагаемых при помощи второго: $x = z \oplus y$ или $y = z \oplus x$.

1) Логическое умножение или конъюнкция:

Конъюнкция - это сложное логическое выражение, которое считается истинным в том и только том случае, когда оба простых выражения являются истинными, во всех остальных случаях данное сложеное выражение ложно.
Обозначение: F = A & B.

Таблица истинности для конъюнкции

A	B	F
1	1	1
1	0	0
0	1	0
0	0	0

2) Логическое сложение или дизъюнкция:

Дизъюнкция - это сложное логическое выражение, которое истинно, если хотя бы одно из простых логических выражений истинно и ложно тогда и только тогда, когда оба простых логических выраженныя ложны.
Обозначение: F = A + B. Таблица истинности для дизъюнкции

A	B	F
1	1	1
1	0	1
0	1	1
0	0	0

3) Логическое отрицание или инверсия:

Инверсия - это сложное логическое выражение, если исходное логическое выражение истинно, то результат отрицания будет ложным, и наоборот, если исходное логическое выражение ложно, то результат отрицания будет истинным. Другими простыми слова, данная операция означает, что к исходному логическому выражению добавляется частица НЕ или слова НЕВЕРНО, ЧТО.

Таблица истинности для инверсии

A	неA
1	0
0	1

4) Логическое следование или импликация:

Импликация - это сложное логическое выражение, которое истинно во всех случаях, кроме как из истины следует ложь. То есть данная логическая операция связывает два простых логических выражения, из которых первое является условием (A), а второе (B) является следствием.

Таблица истинности для импликации

A	B	F
1	1	1
1	0	0
0	1	1
0	0	1

5) Логическая равнозначность или эквивалентность:

Эквивалентность - это сложное логическое выражение, которое является истинным тогда и только тогда, когда оба простых логических выражения имеют одинаковую истинность.

Таблица истинности для эквивалентности

A	B	F
1	1	1
1	0	0
0	1	0
0	0	1

Функции в Delphi:

Функция Chr конвертирует целое число IntValue или в AnsiChar или в WideChar

Функция Ord возвращает порядковое значение символа или элемента перечисления в виде неотрицательного целого.

Функция Length возвращает или число символов в String, или число элементов в Array.

Ключевое слово Div дает целое число полученное в результате деления делимого делителеля.

Операторы цикла в Delphi:

оператор цикла For – Do

Синтаксис оператора имеет две разновидности:

For счетчик цикла:=нач.знач. To конеч.знач. Do оператор

For счетчик цикла:=нач.знач. Downto конеч.знач. Do оператор

Здесь конструкция For .. Do называется заголовком цикла, оператор – телом цикла.

Для циклов должны соблюдаться следующие правила и ограничения:

начальное и конечное значения счетчика цикла должны быть одинаковых простых типов, кроме Real;

в теле цикла счетчик не должен менять значение;

вход в цикл минуя заголовок запрещен;

для первой разновидности начальное значение не должно быть больше конечного;

для второй разновидности начальное значение не должно быть меньше конечного.

Первая разновидность оператора цикла For работает следующим образом. Сначала счетчик цикла принимает нач.знач. и выполняется оператор, расположенный вслед за словом Do. Затем значение счетчика будет увеличено на шаг счетчика 1 и вновь будет выполнен оператор и т. д., пока счетчик не переберет все значения от нач.знач. до конеч.знач.

Пример.

```
s:=                                                                    0;
For i:=1 to 44 do s:= s + z[i];
```

В результате в переменной s будет накоплена сумма первых 44 элементов массива z.

Другая разновидность оператора For отличается лишь отрицательным шагом –1 счетчика.

Оператор цикла While – Do

Синтаксис оператора:

While логическое выражение Do оператор;

Цикл выполняет оператор, расположенный вслед за словом Do до тех пор, пока истинно логическое выражение, расположенное за словом While ("выполняй, пока истинно").

Пример.

```
x:= 0;
i:=0;
While (x < 101.667) do
Begin
Inc (i);
X:= X + 5.617;
Y[i]:= Func (i + 6, 9 * i, X);
End;
```

В этом примере цикл будет выполняться до тех пор, пока не выполнится условие x < 101.667. В теле цикла переменная X с каждым шагом цикла увеличивает свое значение на 5.617 так, что на определенном шаге условие x < 101.667 впервые не будет выполнено. В этот момент без входа в тело цикл закончит работу.

Оператор цикла Repeat – Until

Синтаксис оператора:

```
Repeat
Оператор1;
Оператор2;
…
ОператорN;
Until логическое выражение;
```

Цикл работает, пока логическое выражение ложно ("повторяй, пока не выполнится").

Пример.

```
s:= 0;
i:=0;
Repeat
```

Inc (i);
s:= s + z[i];
Until (i = 44);

В этом примере цикл будет выполняться до тех пор, пока не выполнится условие i = 44. Результат будет тот же, что в примере для For-цикла.

Функции в MathCad:

round - округление z по числу n. Если n опущен, z округляется к самому близкому целому числу.

rnd - выдаёт однородно распределенное случайное число между 0 и x.

matrix(m, n, f) - выдаёт m x n матрицу, в которой ijth элемент дается как f(i, j).

Эта функция как правило доступна в любом математической или программной среде, позволяющей использовать данные в двоичной системе исчисления. В системе MathCad функция xor реализуется встроенной функцией xor(a,b), а в среде Delphi

операцией - a xor b.

Для работы с массивами в системе MathCad необходимо использовать палитру векторов и матриц.

Рис. 1 Панель векторов и матриц

Диапазон чисел для задания циклов и диапазонов можно получить при помощи функции m..n в палитре вычислений.

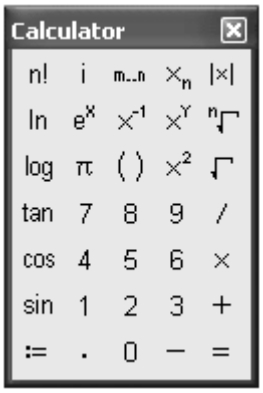


Рис2. Палитра вычислений.

Матрицы задаются через палитру векторов и матриц функцией вектор и матрица, а для ее создания необходимо указать количество строк(rows) и столбцов(columns). Для извлечения чисел из массива необходимо воспользоваться функцией индекс(subscript) в палитре матриц и векторов.

Для реализации алгоритма XOR в среде Delphi необходимо использовать или массивы или строки. Массивы задаются в разделе объявления переменных(var)

в виде A: array[1...10] of char; но в данной работе можно воспользоваться свойствами строковых типов данных и вместо массивов использовать данные стокового типа(s: string;). Для реализации данного алгоритма могут потребоваться функции преобразования типов данных chr(a:integer) и ord(c:char). При работе со строковыми типами данных может пригодится функция Length(s:string);.

Поскольку длина ключа, как правило меньше длины сообщения, то для шифрования всего сообщения длину ключа доводят до длины сообщения при помощи создания ключа длиной равной длине текста путем составления строки или массива равной длине исходного текста и состоящей из повторяющейся строки ключа. Для реализации алгоритма такого растяжения ключа могут потребоваться функции div,For, If и while.

Задание для лабораторной работы.

1) Реализовать алгоритм XOR шифрования в математической системе MathCad, исходным сообщением является одномерный массив с общим числом элементов 20, элементами массива являются числа 0 и 1, ключ представляет собой одномерный массив из 5 элементов 0 и 1.

Шифротекста представить виде одномерного массива из 20 элементов результата каждый элемент которого является результатом операции XOR между элементом сообщения и элементом шифротекста.

2) Реализовать алгоритм XOR шифрования в среде Delphi, при условии, что исходным сообщением является строка текста длиной 15-20 символов, а ключом строка текста из 7-10 символов, вводимых через компонент Edit, вывод шифротекста должен осуществляться в компонент Memo.

Порядок выполнения работ.

1-ое задание:

1. При помощи round и rnd создаем функцию, генерирующая нули и единицы.
2. Задаем исходное сообщение, при помощи функции matrix задаем одномерный массив с общим числом элементов 20.
3. Задаем ключ, при помощи функции matrix задаем одномерный массив с общим числом элементов 5.
4. Выводим значения исходного сообщения.
5. Выводим значения ключа.
6. Применяем XOR к обеим матрицам

$$\text{Encrypt}(i,j) := \left| \begin{array}{l} f \leftarrow \text{mod}(j,5) \\ f \leftarrow 0 \ \text{if} \ f = 5 \\ \text{Crypt} \leftarrow \text{Phrase}_{0,j} \oplus \text{Password}_{0,f} \\ \text{Crypt} \end{array} \right.$$

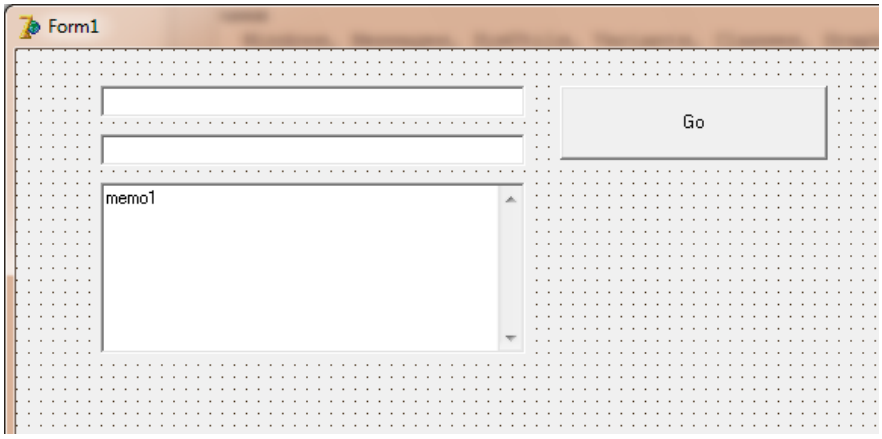
7. Задаем зашифрованное сообщение, при помощи функции matrix задаем одномерный массив с общим числом элементов 20.
8. Выводим зашифрованное сообщение.

Code =

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1	1	0	0	0	1	0	1	0	1	0	1	1	1	0	1	1	1	1	0

2-ое задание:

1. Создаем форму на которой устанавливаем такие объекты как «Edit1», «Edit2», «Memo1», «Button1», «Button2».



2. В общей секции объявления переменных «var» задаем:
   r:integer=1;
3. Во вкладке Unit1 создаем function XOREncrypt(Text,Key: string): string; которая реализует алгоритм шифрования XOR.

4. Используя секцию объявления переменных «var» зададим: счетчик, ключ и шифрованную букву.

```
var
i:integer;  // Счетчик
LKey:string;  //  Длинный ключ
Word:char;  //  Шифрованная буква
```

5. Задаем цикл который будет добивать наш ключ до размеров сообщения для шифрования и цикл который будет каждую букву из сообщения суммировать при помощи «исключающего или» с буквой из длинного ключа:

```
Begin
for i:=0 to (Length(Text) div length(Key)) do
LKey:=LKey+Key;
for i:=1 to length(Text) do
begin
Word:=chr ((ord(Text[i]) XOR ord(LKey[i])));
Result:=Result+Word;
end;
end;
```

Два раза щелкаем левой кнопки мыши на кнопке «GO»

6. При помощи секции объявления переменных «var» зададим:

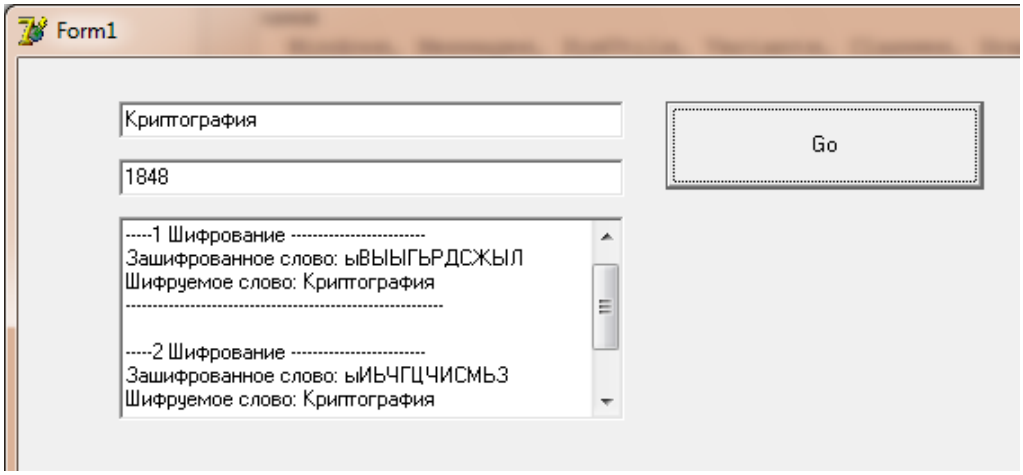
```
var
Text,Encrypt_Text,Decrypt_Text:string;
```

7. Прописываем алгоритм считывания сообщения и ключа и вывода зашифрованного сообщения в поле memo1.

```
begin
Text:=edit1.Text;
Encrypt_Text:=XOREncrypt(Text,edit2.Text);
memo1.Lines.Add('-----' +inttostr(r)+ ' Шифрование -------------------------');
memo1.Lines.Add('Зашифрованное слово: ' + Encrypt_Text);
Decrypt_Text:=XOREncrypt(Encrypt_Text,edit2.Text);
memo1.Lines.Add('Шифруемое слово: ' + edit1.Text);
memo1.Lines.Add('------------------------------------------------------------');
memo1.Lines.Add(' ');
inc(r);
end;
```

Два раза щелкаем левой кнопки мыши на кнопке «Выход» и прописываем ей функцию close.

