**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационной безопасности


# Система аудита информационной безопасности ГИС

Методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения.

Курск 2017

УДК 004
Составители: О.А. Демченко

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» М.О. Таныгин

**Система аудита информационной безопасности ГИС:** методические указания к выполнению практических работ по дисциплинам / Юго-Зап. гос. Ун-т; сост. О.А. Демченко,А.Г. Спеваков,. Курск, 2017, 14 с.: ил. 15; Библиогр.: с. 14.

Содержат сведения по вопросам создания политики информационной безопасности. Указывается порядок выполнения практических работ, правила оформления, содержание отчета.

Методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. 0,81. Уч. –изд.л. 0,74. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

## ЦЕЛЬ РАБОТЫ

Цель лабораторной работы являетсяизучение процесса создания политики информационной безопасности, ознакомление с методикой анализа рисков и международным стандартом ISO 17799.

## ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Сделать вывод

## СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Цель работы
3. Краткая теория по лабораторной работе
4. Задание
5. Ход выполнения работы
6. На основе полученных отчетов в ГРИФ и КОНДОР сделать анализ полученной политики безопасности и анализа рисков. Привести наиболее значимые данные из отчетов (полностью отчет приносить нет необходимости)
7. Выводы по работе

# ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Организационные методы защиты информации, как правило, используются для парирования угроз. Кроме того, организационные методы используются в любой системе защиты без исключений.

Угроза безопасности - это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.

Уязвимость - это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.

Атака - это действие по использованию уязвимости; реализация угрозы.

Угроза конфиденциальности - это угроза раскрытия информации.

Угроза целостности - это угроза изменения информации.

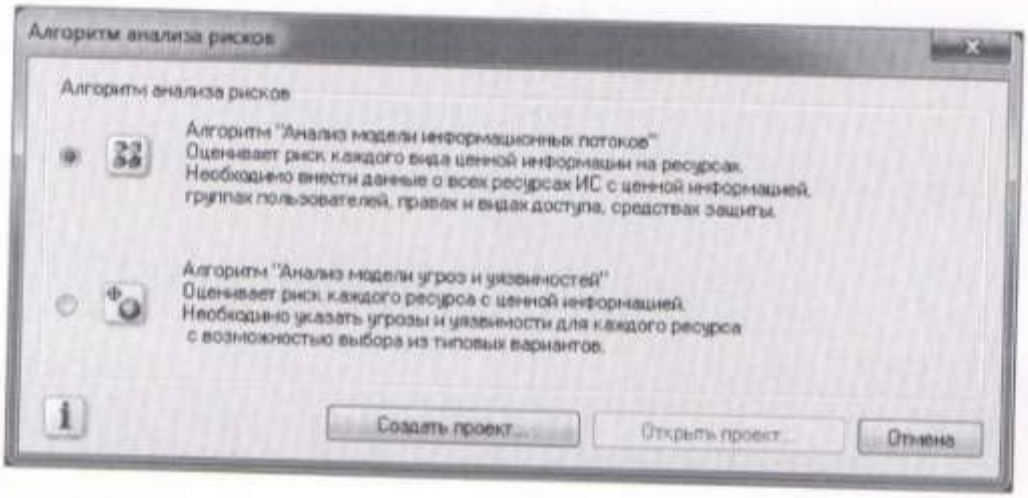
Угроза доступности - это угроза нарушения работоспособности системы при доступе к информации.

Ущерб - это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в информационной системе. Ущерб является характеристикой информационной системы и не зависит от степени её защищенности.

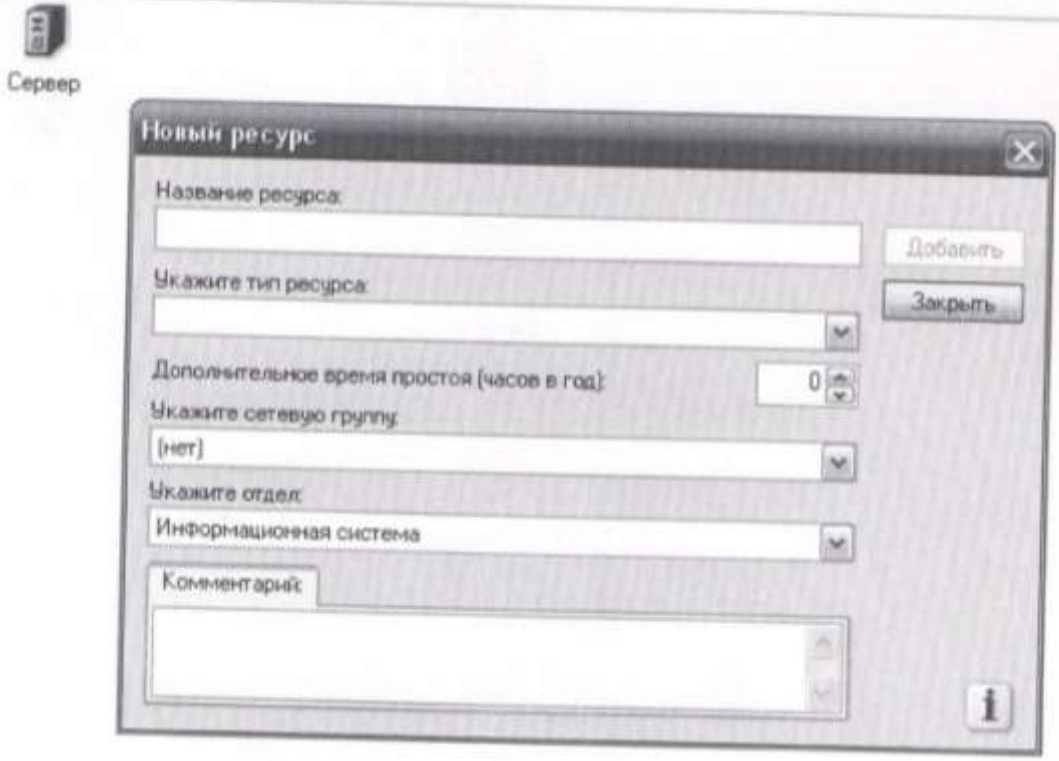
Риск - это вероятный ущерб, который зависит от защищенности системы.

# ВЫПОЛНЕНИЕ РАБОТЫ

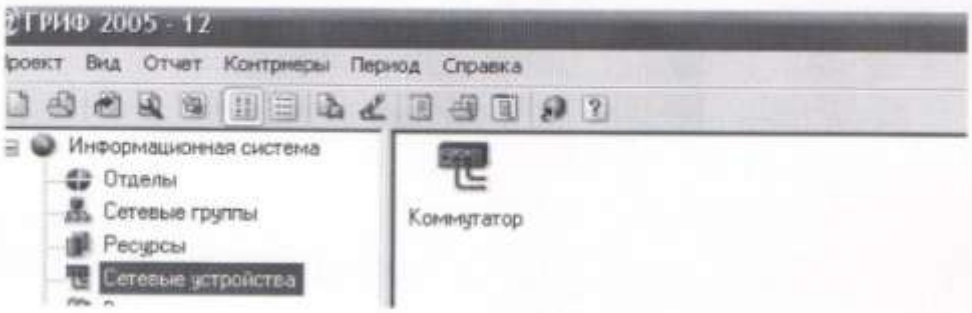
При входе в программу Гриф выбираем модель «анализ модели информационных угроз»



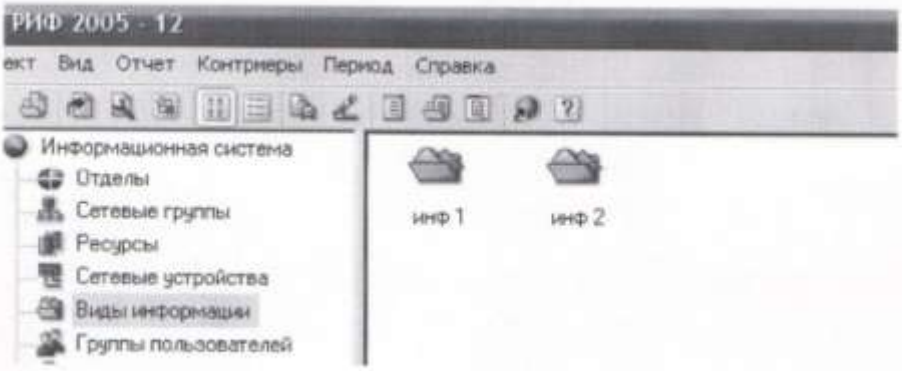

Создадим необходимые нам 3 ресурса



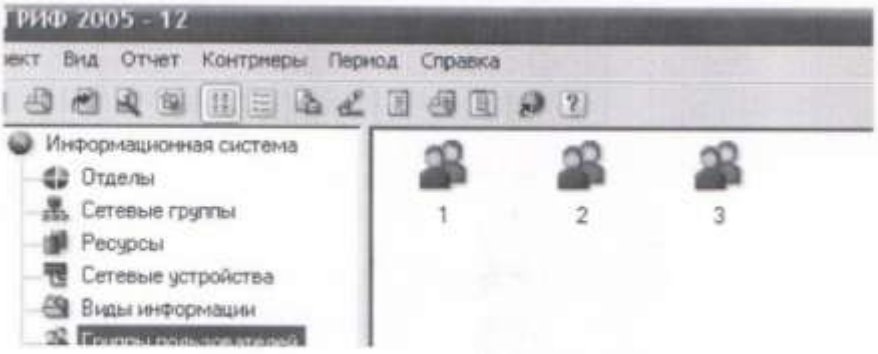
Создадим канал



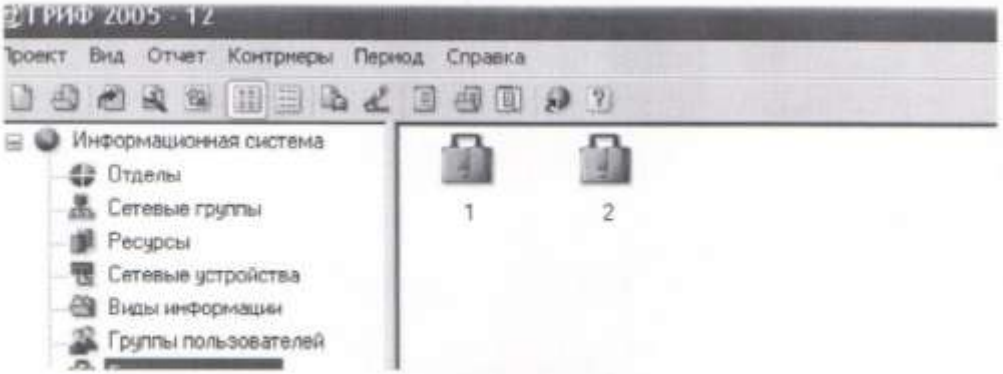

Сделаем 2 вида информации



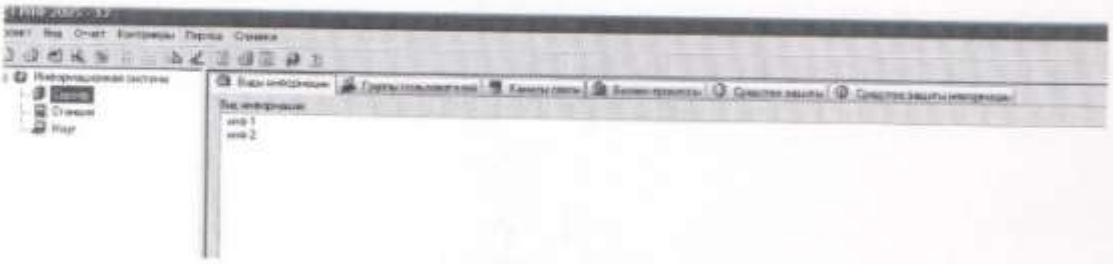

Теперь зададим пользователей



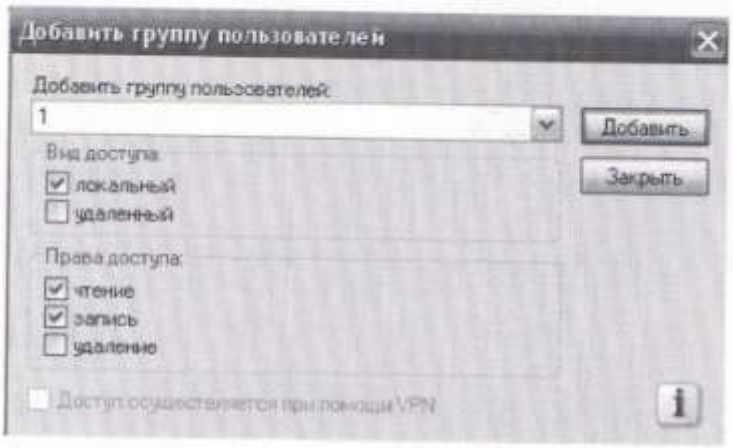

И коммерческие процессы



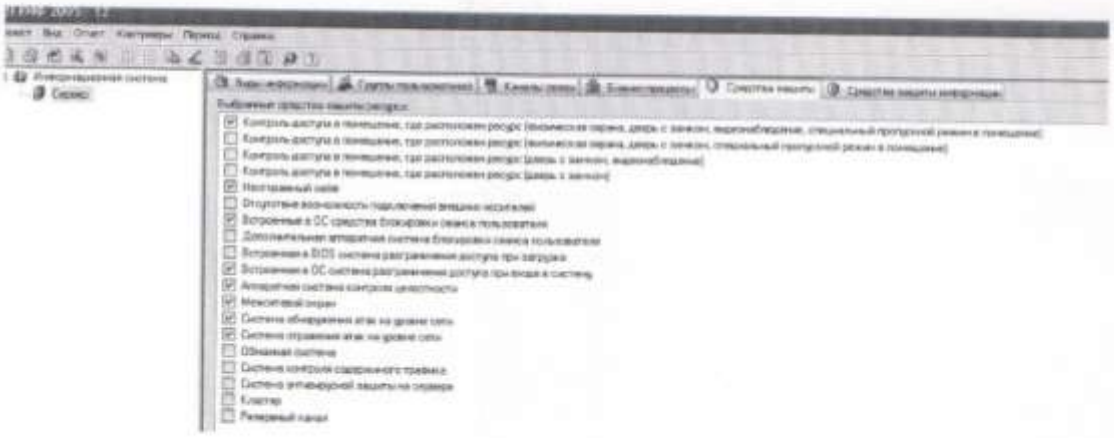
Далее перейдем в режим «связь» и настроем соединения всех выбранных нами компонентов