8. При нажатии на кнопку введенный текст в поле Edit1 присваивается значению Text. Далее присваиваем например Encrypt_Text:= XOREncrypt(Text, edit2.Text); то есть ссылаемся на функцию XOREncrypt которая реализует алгоритм шифрования XOR. Потом выводим значения зашифрованного текста и шифруемого слова в поле Memo1.



Контрольные вопросы:

1. Булевы операции, их типы, условные обозначения и таблицы истинности.

2. Алгоритм шифрования XOR.
3. Назначение функций chr, ord, length, div.
4. Операторы циклов в среде Delphi(или Pascal).

Содержание отчета:

1. Отчет должен быть выполнен на бумаге формата А4.
2. Отчет должен содержать краткую теорию по теме работы.
3. Отчет должен содержать текст программ MathCad с комментариями.
4. Отчет должен содержать листинг программ выполненных в Delphi с комментариями.
5. Отчет должен содержать выводы о проделанной лабораторной работе.

Лабораторная работа №6

Изучение системы охранной сигнализации на базе оборудования «Болид». Настройка тактики работы системы охранной сигнализации при помощи программы «Pprog».

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

Краткая теория.

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

Из определения можно выделить несколько основных задач охранной сигнализации:

Обнаружение нарушителя;

Формирование извещения об обнаружении нарушителя в нужном информационном формате;

Передача извещения в нужном формате в определённое место;

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

Термины и определения

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

Приемно-контрольные приборы (ПКП) – многофункциональные устройства для приёма сигналов от извещателей по шлейфам сигнализации, включения световых и звуковых оповещателей, выдачи информации на пульты централизованного наблюдения, обеспечения процедуры поставки/снятия с помощью органов управления. В качестве органов управления можно использовать выносные и встроенные пульты и клавиатуры с секретными кодами, а также считыватели совместно с электронными идентификаторами (карточками и ключами).

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

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

Неадресная система охранной сигнализации.

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

С2000-4;

Сигнал-20П;

Сигнал-20М.

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

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

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

Тип 4. Охранный;

Тип 5. Охранный с распознаванием нарушения блокировочного контакта извещателя;

Тип 7. Охранный входной;

Тип 11. Тревожный.

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

Адресная система охранной сигнализации.

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

«С2000-ИК» - охранный объёмный оптико-электронный извещатель;

«С2000-ШИК» - охранный оптико-электронный поверхностный;

«С2000-ПИК» - охранный объёмный потолочный оптико-электронный извещатель;

«С2000-СТ» - охранный поверхностный звуковой извещатель;

«С2000-В» - охранный вибрационный поверхностный извещатель;

«С2000-СТИК» - охранный совмещённый объёмный оптико-электронный и поверхностный звуковой извещатель;

«С2000-СМК» - охранный магнитоконтактный извещатель («С2000-СМК Эстет» в исполнении для металлических дверей);

«С2000-КТ» - тревожная кнопка;

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

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

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

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

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

Тип 4. Охранный;

Тип 5. Охранный с распознаванием нарушения блокировочного контакта извещателя;

Тип 7. Охранный входной;

Тип 11. Тревожный;

Адресная система охранной сигнализации под управлением пульта.

Одним из главных критериев построения охранной сигнализации с помощью адресной системы является задача определения места проникновения нарушителя с точностью до места установки сработавшего извещателя, так как в адресной системе каждый извещатель имеет уникальный адрес. Осуществлять управление такой системой можно как с пульта, так и с помощью бесконтактных идентификаторов или бесконтактных Proxy-карт со считывателя, подключенного к контроллеру двухпроводной линии «С2000 КДЛ». При использовании функции управления взятием/снятием со считывателя в память «С2000 КДЛ» можно занести до 512 кодов ключей пользователей. К контроллеру можно подключать любые считыватели ключей Touch Memory или бесконтактных

Proxy-карт, имеющие на выходе интерфейс Touch Memory (например, «Считыватель-2», «С2000 Proxy», «Proxy-2А», «Proxy-3А» и т. д.). Также при использовании адресной системы нет необходимости подводить отдельно питание к каждому извещателю, так как они питаются непосредственно от двухпроводной линии связи.

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

Также на приборе имеются функциональные индикаторы работы и состояния линий связи (RS-485 и ДПЛС). В качестве сетевого контроллера в такой системе используется пульт и/или компьютер с установленным на нём АРМ «Орион Про».

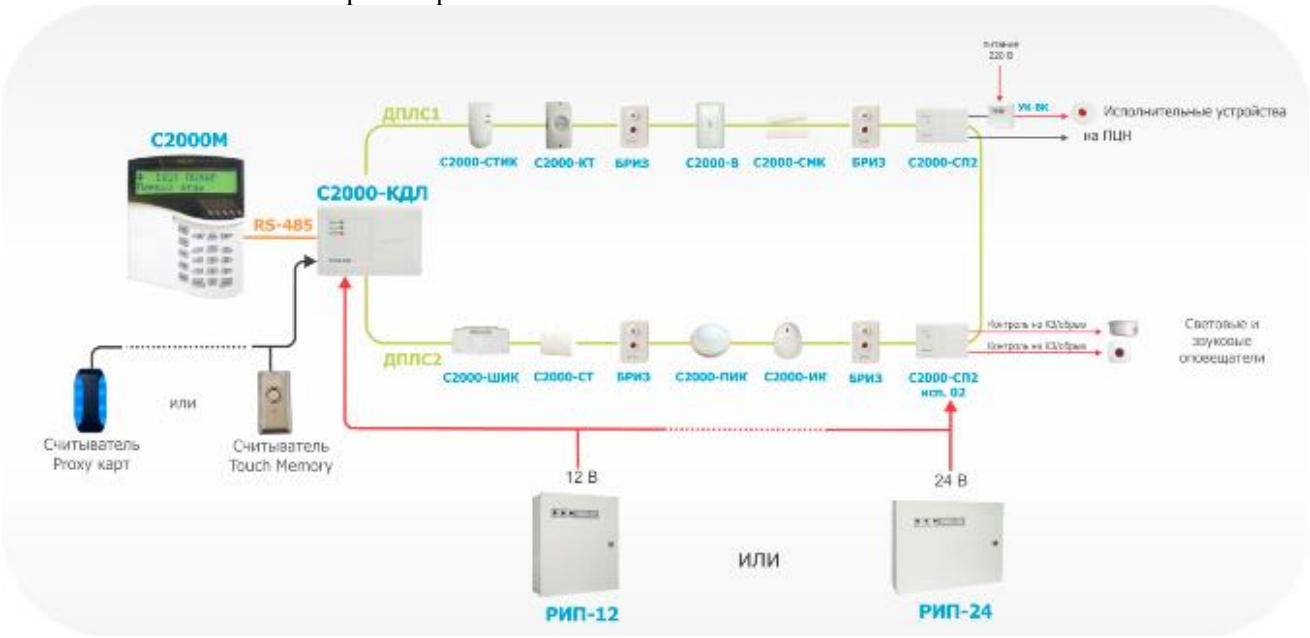


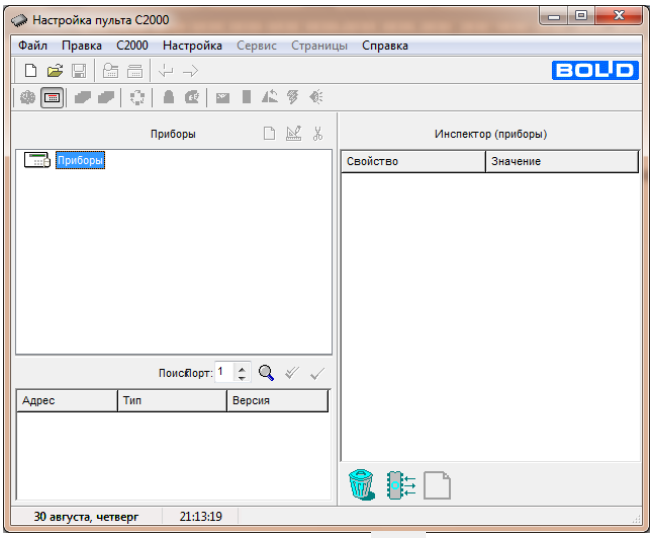
Рисунок 3. Адресная система охранной сигнализации

Задание к лабораторной работе:

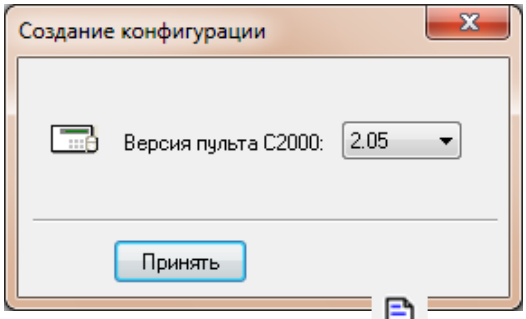
1. Расставить охранные извещатели на плане согласно вашему варианту (см. Приложение А).
2. Задать адрес каждому охранному извещателю.
3. Открыть Pprog.exe
4. Добавить прибор приемно-контрольный охранно-пожарный.
5. Создать разделы для системы охраной сигнализации.
6. Настроить тактику работы реле для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

Порядок выполнения работы:

Запустить программу «Pprog.exe»