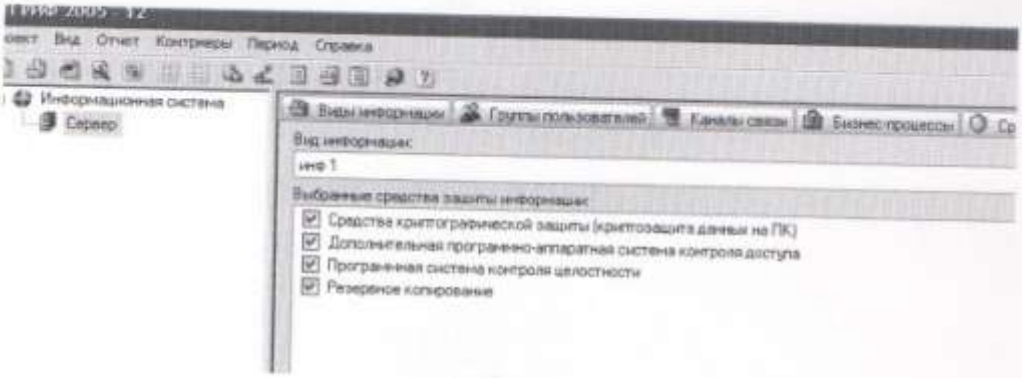
Зададим доступ пользователей к информации



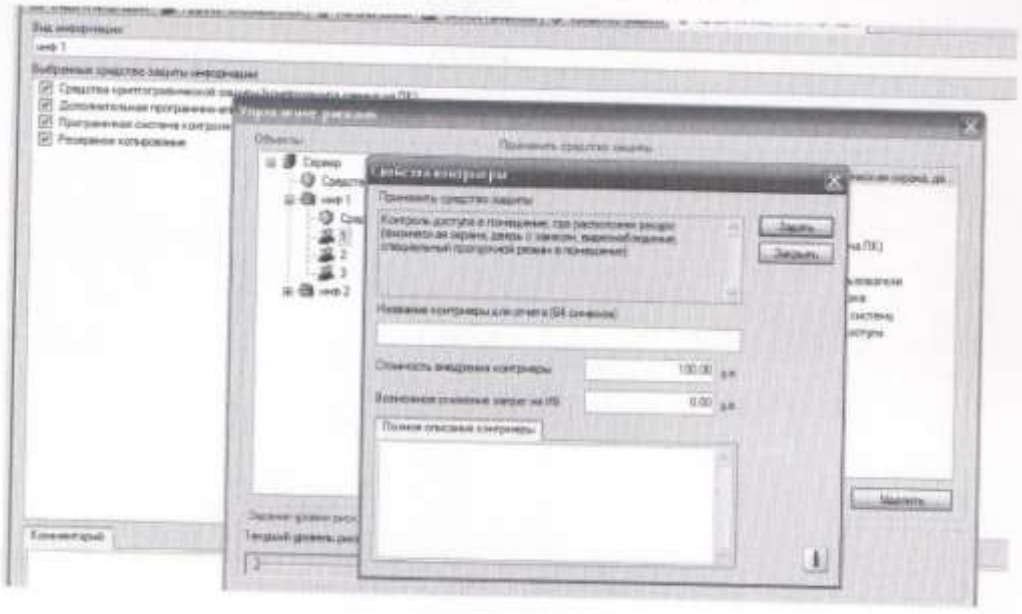

Определим средства защиты



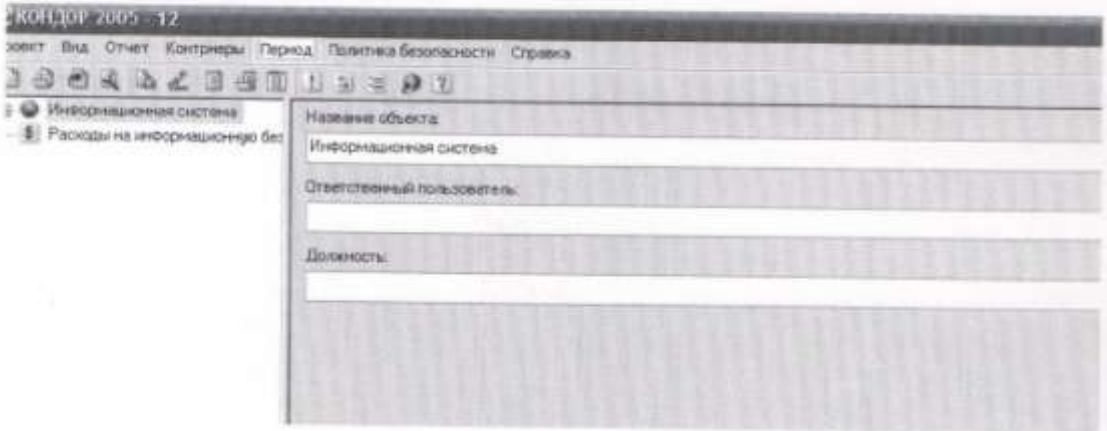
Зададим средства защиты информации для пользователей



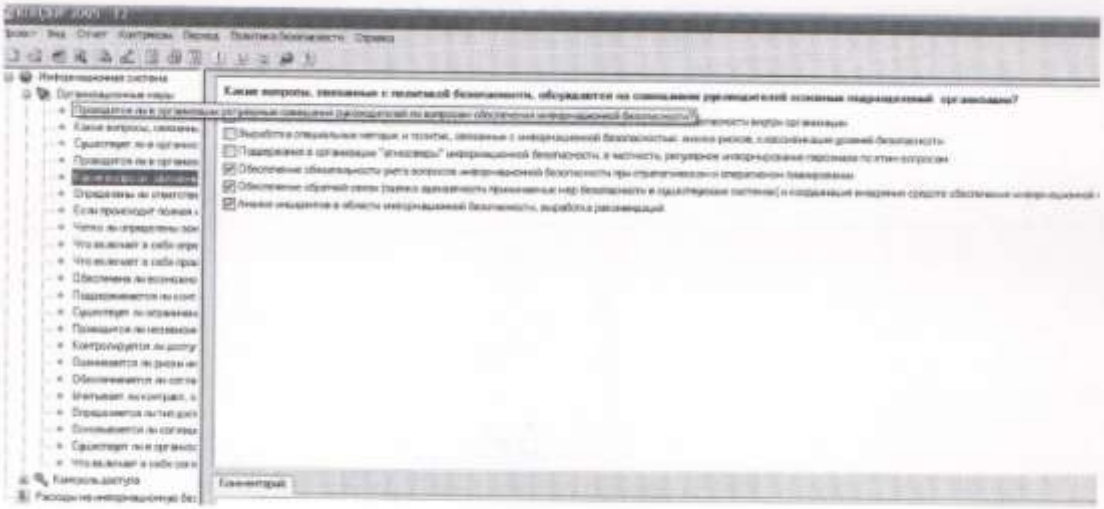

Теперь выполним контрмеры. Для этого перейдем в графу «анализ рисков» и в списке возможных контрмер выберем контрмеру и нажмем «свойства». Зададим стоимость контрмеры и посмотрим насколько изменилась эффективность контрмер благодаря заданной контрмере.



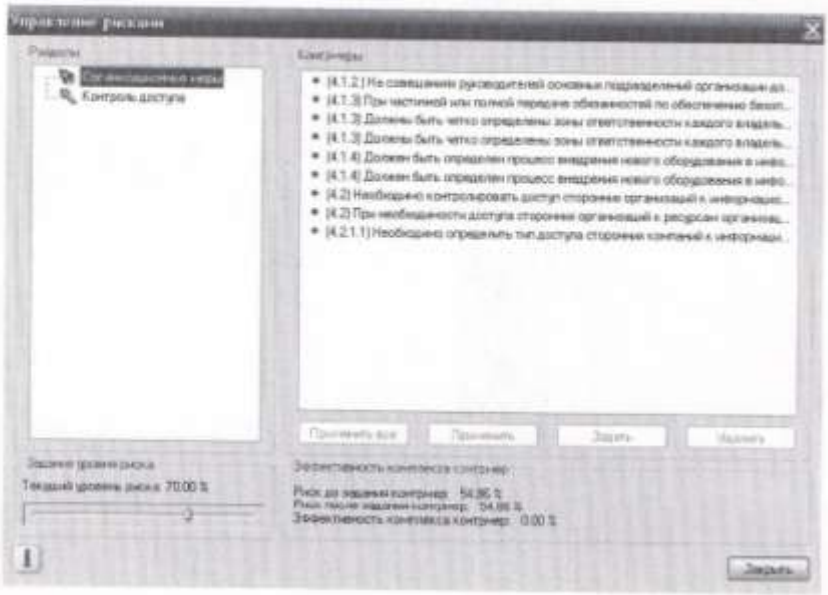
Теперь перейдем к программе кондор. В этой программе можно задать организационные меры и меры контроля доступа



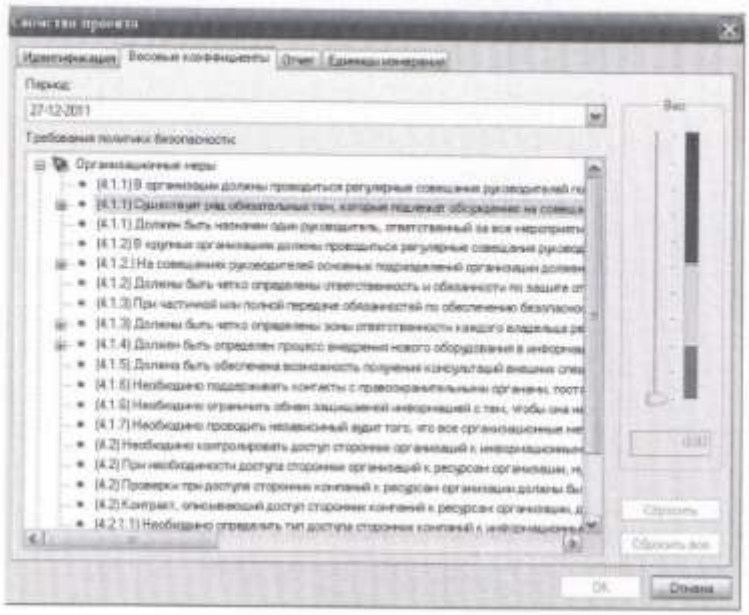

Осуществляется это при помощи системы вопросов, в результате которых определяется уровень угрозы



После анкетирования получим набор используемых в нашей системе мер, с возможностями осуществления их и финансирования (так же как в ГРИФе)




Также программа имеет гибкую возможность настройки – каждой мере можно задать весовой коэффициент.



## ЗАДАНИЕ:

Провести анализ рисков и проверку политики информационной безопасности с помощью программного комплекса Office 2005 Demo(ГРИФ, КОНДОР). В ходе выполнения лабораторной работы разработать политику информационной безопасности и анализировать риски предприятия.

Варианты: (указывается количество вводимых данных, сами данные пользователь выбирает сам), ресурсов 3, отдел 1

| Вариант | Вид информации | Группы пользователей | Каналы связи | Бизнес-процессы | Средства защиты | Средства защиты информации |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 1 | 2 | 7-8 | 3-4 |
| 2 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 3 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 4 | 2 | 3 | 1 | 2 | 7-8 | 3-4 |
| 5 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 6 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 7 | 2 | 3 | 1 | 2 | 7-8 | 3-4 |
| 8 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 9 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 10 | 2 | 3 | 1 | 2 | 7-8 | 3-4 |
| 11 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 12 | 4 | 2 | 1 | 2 | 7-8 | 3-4 |
| 13 | 2 | 2 | 1 | 2 | 7-8 | 3-4 |
| 14 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 15 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 16 | 2 | 2 | 1 | 2 | 7-8 | 3-4 |
| 17 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 18 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 19 | 2 | 2 | 1 | 2 | 7-8 | 3-4 |
| 20 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |

| Вариант | Вид информации | Группы пользователей | Каналы связи | Бизнес-процессы | Средства защиты | Средства защиты информации |
|---|---|---|---|---|---|---|
| 21 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 22 | 2 | 2 | 1 | 2 | 7-8 | 3-4 |
| 23 | 3 | 2 | 1 | 2 | 7-8 | 3-4 |
| 24 | 4 | 3 | 1 | 2 | 7-8 | 3-4 |
| 25 | 2 | 2 | 1 | 2 | 7-8 | 3-4 |

По результатам выполнения составить отчет ГРИФ, потом открыть данный проект в программе КОНДОР и составить отчет по организационным мерам и политике доступа.

## КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое политика информационной безопасности?
2. Какие организационные меры защиты существуют?
3. Назначение организационных мер?
4. Какие из них наиболее эффективны? Почему?
5. Перечислите основные нормативные документы, регламентирующие ИБ в России
6. Какой состав и организационная структура системы обеспечения информационной безопасности?
7. В чем заключается стандарт ISO 17799?
8. Опишите методику анализа рисков.

# СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ


1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоиздат, 1994. Кн. 1-2.
2. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. - Москва, 1992.
3. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.
4. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.
5. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. - Москва, 1992.
6. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Москва, 1992.
7. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М., Яхтсмен, 1996.
8. И.Н. Анисимова, Е.В. Стельмашонок. Защита информации.: Учебное пособие - СПб, СпбГИЭУ, 2002.

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационной безопасности


# Решение ситуационных задач (кейсов)

Методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения.

Курск 2017

УДК 004
Составители: О.А. Демченко

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» М.О. Таныгин

**Решение ситуационных задач (кейсов):** методические указания к выполнению практической работы по дисциплине «Управление информационной безопасностью» / Юго-Зап. гос. Ун-т; сост. О.А. Демченко, Курск, 2017, 7 с.: ил. 0; Библиогр.: с. 7.

Содержат сведения по вопросам создания политики информационной безопасности. Указывается порядок выполнения практической работы, правила оформления, содержание отчета.

Методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. 0,41. Уч. –изд.л. 0,37. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

# СОДЕРЖАНИЕ

## ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является Решение ситуационных задач (кейсов).

## ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Сделать вывод

## СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист;
2. Цель работы;
3. Перечень документов для создания и оформления информационных систем;
4. ТЗ на создание информационной системы и системы защиты информации.
5. Модель угроз и модель нарушителя;
6. Смета на технические средства обработки информации, закупку лицензионного ПО, средств защиты информации, коммутационное оборудование (СКС, установку и монтаж не включать);
7. Доклад;
8. Выводы по проделанной работе.

# ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Организационные методы защиты информации, как правило, используются для парирования угроз. Кроме того, организационные методы используются в любой системе защиты без исключений.

Угроза безопасности - это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.

Уязвимость - это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.

Атака - это действие по использованию уязвимости; реализация угрозы.

Угроза конфиденциальности - это угроза раскрытия информации.

Угроза целостности - это угроза изменения информации.

Угроза доступности - это угроза нарушения работоспособности системы при доступе к информации.

Ущерб - это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в информационной системе. Ущерб является характеристикой информационной системы и не зависит от степени её защищенности.

Риск - это вероятный ущерб, который зависит от защищенности системы.

## ЗАДАНИЕ:

В Курской области создается Комитет Курской области по контролю успеваемости учащихся образовательных организациях Курской области (выделяется часть функций из комитета образования и науки).

В рамках комитета создается автоматизированная система внутренней работы. Все сотрудники должны иметь автоматизированные рабочие места.

Структура комитета:

Руководитель – 1

Заместитель руководителя по внутренней работе – 1

Заместитель руководителя по контролю успеваемости – 1

Отдел кадров – 1

Бухгалтерия – 2

Отдел контроля успеваемости – 5

Отдел автоматизации деятельности – 1

Должен быть создан банк данных успеваемости, при этом имеется разработчик специального ПО, который реализует интерфейсную часть по необходимым требованиям с учетом выбранной аттестуемым СУБД. СУБД интегрируется с порталом госуслуг. Ввод данных осуществляется путем выгрузки данных из действующей системы Аверс по каналу связи.

Руководитель и заместители должны иметь доступ ко всей информации и Интернет, отдел контроля – только к ИС контроля, бухгалтерия и отдел кадров – только к ресурсу кадров и бухгалтерии, а так же к АС бюджетная система и закупки.

Деятельность бухгалтерии – стандартная, база данных 1С совмещена с отделом кадров.

Комитет занимает 8 помещений на 1 этаже (схема составляется самостоятельно), возможен прием посетителей.

Примерный бюджет на всю информатизацию и защиту информации 2,5 млн. руб.

Разрешаются любые уточняющие вопросы по электронной почте, при этом отметки о ходе работы и отметки о переписке должна быть внесена в ЖИРУ.

## КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Где необходима электронная подпись документов?
2. Какие могут быть альтернативные наборы вариантов решения?
3. Как определялась схема рассадки людей?
4. Какой перечень документов по которым готовился?

## СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

1. Справочно-поисковая система «Консультант Плюс».
2. Справочно-поисковая система «Гарант».

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационной безопасности


# Основные методы управления информационной безопасностью в ГИС

Методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения.

Курск 2017

УДК 004
Составители: О.А. Демченко

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» М.О. Таныгин

**Основные методы управления информационной безопасностью в ГИС**: методические указания к выполнению практической работы по дисциплине «Управление информационной безопасностью» / Юго-Зап. гос. Ун-т; сост. О.А. Демченко, Курск, 2017, 20 с.: ил. 12; Библиогр.: с. 20.

Содержат сведения по вопросам создания политики информационной безопасности. Указывается порядок выполнения практических работ, правила оформления, содержание отчета.

Методические указания по выполнению практической работы по дисциплине «Управление информационной безопасности» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/17.
Усл. печ. л. 1,16. Уч. –изд.л. 1,05. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

## ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является оценка показателей качества функционирования комплексной системы защиты информации на предприятии, расчет защищенности от физического проникновения и от несанкционированного доступа в локальную сеть.

## ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Сделать вывод

## СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Цель работы
3. Краткая теория по лабораторной работе
4. Задание
5. Ход выполнения работы
6. Выводы по работе

# ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

## Перечень информации, циркулирующей на предприятии

| *Перечень информации* | *Возможные потери, руб* |
|---|---|
| Плановая документация | 100000 |
| Информационно-справочная и справочно-аналитическая документация | 150000 |
| Отчетная документация | 80000 |
| Документация по обеспечению кадрами | 50000 |
| Финансовая документация | 1000000 |
| Материально-техническое снабжение | 50000 |
| Договорная документация | 200000 |

## Параметры локальной сети и список сотрудников

*Параметры локальной сети:*

Количество компьютеров – 7;

Сеть на витой паре Ethernet 100Мбит;

*Персонал состоит из постоянного и переменного состава*

1) Постоянный:

- генеральный директор;
- зам. директора;
- юрист;
- секретарь;
- администратор сети и безопасности;
- сотрудники – 3 человека;
- программист;
- охранники – 3 человека;
- уборщицы – 2 человека.

2) Переменный состав:

- группа поиска – 3 человека;
- бухгалтер;
- электрик-телефонист;
- заказчики.