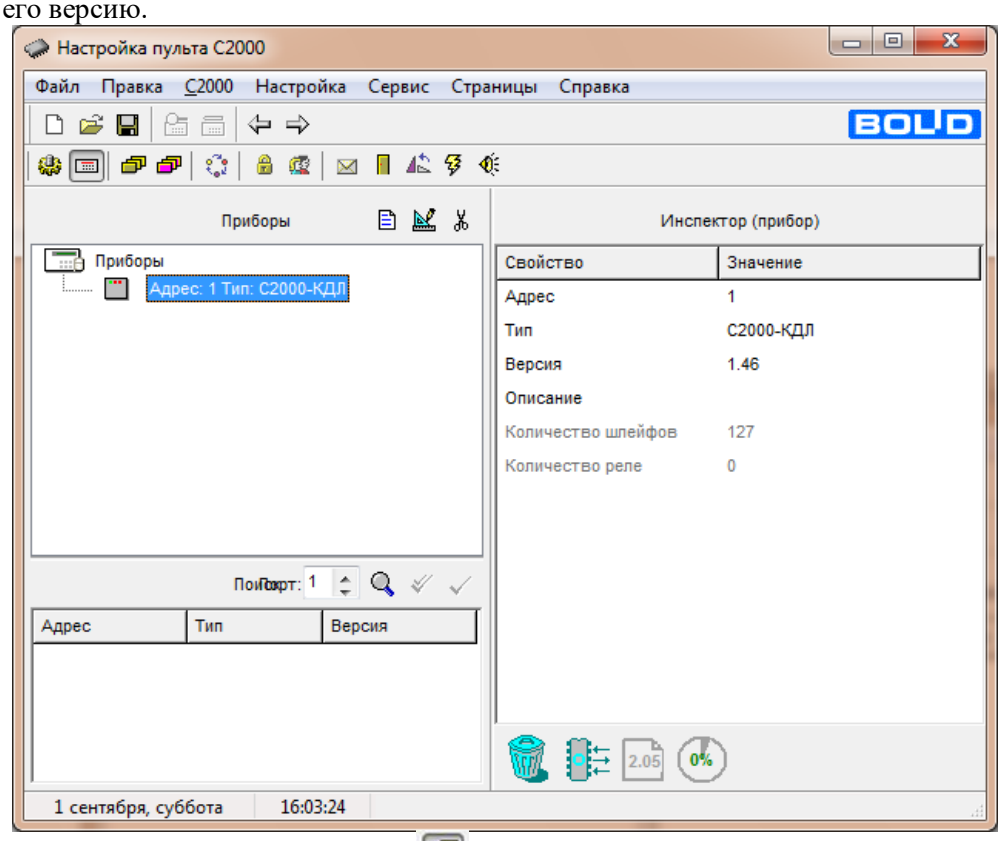


Создать новую конфигурацию при помощи кнопки



Добавить новый прибор при помощи кнопки

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

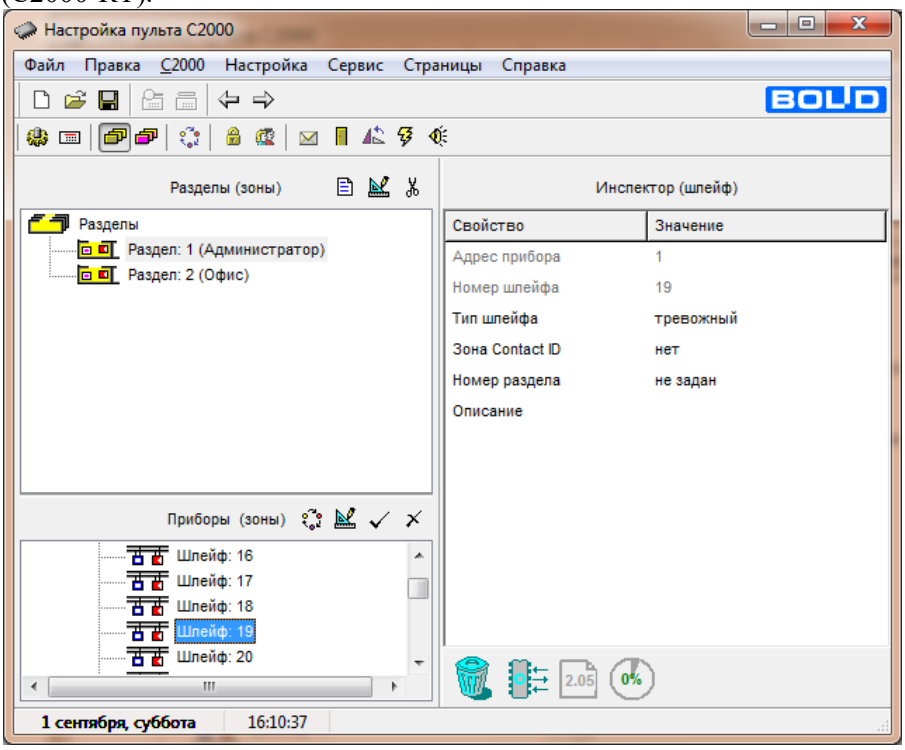


Во вкладке «Разделы» в зоне «Разделы» добавить несколько разделов при помощи кнопки и дать им название при помощи кнопки (согласно индивидуальному заданию).

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

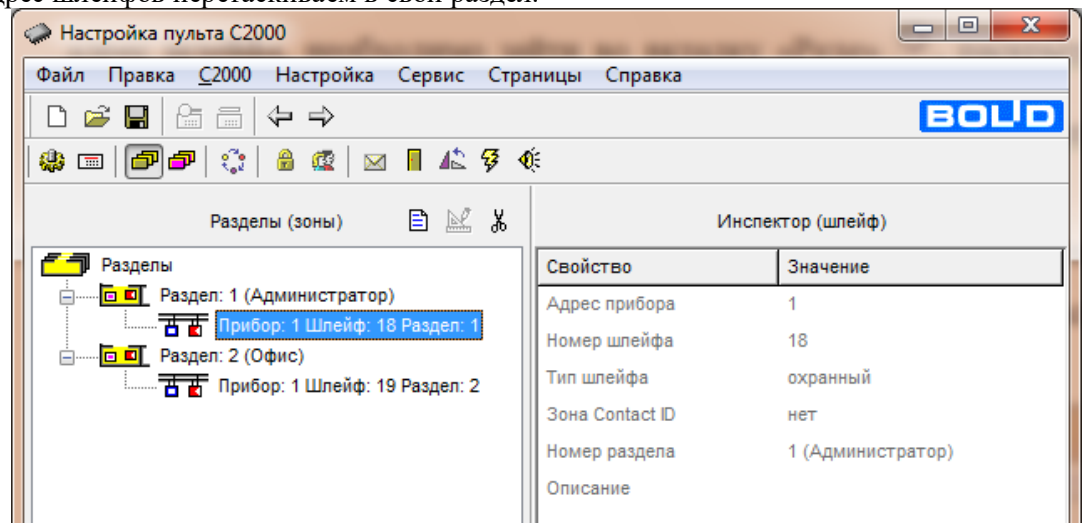
Охранный (С2000-ИК, С2000-СТИК, С2000-ПИК, С2000-СМК, С2000-АР8);

Тревожный (С2000-КТ).



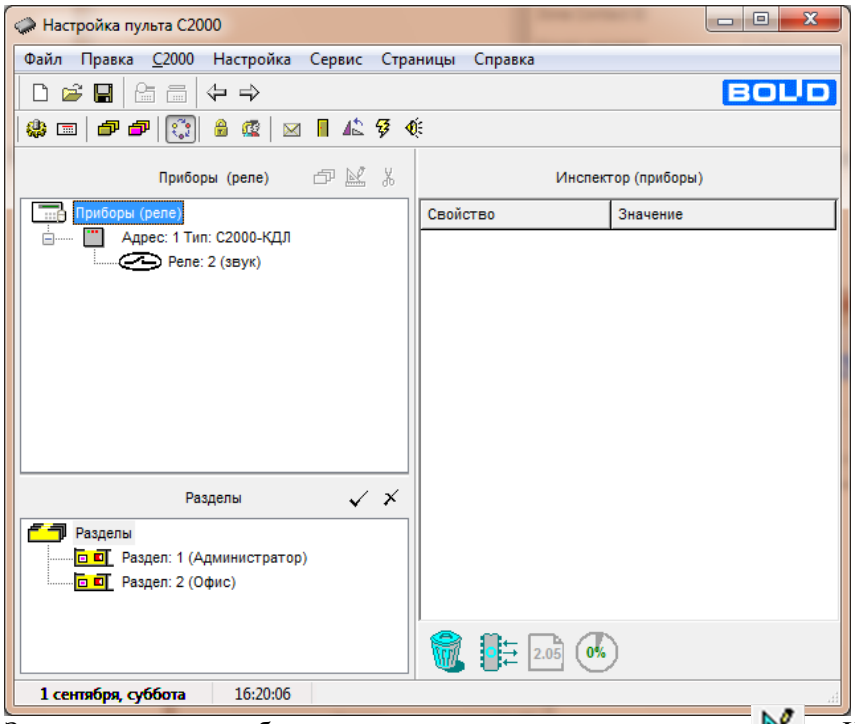
Для того что расписать тактику работы адресного релейного блока С2000-СП2 превращаем 2 адрес шлейфа (согласно исходным данным адресов пожарных извещателей интегрированной системы «Орион» используемые на стенде) прибора С2000-КДЛ в реле при помощи кнопки . Если случайно был превращен в реле не тот адрес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

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



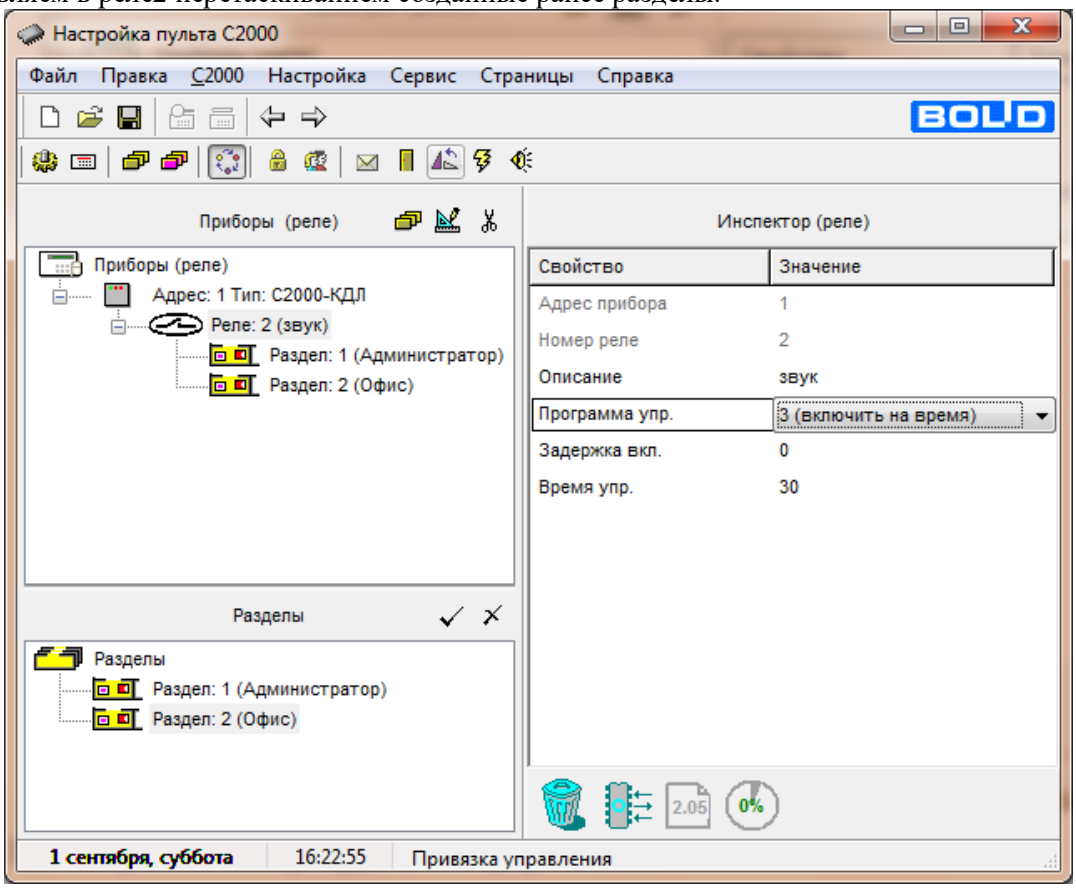
Во вкладке «Реле» раскрываем список реле прибора С2000-КДЛ и изменяем название реле при помощи кнопки :

Реле:2 (Звук).



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

Добавляем в реле2 перетаскиванием созданные ранее разделы.



Сохранить конфигурацию в формате txt.

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

Оформление отчета:

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

Отчет должен содержать:

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

Контрольные вопросы:

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

Лабораторная работа №7

Тема: Изучение системы Орион Про на базе оборудования «Болид». Настройка уровней доступа для охранно-пожарной системы при помощи программы «Pprog».

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

Краткая теория.

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

Уровни доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам (например, пользователям системы) над объектами данных.

Для этого требуется некая система для предоставления субъектам различных прав доступа к объектам. Это система разграничения доступа субъектов к объектам, которая рассматривается в качестве главного средства защиты от несанкционированного доступа к информации.

Существует три модели управления доступом:

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

Дискреционное управление доступом

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

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

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

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

Мандатное управление доступом

Для реализации этого принципа каждому субъекту и объекту должны сопоставляться классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

- субъект может читать объект, только если иерархическая классификация субъекта не меньше, чем иерархическая классификация объекта, и неиерархические категории субъекта включают в себя все иерархические категории объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта не больше, чем классификационный уровень объекта, и все иерархические категории субъекта включаются в неиерархические категории объекта.

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

Ролевое разграничение

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

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

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

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

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

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

Механизм контроля доступа пользователей в системе «Орион» базируется на создании уровней доступа, каждый из которых включает себя ряд разделов системы, которыми будет

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

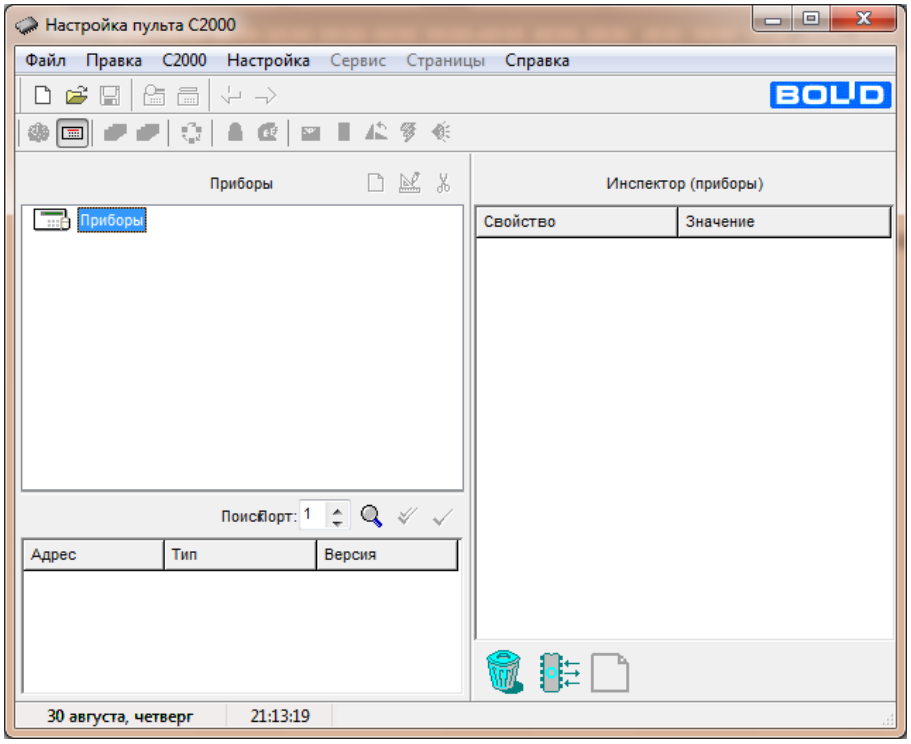
Работа с уровнями доступа (создание/редактирование/удаление) и привязка к ним правил управления определенными разделами системы «Орион» производится на странице «Уровни доступа» программы Pprog, а добавление зарегистрированных пользователей и выбор для них уровня доступа – на странице «Пароли».

Задание к лабораторной работе:

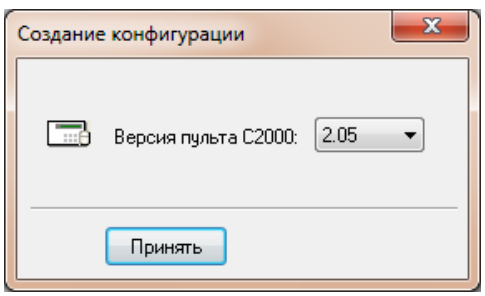
1. Добавить пульт контроля и управления;
2. Добавить прибор приемно-контрольные охранно-пожарный;
3. Создать разделы для системы пожарной и охранной сигнализации;
4. Добавить три уровня доступа;
5. Настроить уровни доступа для охранно-пожарных разделов;

Порядок выполнения работы:

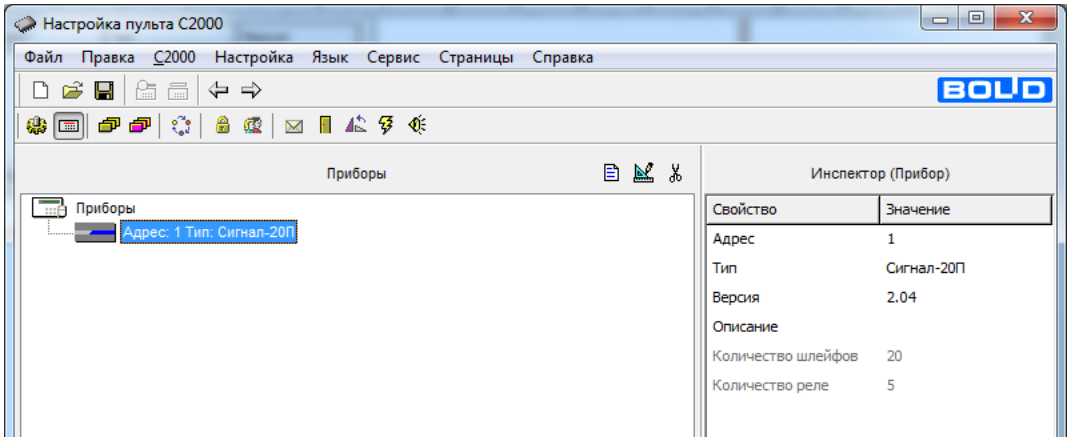
1. Запустить программу «Pprog.exe»



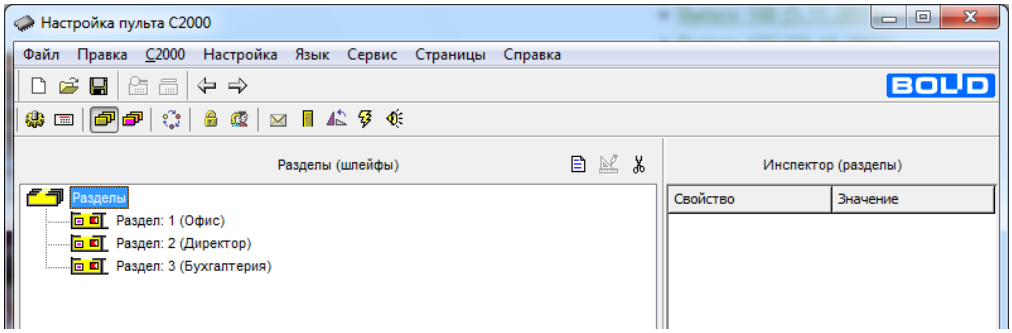
2. Создать новую конфигурацию при помощи кнопки 



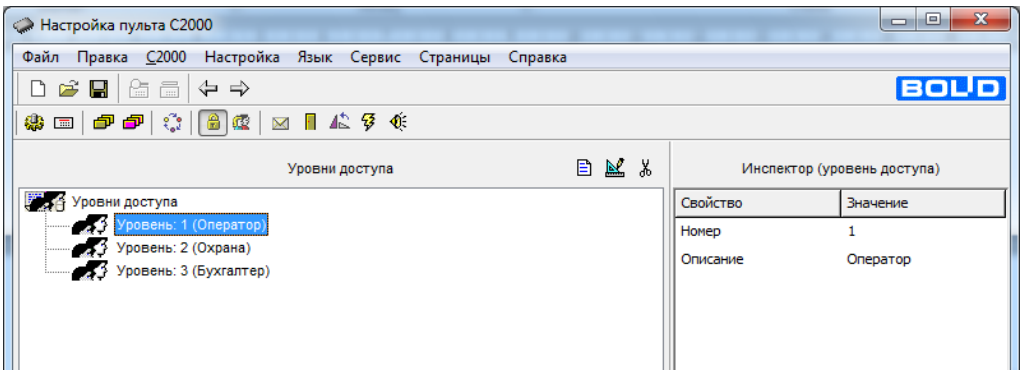
3. Добавить один новый прибор при помощи кнопки 
4. При помощи кнопки «Править прибор»  в инспекторе приборов изменить свойства и значения прибора. Для первого выбираем тип прибора Сигнал-20П.



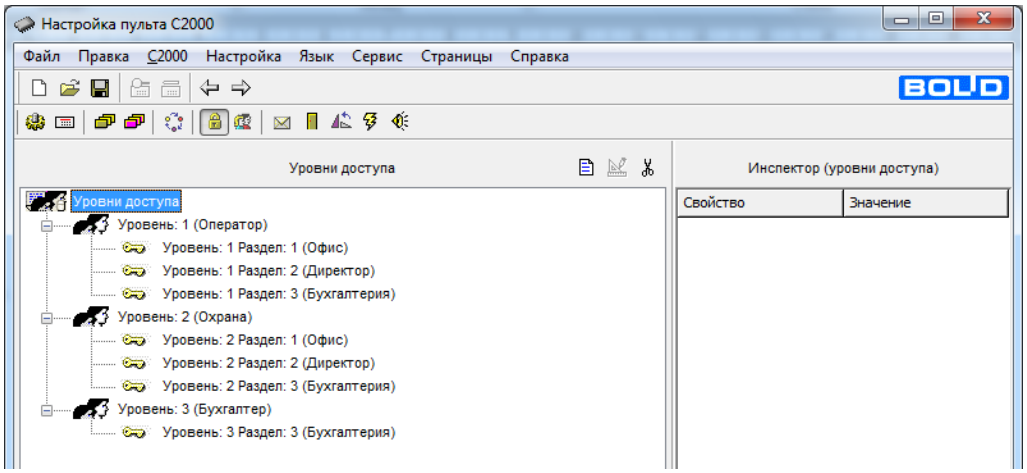
5. Во вкладке «Разделы» в зоне «Разделы»  добавить несколько разделов при помощи кнопки  и дать им название при помощи кнопки  создать три раздела (офис, директор и бухгалтер)



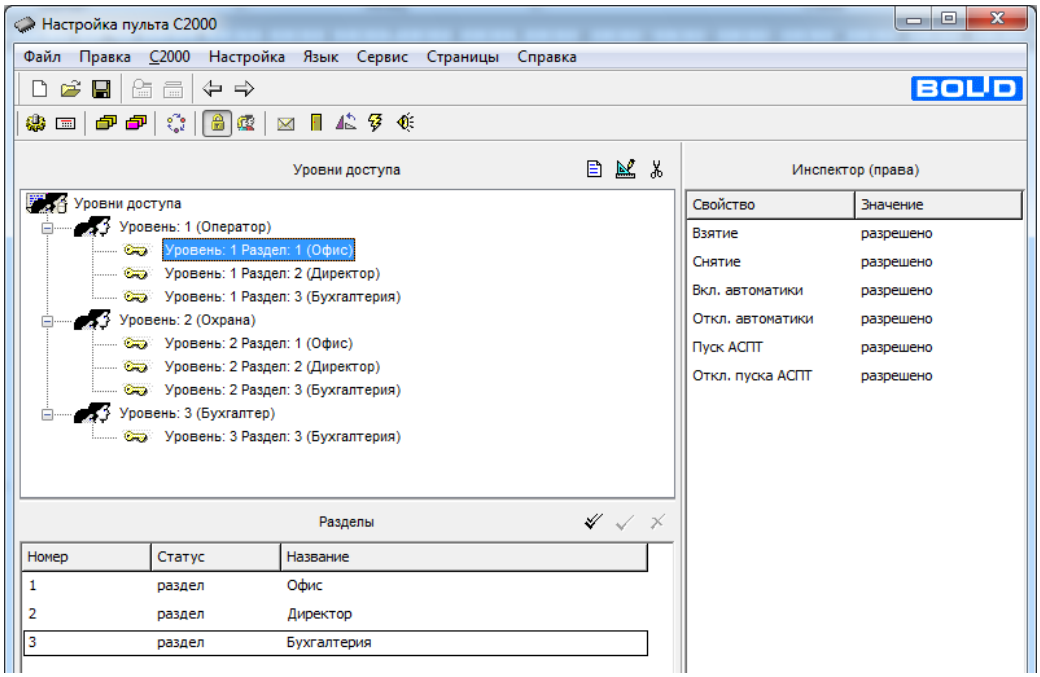
6. Во вкладке «уровни доступа» добавляем три уровня (оператор, охрана и бухгалтер)



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



8. Настраиваем права доступа:
    1. Уровень оператор – разрешаем все;
    2. Уровень охрана – разрешаем только «Взятие» и «Снятие»;
    3. Уровень бухгалтер – разрешаем только «Взятие» и «Снятие»;



Оформление отчета:

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

Отчет должен содержать:

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

3. Заключения и выводы.

Контрольные вопросы:

1. Дайте определение права доступа?
2. Три модели разграничения доступа?
3. Ролевое разграничение доступа?
4. Мандатное разграничение доступа?
5. Дискреционное разграничение доступа?

Лабораторная работа №8

Изучение системы охранной сигнализации на базе оборудования «Стрелец». Настройка паролей для охранно-пожарной системы при помощи Пульта управления.