**Перечень угроз с учетом возможных потерь**

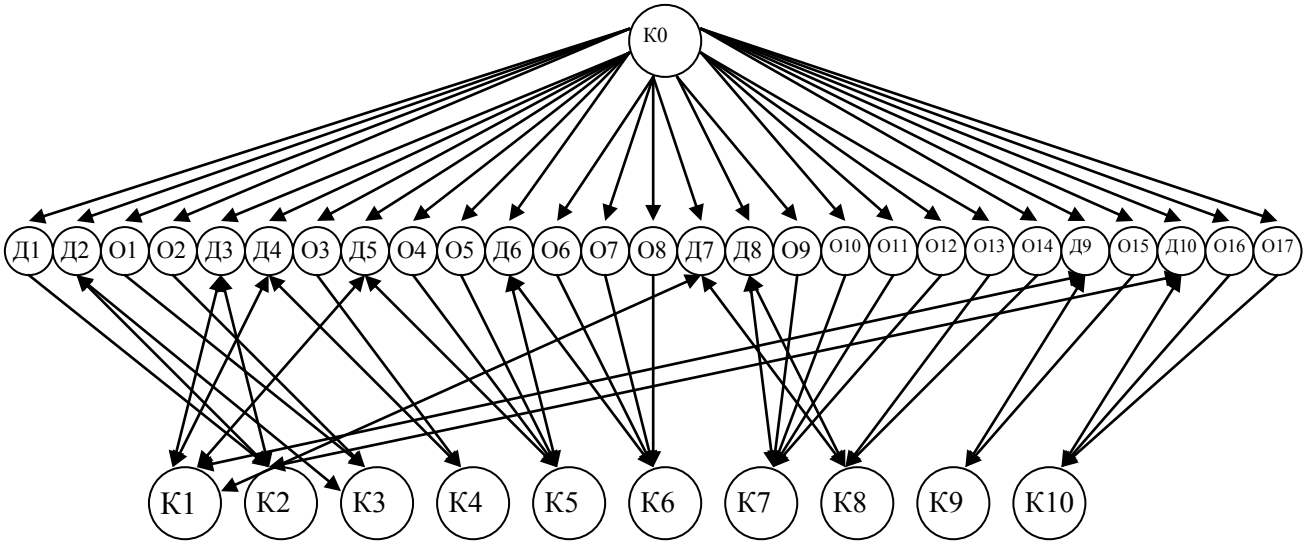
| | *Угроза* | *Объект угрозы* | *Опас-ность угрозы в баллах от 1 до 100* | *Возможные потери* |
|---|---|---|---|---|
| 1 | Утечка за счет структурного звука в стенах и перекрытиях | Переговоры | 20 | 50 тыс. |
| 2 | Съем информации с плохо стертых дискет | Информация на дискетах | 40 | Незначите-льные |
| 3 | Программно-аппаратные закладки в ПЭВМ | Информация в локальной сети | 50 | 90 тыс. |
| 4 | Радио-закладки в стенах и мебели | Секретные переговоры | 70 | 90 тыс. |
| 5 | Съем информации по системе вентиляции | Разговоры | 40 | Незначите-льные |
| 6 | Лазерный съем акустической информации с окон | Секретные переговоры | 70 | 90 тыс. |
| 7 | Производственные и технологические отходы | Служебная и профессиональная тайны | 20 | Незначите-льные |
| 8 | Компьютерные вирусы, логические бомбы и т.п | Информация в локальной сети | 50 | 90 тыс. |
| 9 | Съем информации за счет наводок и навязывания | Секретные переговоры, информация в локальной сети | 80 | 90 тыс |
| 10 | Дистанционный съем видеоинформации | Персонал, клиенты | 40 | 50 тыс. |
| 11 | Съем акустической информации с | Разговоры, переговоры | 70 | 50 тыс. |

| | | | | |
|---|---|---|---|---|
| | использованием диктофонов | | | |
| 12 | Хищение носителей информации | Документированная информация, информация на НЖМД | 40 | 90 тыс. |
| 13 | Высокочастотный канал утечки в бытовой технике | Переговоры | 30 | Незначительные |
| 14 | Съем информации направленным микрофоном | Переговоры, разговоры | 30 | 50 тыс. |
| 15 | Внутренний канал утечки (обслуживающий персонал, несанкционированное копирование); | Информация на НЖМД, документированная информация, переговоры | 80 | 90 тыс. |
| 16 | Утечка за счет побочного излучения терминалов | Компьютерная информация, разговоры | 40 | 90 тыс. |
| 17 | Съем информации с телефонного уха | Телефонные переговоры | 50 | Незначительные |
| 18 | Визуальный съем с дисплея и принтера | Различная информация | 20 | Незначительные |
| 19 | Утечка по линиям связи | Переговоры | 80 | 50 тыс. |
| 20 | Утечка по цепям заземления | Различная информация | 20 | Незначительные |
| 21 | Утечка по цепи электропитания | Переговоры | 40 | 50 тыс. |

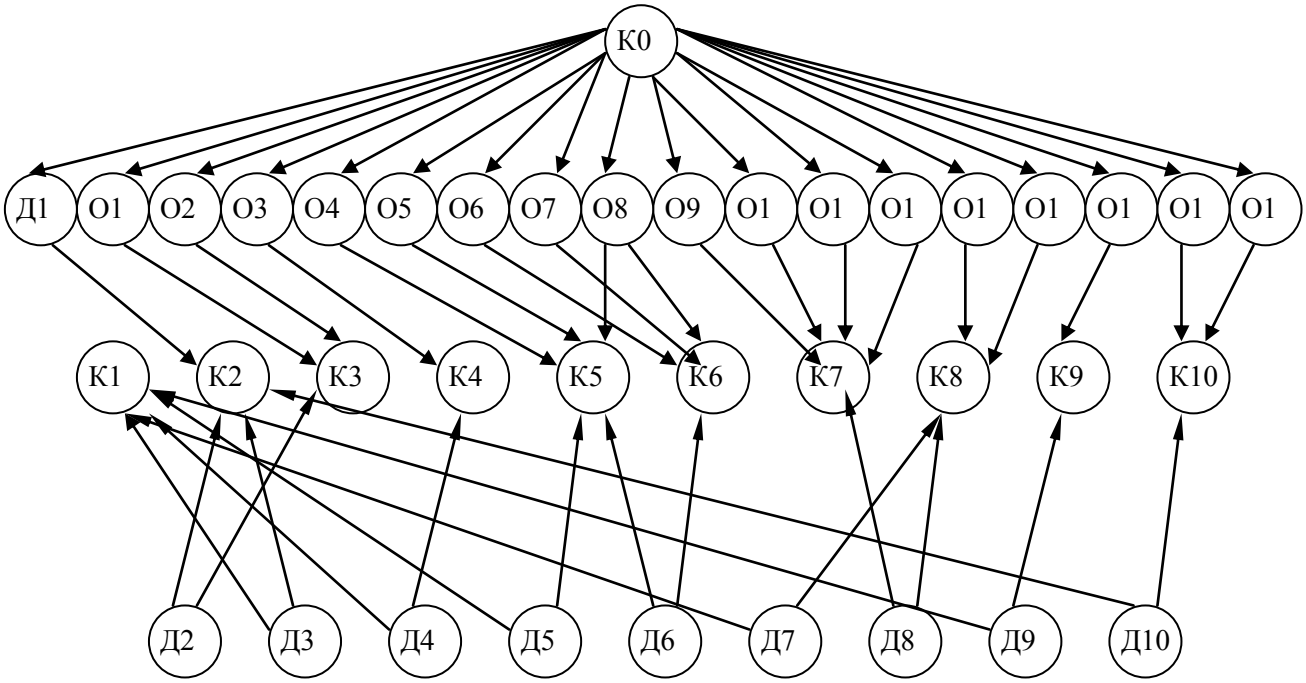
**Расчет защищенности от физического проникновения**

**Для поставленной задачи рассчитать вероятность доступа в помещения предприятия** (для построения графов можно воспользоваться программой *Deadlock*)

*Пример.* Помещение имеет 10 комнат, включая коридор (обозначим буквой «К»), 17 окон (обозначим буквой «О») и 10 дверей (обозначим буквой «Д»).Построенный для данного здания граф имеет следующий вид, при этом помещением 0 считаем внешнюю среду.