Цель работы: научиться настраивать уровни доступа интегрированной системы «Стрелец» для системы охранно-пожарной сигнализации.

Краткая теория.

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

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

Существует три модели управления доступом:

4. дискреционная;
5. мандатная;
6. ролевая.

Интегрированная система безопасности “Стрелец-Интеграл” (далее ИСБ) предназначена для организации на объектах подсистем:

- охранной сигнализации;
- пожарной сигнализации;
- оповещения и управления эвакуацией;
- управления автоматическими установками дымоудаления и пожаротушения;
- медицинской сигнализации;
- технологической сигнализации;

Оборудование ИСБ обеспечивает единообразный централизованный контроль радиоканальных и проводных (адресных и неадресных) извещателей и управление радиоканальными и проводными исполнительными устройствами.

Оборудование ИСБ разделяется на сегменты. Оборудование одного сег- мента управляется контроллером сегмента (КСГ). В одном сегменте может функционировать до 127 устройств.

Передача информации внутри сегмента осуществляется по линиям связи интерфейса S2 в направлении к КСГ (информация об изменении состоя- ния), либо обратно (команды управления).

В одной системе может функционировать до 254 сегментов. Оборудование различных сегментов управляется контроллером сети (КС), выполнен- ным на базе персонального компьютера и ПО "Стрелец-Интеграл" ("Стре- лец-Мастер").

Для обмена данными между различными устройствами ИСБ используются линии связи интерфейса S2, построенного на основе сетевой платформы LONWORKS.

Платформа LONWORKS приятa в качестве стандарта сетей автоматизации зданий во многих странах и регламентируется требованиями международ-ного стандарта ANSI/EIA709.1 (EN 14908, ISO/IEC 14908). Платформа используется для передачи данных во многих десятках миллионов устройств, инсталлированных во всём мире. Сетевые интерфейсы LON-WORKS применяются в различных системах автоматизации зданий, безопасности, пожарной сигнализации, пожаротушения и контроля доступа, управления станками, освещением городских и шоссейных улиц, системах отопления и кондиционирования воздуха, измерения расхода энергоресурсов, контроля и управления поездами подземного транспорта, освещения стадионов, а также многих других.

Преимущества использования сетевой платформы LONWORKS следующие:

1. Высокая помехозащищённость линий связи, благодаря:
   - ✓ Дифференциальному способу передачи данных
   - ✓ Гальванической изоляции устройств от линии связи
   - ✓ Алгоритмам помехоустойчивого кодирования
   - ✓ Квитированию и многократному повторению каждого пакета данных
2. Отсутствие необходимости использования кабелей с экранированной витой парой
3. Отсутствие необходимости соблюдения полярности подключения проводников
4. Возможность использования единой среды для передачи сигналов различных систем
5. Возможность использования произвольных сетевых топологий (ши-на, звезда, кольцо, смешанная)
6. Высокая скорость передачи информации (от 78 кбит/с)
7. Поддержка различных физических сред передачи данных (витые па-ры, Ethernet/Internet)
8. Высокая имитостойкость обмена данными, предотвращающая не-санкционированное вмешательство в работу системы.

ИСБ имеет два режима работы безопасности:

1. Стандартный режим

Уровень безопасности соответствует другим уровню других систем безопасности и технологических систем, представленных на рынке.

2. Режим повышенной безопасности

Обмен данными между каждой парой устройств системы сопровождается процедурами двухсторонней аутентификации. Все информационные пакеты, передаваемые по линии связи, подвергаются криптографическому закрытию (шифрации). Благодаря этим мерам исключается несанкционированное вмешательство в работу системы.

При включении режима повышенной безопасности увеличивается загрузка линий связи служебной информацией и возрастают вычислительные затраты обработки информации в

устройствах, поэтому по умолчанию при создании новой системы устанавливается стандартный режим. В случае предъявления жёстких требований к безопасности инсталляции необходимо включить режим повышенной безопасности.

Для включения режима повышенной безопасности необходимо ввести ключ безопасности длиной от одного до восьми пар шестнадцатеричных1 символов (например, “12 34 56 78 9A BC DE F0”). Значение этого ключа следует сохранять в секрете с целью предотвращения постороннего доступа к системе.

Параметры РРОП:

- Контроль ОП/РП – Включение/выключение режимов контроля источников основного и резервного питания.
- Запрет постановки под охрану – Запрещение постановки под охрану разделов расширителя в случае наличия в них взломов либо неисправностей.
- Связь неисправностей с реле – связь с реле собственных событий расширителя (неисправностей либо взломов). События удалённых расширителей могут быть также связаны с реле КР.
- Разрешить обход адресов (ручной) – разрешение выполнения пользователями ручного обхода адресов.
- Разрешить обход адресов (форсированный) - разрешение форсированного обхода адресов (при постановке на охрану нарушенные охранные извещатели будут обойдены).

Вкладка "Пользователи" используется для конфигурирования свойств пользователей РРОП. Пользователи РРОП имеют возможность управления постановкой на охрану, снятия с охраны и сброса пожарных тревог и неисправностей с помощью пультов управления ПУЛ и ПУЛ-Р.

При установке опции "Управление глобальными разделами с ПУЛ и ПУЛ-Р" (доступна только для ПКУ-КР) устройства ПУЛ и ПУЛ-Р, связанные с ПКУ-КР, будут отображать состояние и управлять только глобальными разделами (а не локальными разделами ПКУ-КР).

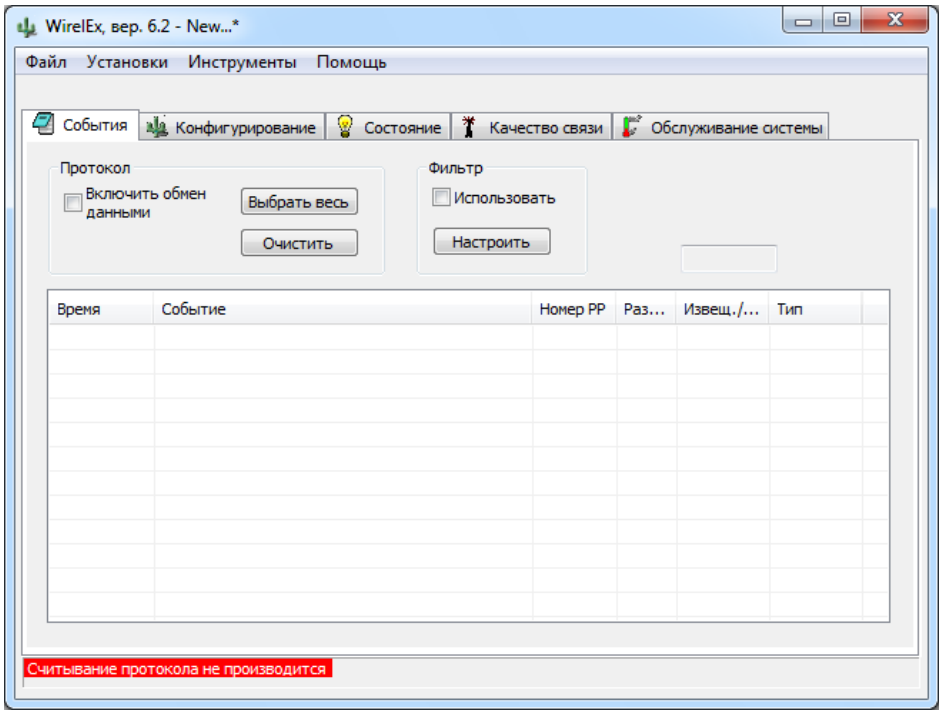
- Список разделов – список локальных разделов, управляемых данным кодом пользователя.
- Пароль – код доступа данного пользователя к управлению списком разделов (число от 0000 до 9999).

Задание к лабораторной работе:

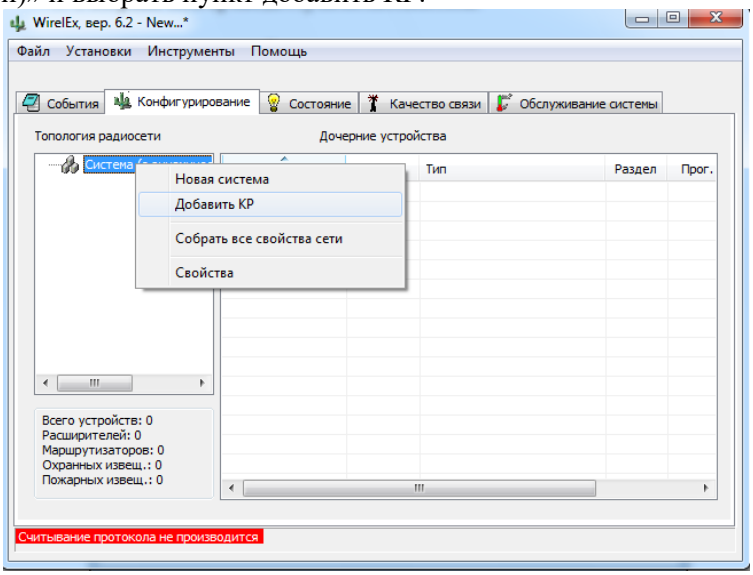
1. Задать новый пароль для созданной системы
2. Добавить пользователей и пароли для каждого пользователя.
    - Охрана (разделы 1-10)
    - Директор (разделы (1-3)
    - Бухгалтер (раздел 9)
    - Юрист (раздел 11)

Порядок выполнения работы:

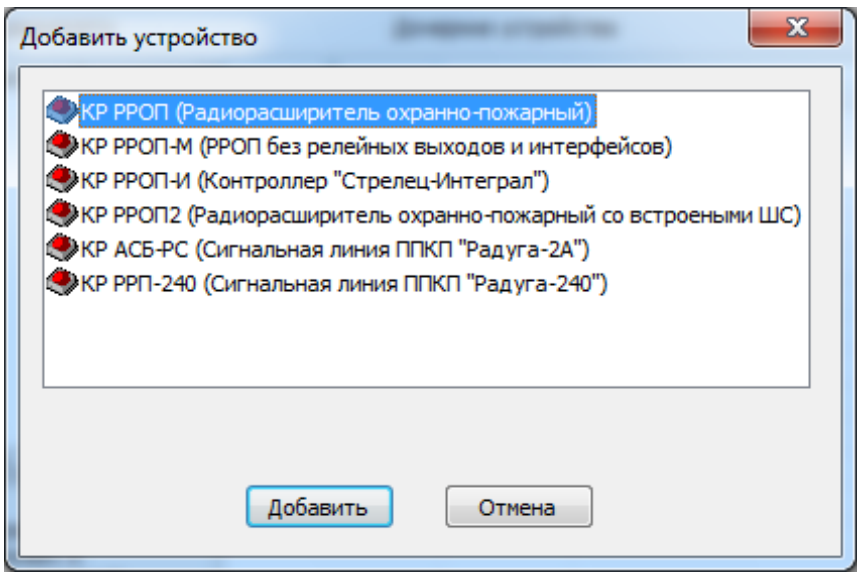
1. Запустить программу WirelEx.exe



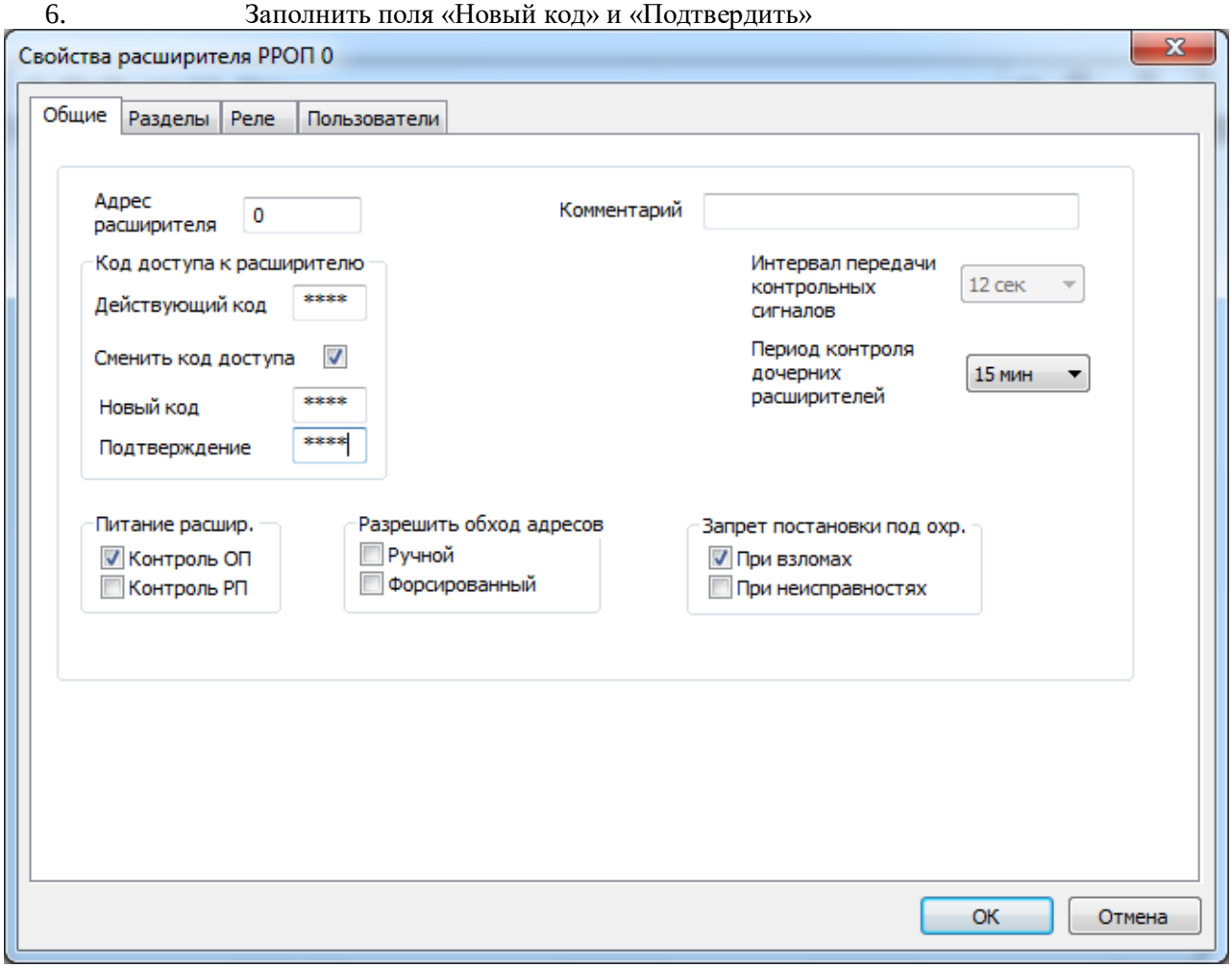
2. Открыть вкладку конфигурирование
3. Щелкнуть правой клавишей мыши на пункте «Система (с динамической маршрутизацией)» и выбрать пункт добавить КР.



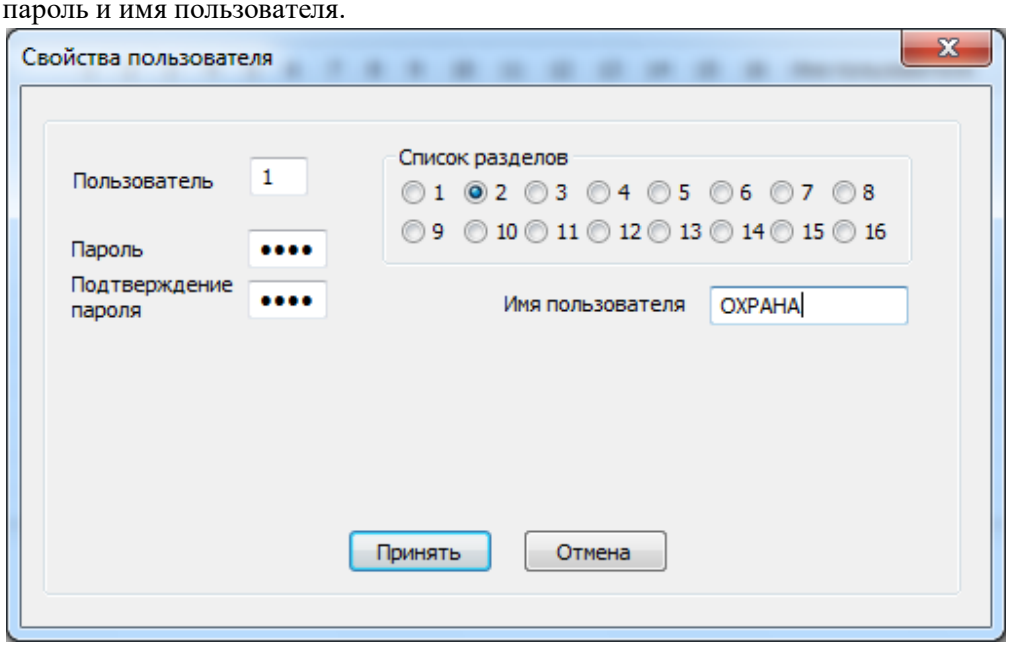
4. Из появившегося списка выбираем «КР РРОП»



5. В окне «Свойства расширителя РРОП 0» во вкладке общие ставим галочку в пункте «Сменить код доступа»
6. Заполнить поля «Новый код» и «Подтвердить»



7. Открываем вкладку Пользователи
8. Делаем правый клик на строке с нужным номером пользователя и в появившемся окне выбираем пункт «Добавить пользователя»
9. В открывшемся окне «Свойства пользователей» ставим галочку в нужном разделе, а также задаем пароль и имя пользователя.



10. Нажимаем принять и выходим и окна «Свойства расширителя РРОП 0»
11. Сохранить конфигурацию в формате sts.

Оформление отчета:

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

Отчет должен содержать:

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

Контрольные вопросы:

1. Дайте определение права доступа?
2. Три модели разграничения доступа?
3. Два режима работы безопасности ИСБ?
4. Максимальная длина пароля в системе ИСБ?
5. Предназначение интегрированная система безопасности “Стрелец-Интеграл”?

Лабораторная работа №9
Изучение системы пожарной сигнализации на базе оборудования «Стрелец».

Цель работы: научиться настраивать параметры и тактику работы интегрированной системы «Стрелец» для системы пожарной сигнализации.

Краткая теория.

Пожарная сигнализация – совокупность технических средств для обнаружения пожара, обработки, представления в заданном виде извещения о пожаре, специальной информации и (или) выдачи команд на включение автоматических установок пожаротушения и технические устройства.

Основные задачи функционирования системы пожарной сигнализации в совокупности с организационными мероприятиями – это задачи спасения жизни людей и сохранения имущества. Минимизация ущерба при пожаре напрямую зависит от своевременного обнаружения и локализации очага возгорания.

Термины и определения:

1. Шлейф пожарной сигнализации – это линия связи в системе пожарной сигнализации между приёмно-контрольным прибором, пожарным извещателем и другими техническими средствами системы пожарной сигнализации
2. Пожарные извещатели – техническое средство, предназначенное для обнаружения факторов пожара и/или формирования сигнала о пожаре. Существуют различные факторы пожара – дым, тепло, открытое пламя.
3. Приёмно-контрольные охранно-пожарные приборы – многофункциональные устройства, предназначенные для приёма сигналов от извещателей по шлейфам сигнализации, включения световых и звуковых оповещателей, выдачи информации на пульты централизованного наблюдения, обеспечения процедуры управления состоянием зон (шлейфов) с помощью органов управления. В качестве органов управления можно использовать выносные и встроенные клавиатуры с секретными кодами, а также считыватели совместно с электронными идентификаторами (карточками и ключами).

4. Оповещатели - устройства для оповещения людей о тревоге на объекте с помощью звуковых или световых сигналов.
5. ВУОС – выносное устройство оптической индикации. Предназначены для определения места сработавшего извещателя (если извещатели не имеют своего адресного устройства).

Принципы обнаружения факторов пожара

В системах пожарной сигнализации извещатели предназначены для обнаружения конкретного фактора пожара или комбинаций факторов:

1. Дым. При оценке этого фактора извещателем анализируется наличие продуктов горения в воздухе в объёме защищаемого помещения. Можно выделить два наиболее распространённых типа извещателей, работающих по факту обнаружения дыма:
   - Извещатели, производящие локальный (точечный) контроль оптической плотности воздуха, попадающего в оптическую камеру извещателя при перемещении воздушных потоков в помещении. Для этого в оптической камере пожарного извещателя под определённым углом устанавливаются инфракрасный светодиод и фотоприёмник. В дежурном режиме работы извещателя инфракрасное излучение от светодиода не попадает на фотоприёмник. Однако при наличии в оптической камере дыма, его частицы рассеивают инфракрасное излучение, и оно достигает фотоприёмника. При потоке отражённого света выше установленной величины извещатель пожарный дымовой формирует сигнал пожарной тревоги.
   - Извещатели, контролирующие оптическую плотность воздуха в определённом объёме (линейные извещатели). Данные извещатели являются двухкомпонентными, состоящими из излучателя и приёмника (либо из одного блока приёмника-излучателя и отражателя). Приёмник и передатчик такого извещателя располагаются у потолка на противоположных стенах защищаемого помещения. В дежурном режиме сигнал передатчика фиксируется приёмником. В случае возгорания дым, поднимается к потолку, отражая и рассеивая сигнал передатчика. В приёмнике вычисляется отношение уровня текущей величины этого сигнала к уровню сигнала, соответствующему сигналу в дежурном режиме. При достижении определённого порога этой величины формируется тревожное извещение о пожарной тревоге.
2. Тепло. В данном случае извещателями оценивается величина и рост температуры в защищаемом помещении. Тепловые извещатели подразделяются на:
   - Максимальные – формирующие извещение о пожаре при достижении ранее заданных значений температуры окружающей среды;
   - Дифференциальные - формирующие извещение о пожаре при превышении скорости нарастания температуры окружающей среды выше установленного порогового значения;
   - Максимально-дифференциальные - совмещающие функции максимального и дифференциального тепловых пожарных извещателей.

Типы пожарной сигнализации

Неадресная (традиционная) система пожарной сигнализации

В таких системах приёмно-контрольные приборы определяют состояние шлейфа сигнализации, измеряя электрический ток в шлейфе сигнализации с установленными в него извещателями, которые могут находиться лишь в двух статических состояниях: «норма» и «пожар». При фиксации фактора пожара извещатель формирует извещение «пожар», скачкообразно изменяя своё внутреннее сопротивление и, как следствие, изменяется ток в шлейфе сигнализации.

Важно отделить тревожные извещения от служебных, связанных с неисправностями в шлейфе сигнализации или ложными срабатываниями. Поэтому весь диапазон значений сопротивления шлейфа для приемно-контрольного прибора разделён на несколько областей, за каждой из которых закреплён один из режимов («Норма», «Внимание», «Пожар», «Неисправность»). Извещатели определённым образом подключаются к линии шлейфа сигнализации, с учетом их индивидуального внутреннего сопротивления в состоянии «норма» и «пожар».

Для традиционных систем предусматриваются такие особенности, как возможность автоматического сброса питания пожарного извещателя с целью подтверждения сработки, возможность обнаружения нескольких сработавших извещателей в шлейфе, а также реализация механизмов, предусматривающих минимизацию влияния переходных процессов в шлейфах.

Адресно-пороговая система пожарной сигнализации

Отличие адресно-пороговой системы сигнализации от традиционной заключается в топологии построения схемы и алгоритме опроса датчиков. Приёмно-контрольный прибор циклически опрашивает подключенные пожарные извещатели с целью выяснить их состояние. При этом каждый извещатель в шлейфе имеет свой уникальный адрес и может находиться уже в нескольких статических состояниях: «норма», «пожар», «неисправность», «внимание», «запылён» и проч. В отличие от традиционных систем подобный алгоритм опроса позволяет с точностью до извещателя определить место возникновения пожара. Противопожарными нормами в России допускается установка одного адресного извещателя для обнаружения пожара при условии, что по срабатыванию этого пожарного извещателя не формируется сигнал на управление установками пожаротушения или системами оповещения о пожаре 5-го типа.