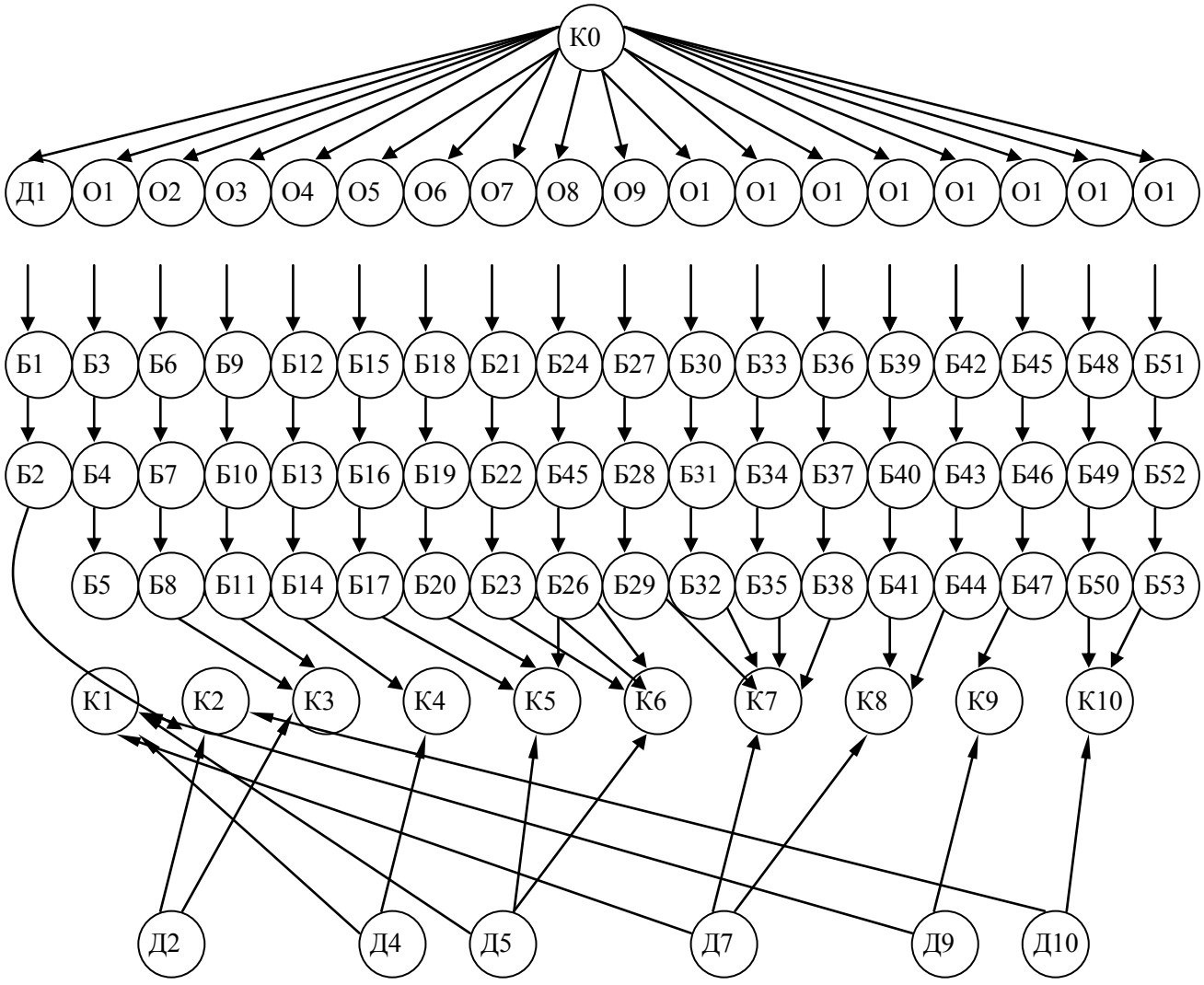

Для наглядности вынесем переходы, доступ к которым невозможен из внешней среды отдельно.



Данный граф представляет собой схему переходов между помещениями предприятия. При построении графа не учитывались возможные средства защиты от проникновения. При появлении таких средств они будут представлять собой дополнительные вершины. В нашем случае на окнах имеются следующие средства защиты:

- решетки;
- жалюзи;
- датчики разбития стекла.

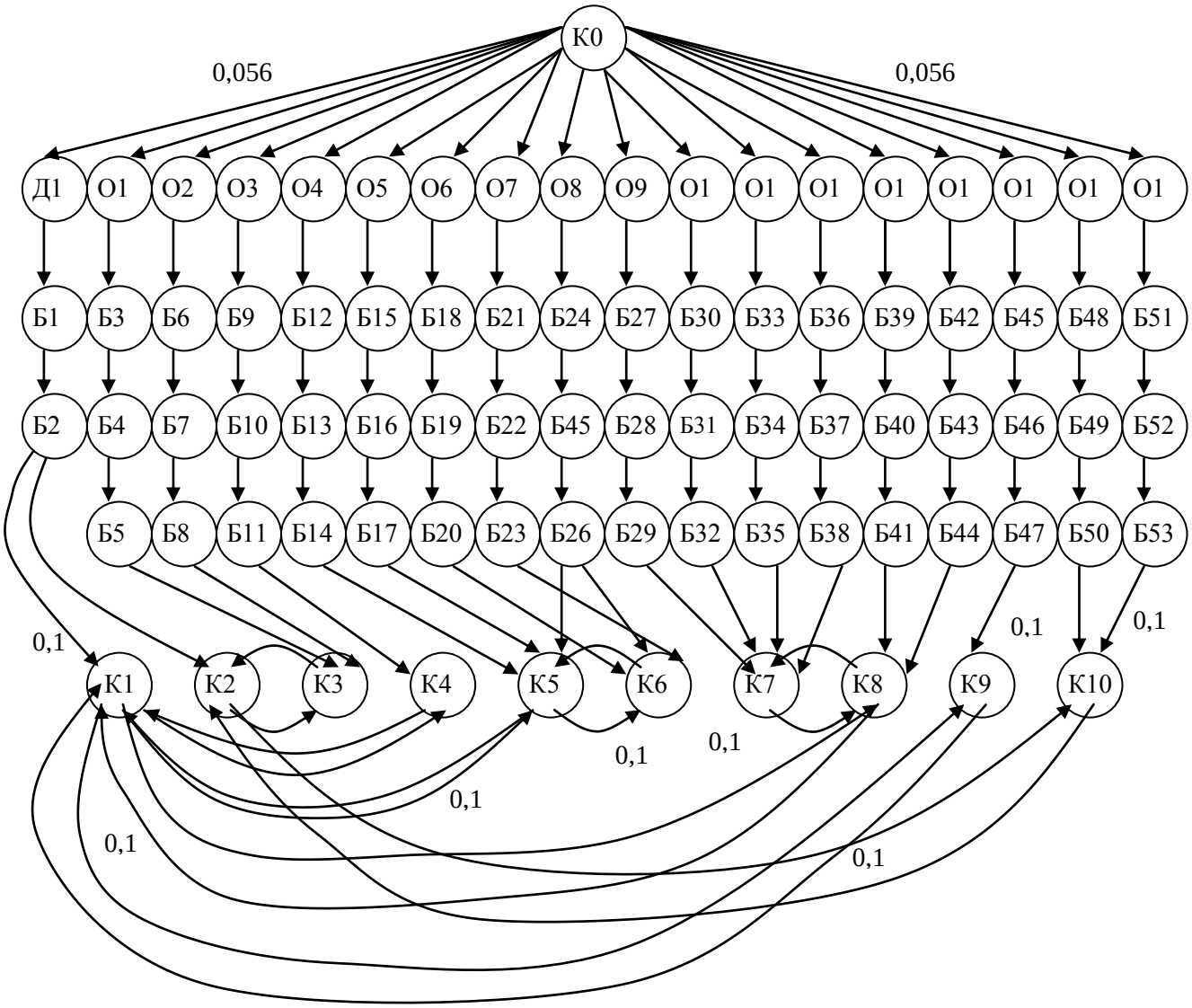
А на входной двери имеется замок и дверь бронирована.