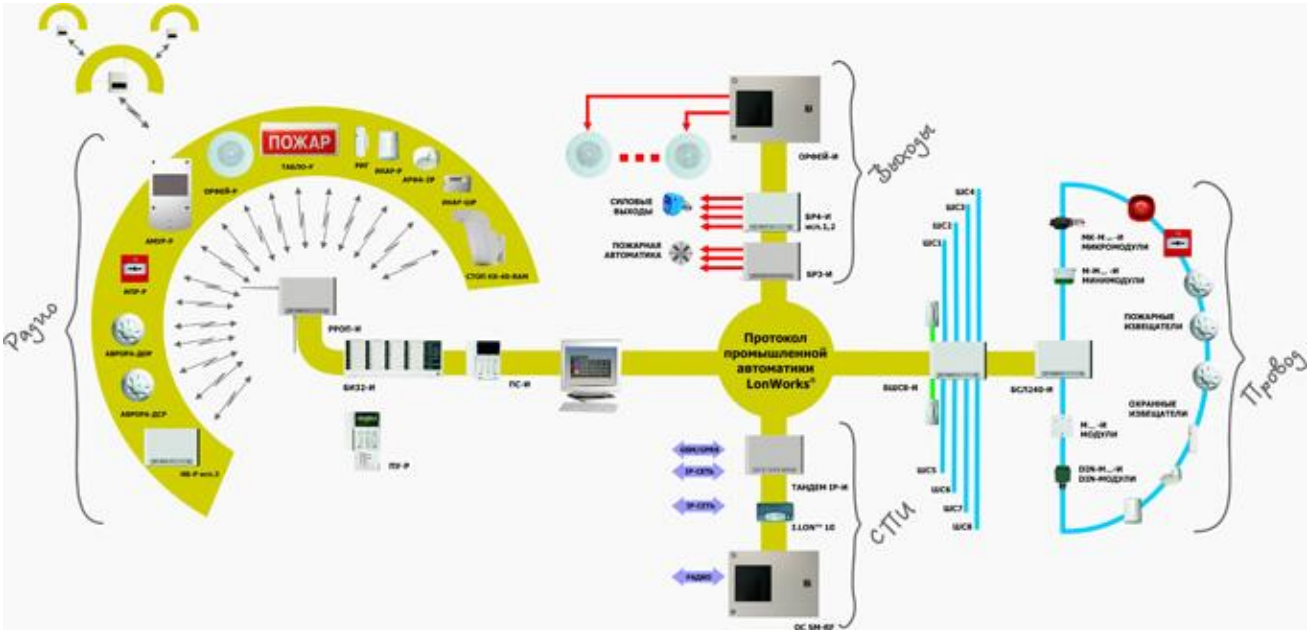
Адресно-аналоговая система пожарной сигнализации

Адресно-аналоговые системы на текущий момент являются самыми прогрессивными, они обладают всеми преимуществами адресно-пороговых систем, а также дополнительным функционалом. В адресно-аналоговых системах решение о состоянии объекта принимает контрольный прибор, а не извещатель. То есть, в конфигурации контрольного прибора для каждого подключенного адресного устройства заданы пороги срабатывания («Норма», «Внимание» и «Пожар»). Это позволяет гибко формировать режимы работы пожарной сигнализации для помещений с разной степенью внешних помех (пыль, уровень производственной задымленности и др.), в том числе в течение суток. Контрольный прибор постоянно производит опрос подключенных устройств и анализирует полученные значения, сравнивая их с пороговыми значениями, заданными в его конфигурации. При этом топология адресной линии, к которой подключены извещатели, может быть кольцевой. В этом случае обрыв адресной линии приведёт к тому, что она просто распадётся на два радиальных независимых шлейфа, которые полностью сохранят свою работоспособность.

Преимущества радиоканальных систем пожарной сигнализации:

- Все устройства радиоканальных систем должны быть укомплектованы надежными источниками основного и резервного питания, при этом информация об отказе каждого источника питания должна передаваться на приемно-контрольное оборудование, а обслуживающий персонал должен быть проинструктирован о требованиях к проведению регламентных работ, в частности, о замене и/или подзарядке источников питания.
- Для устойчивой радиосвязи между компонентами системы на объекте ее применения должны отсутствовать источники электромагнитного излучения, работающие в том же частотном диапазоне, что и сама система, а также экранирующие преграды.
- Электромагнитное излучение, создаваемое компонентами системы, не должно оказывать отрицательного воздействия на иные технические средства, функционирующие на территории защищаемого объекта.
- Алгоритм взаимодействия приемно-контрольного оборудования с периферийными устройствами системы должен обеспечивать автоматический контроль наличия взаимной радиосвязи, а периферийные устройства должны быть снабжены функциями самоконтроля с возможностью передачи информации о своей неисправности или некорректной работе на приемно-контрольное оборудование.
- Тревожный сигнал, поступающий от периферийных устройств, должен иметь приоритет над другими сигналами, формируемыми компонентами системы.

Структура Стрелец-интеграл

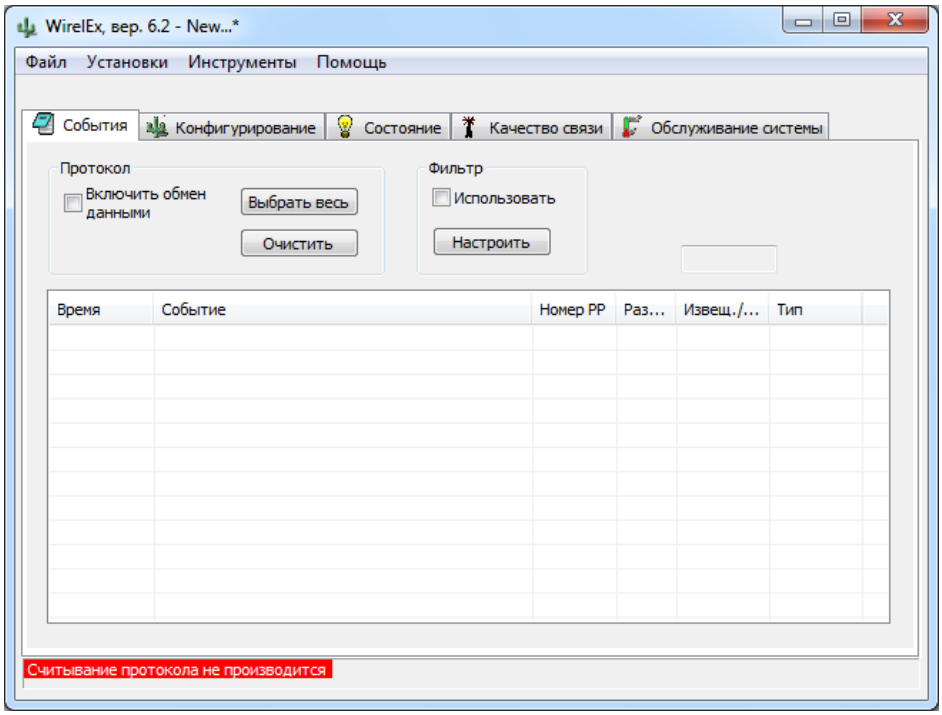


Задание к лабораторной работе:

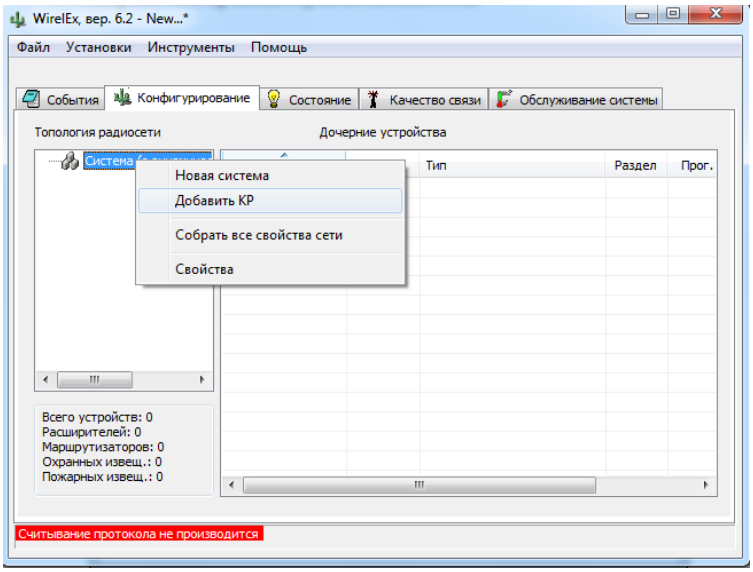
1. Добавить два прибора РРОП
2. Согласно индивидуальному заданию добавить пожарные извещатели к соответствующим раздела.
3. Добавить по одному звуковому оповещателю в каждый РРОП
4. Запрограммировать работу звуковых оповещателей на с работку в каждом использованном разделе.

Порядок выполнения работы:

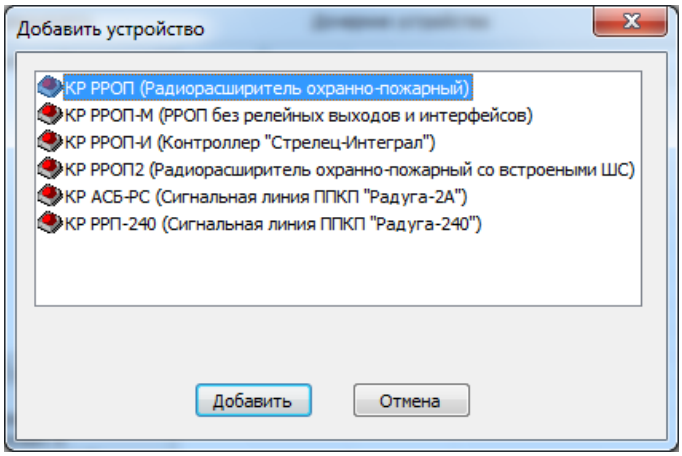
1. Запустить программу WirelEx.exe



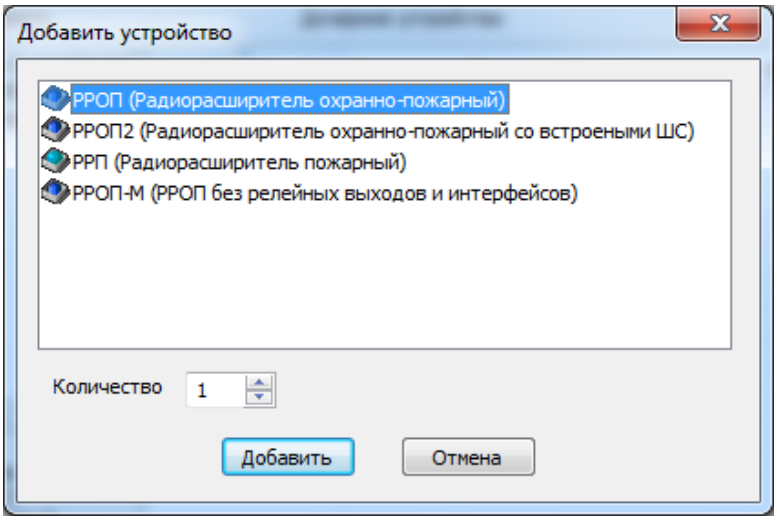
2. Открыть вкладку конфигурирование
3. Щелкнуть правой клавишей мыши на пункте «Система (с динамической маршрутизацией)» и выбрать пункт добавить КР.



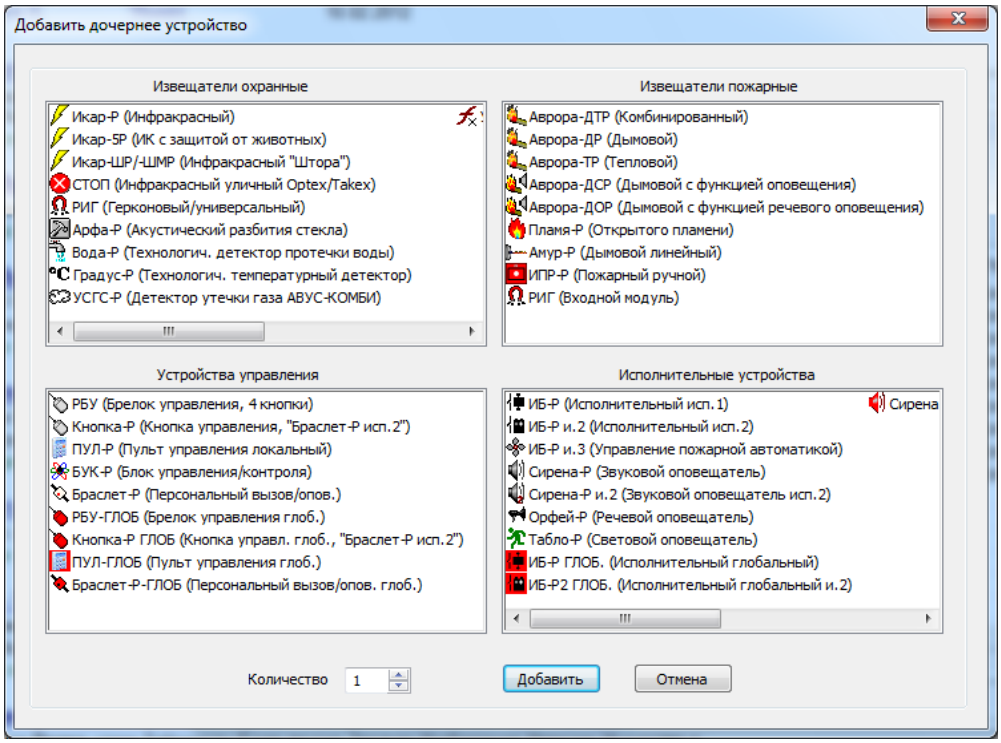
4. Из появившегося списка выбираем «КР РРОП»



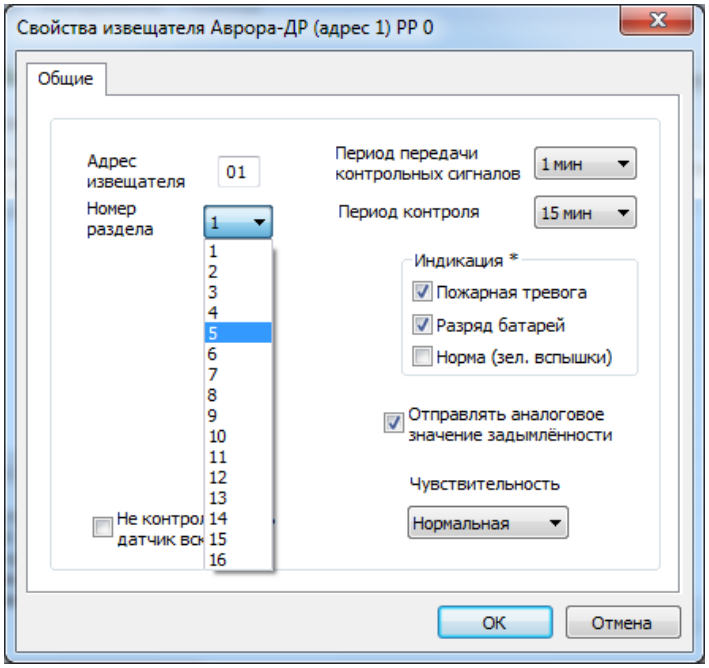
5. Новый КР РРОП появился в поле топология радиосети. Щелкаем правой кнопкой мыши на созданном КР РРОП 0 и выбираем пункт «Добавить расширитель» из появившегося списка выбираем РРОП.



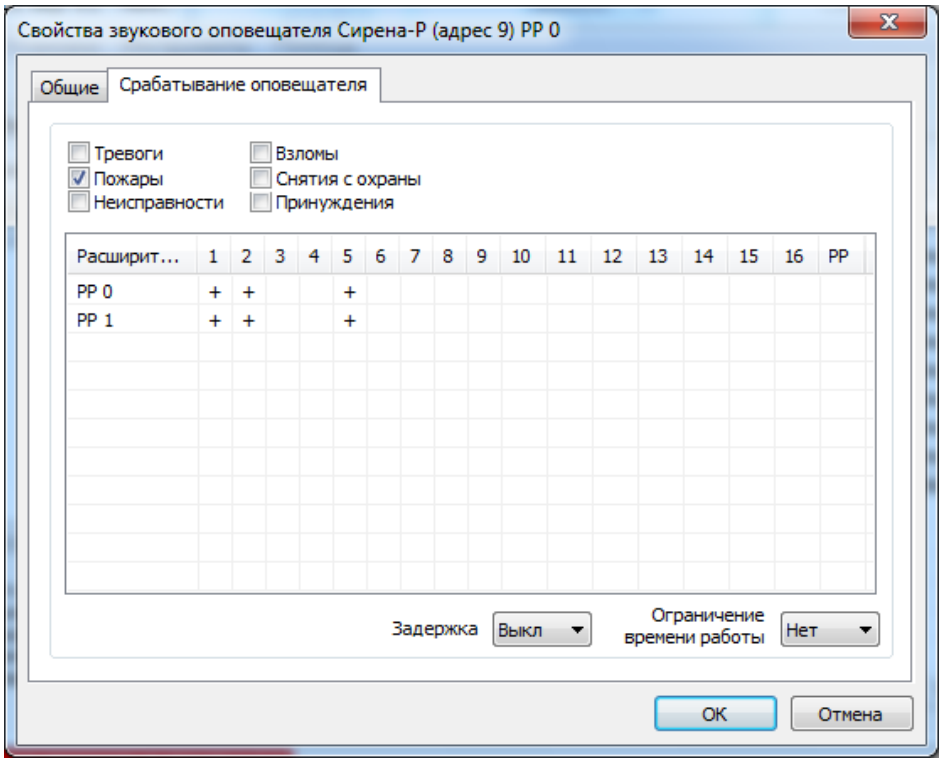
6. Щелкаем правой кнопкой мыши на КР РРОП 0 и выбираем «Добавить дочерние устройства» и выбираем нужные извещатели и их количество.



7. Такие же действия проделываем с РРОП 1
8. Открываем КР РРОП 0 и в поле «Дочерние устройства» щелкаем два раза по извещателю. В появившемся окне «Свойства извещателя» задаем номер раздела извещателя согласно индивидуальному заданию.



9. Такие же действия проделываем с РРОП 1
10. В КР РРОП 0 и РРОП 1 добавляем по одному оповещателю «Сирена-Р» как показано в п.6.
11. Открываем окно «Свойства оповещателя» как показано в п.8.
12. Открываем вкладку «Срабатывание оповещателя» и ставим галочку напротив слова «Пожары». Далее ставим плюсик под каждым использованном разделе (согласно индивидуальному заданию)



13. Сохранить конфигурацию в формате sts.

Индивидуальное задание

№ варианта	Наименование расширителя	Тип извещателя	Кол-во	Номер раздела
1	КР РРОП 0	Аврора-ДР	3	2
		ИПР-Р	1	1
	РРОП 1	Аврора-ДР	2	1
		ИПР-Р	2	2
		Аврора-ТР	1	4
2	КР РРОП 0	Аврора-ДР	2	1
		ИПР-Р	1	2
		Аврора-ДР	3	
	РРОП 1	ИПР-Р	2	1
		Аврора-ТР	2	3
3	КР РРОП 0	Аврора-ДР	3	2
		Аврора-ДР	2	3
	РРОП 1	ИПР-Р	2	1
		Аврора-ТР	3	4
4	КР РРОП 0	Аврора-ДР	2	1
		ИПР-Р	2	2
	РРОП 1	Аврора-ТР	2	4
		Аврора-ДР	3	2
5	КР РРОП 0	Аврора-ДР	4	1
		ИПР-Р	1	2
		Аврора-ТР	1	4
	РРОП 1	ИПР-Р	2	3
		Аврора-ТР	2	2
6	КР РРОП 0	Аврора-ТР	3	1
		ИПР-Р	1	3
	РРОП 1	Аврора-ДР	2	2
		Аврора-ДР	4	1
7	КР РРОП 0	ИПР-Р	2	2

		Аврора-ТР	3	1
	РРОП 1	Аврора-ТР	2	1
		ИПР-Р	2	2
		Аврора-ДР	4	3
8	КР РРОП 0	Аврора-ДР	2	1
		Аврора-ДР	3	3
	РРОП 1	Аврора-ДР	2	1
		ИПР-Р	1	2

Оформление отчета:

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

Отчет должен содержать:

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

Контрольные вопросы:

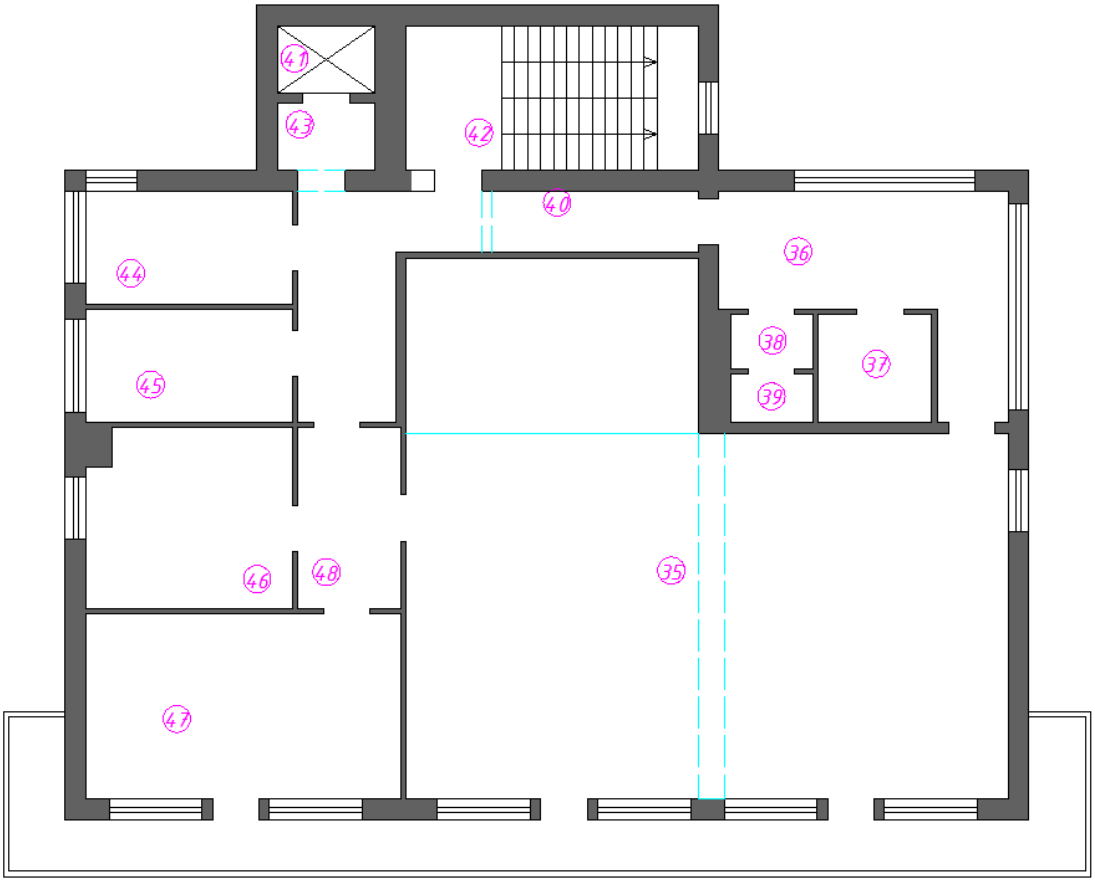
1. Дайте определение пожарной сигнализации?
2. Назовите три типа пожарной сигнализации?
3. Преимущества радиоканальных систем пожарной сигнализации?
4. Максимальное количество разделов в РРОП?

Приложение А

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

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

Вариант для четных студентов в списке преподавателя



Экспликация помещения		
№ помещения	Наименование	Площадь м²
35	зал ЛФК	105,6
36	раздевалка	17,8
37	душевая	3,4
38	санузел	1,3
39	санузел	1,2
40	коридор	14,3
41	лифт	1,7
42	лестничная клетка	15,8
43	коридор	1,7
44	кабинет	8,8
45	кабинет	9,0
46	кабинет	13,6
47	кабинет	20,7
48	коридор	5,2

Вариант для нечетных студентов в списке преподавателя

Экспликация помещения		
№ помещения	Наименование	Площадь м²
18	кабинет	20,1
19	санузел	1,9
20	раздевалка	17,2
21	подсобное помещение	23,9
22	холл	13,9
23	лестничная клетка	15,8
24	лифт	1,7
25	коридор	1,7
26	кабинет	18
27	кладовая	3,8
28	кабинет	17,2
29	кабинет	23,9
30	кабинет	13,9
31	подсобное помещение	3,4
32	пультовая	6,5
33	кабинет	27,5
34	кабинет	16,8