Поэтому появляются три барьера (обозначим их буквой «Б») от Б1 до Б53. В том случае, если на двери нет замка, то соответствующую ей вершину можно удалить из графа, соединив соответствующие комнаты между собой непосредственно. Вершины, соответствующие этим двум комнатам, можно объединить в одну вершину, поскольку доступ в одну из комнат равносилен доступу в другую. Таким образом, из графа исключаются вершины Д3, Д6, Д8.

Каждой дуге ставится в соответствие ее вес – вероятность совершения данного перехода. При этом двунаправленные дуги распадаются на две. Путь проникновения нарушителя в какое-либо помещение представляет собой путь в графе. Начальной точкой пути всегда считаем вершину К0. Все переходы, начинающиеся в вершине К0, примем равновероятными, поскольку нам неизвестно, по какому пути пойдет преступник. При этом сумма всех этих вероятностей равна вероятности возникновения соответствующей угрозы, в нашем случае – физического проникновения. В нынешних условиях вероятность попытки проникновения можно принять равной 1. Таким образом, вес дуг, начинающихся в К0 равен 0.056. Для упрощения расчетов в лабораторной работе примем вероятность совершения всех остальных переходов равными 0,1.

С учетом сказанного выше граф примет следующий вид:




Каждой вершине можем приписать вероятность попадания в данную вершину. Эту вероятность можем рассчитать по формуле:

$$p_i = \sum_{j=1}^{n} v_j \cdot p_j , \qquad (1)$$

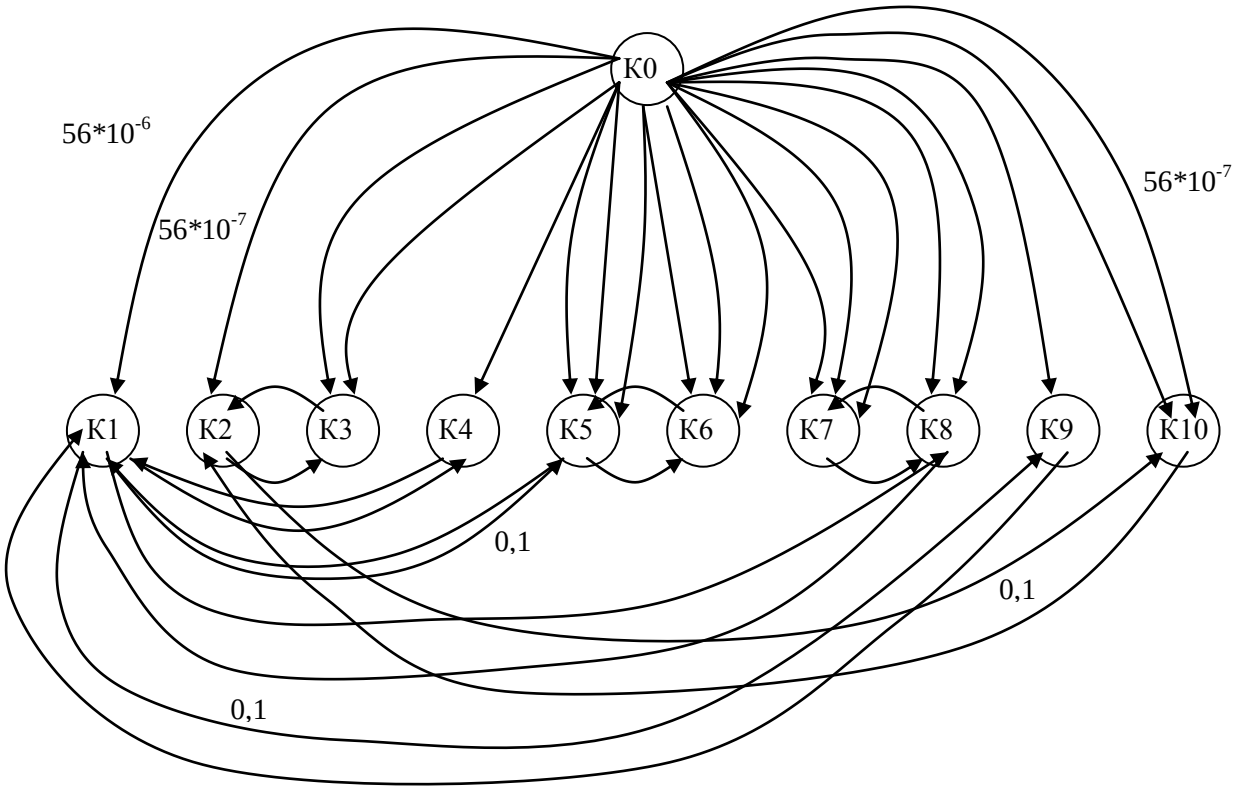
где $v_j$ – вес $j$-й дуги;

$p_j$ – вероятность нахождения преступника в соседнем состоянии (соседней вершине) $j$,

$n$ – число соседних состояний (вершин).

Если в графе присутствует вершина, переход в которую возможен только из одной вершины и из которой выходит только одна дуга, то такую вершину можно исключить, заменив ее дугой с

весом, равным произведению весов входящей и исходящей дуги. Исключив, таким образом, все такие вершины, получим новый граф.



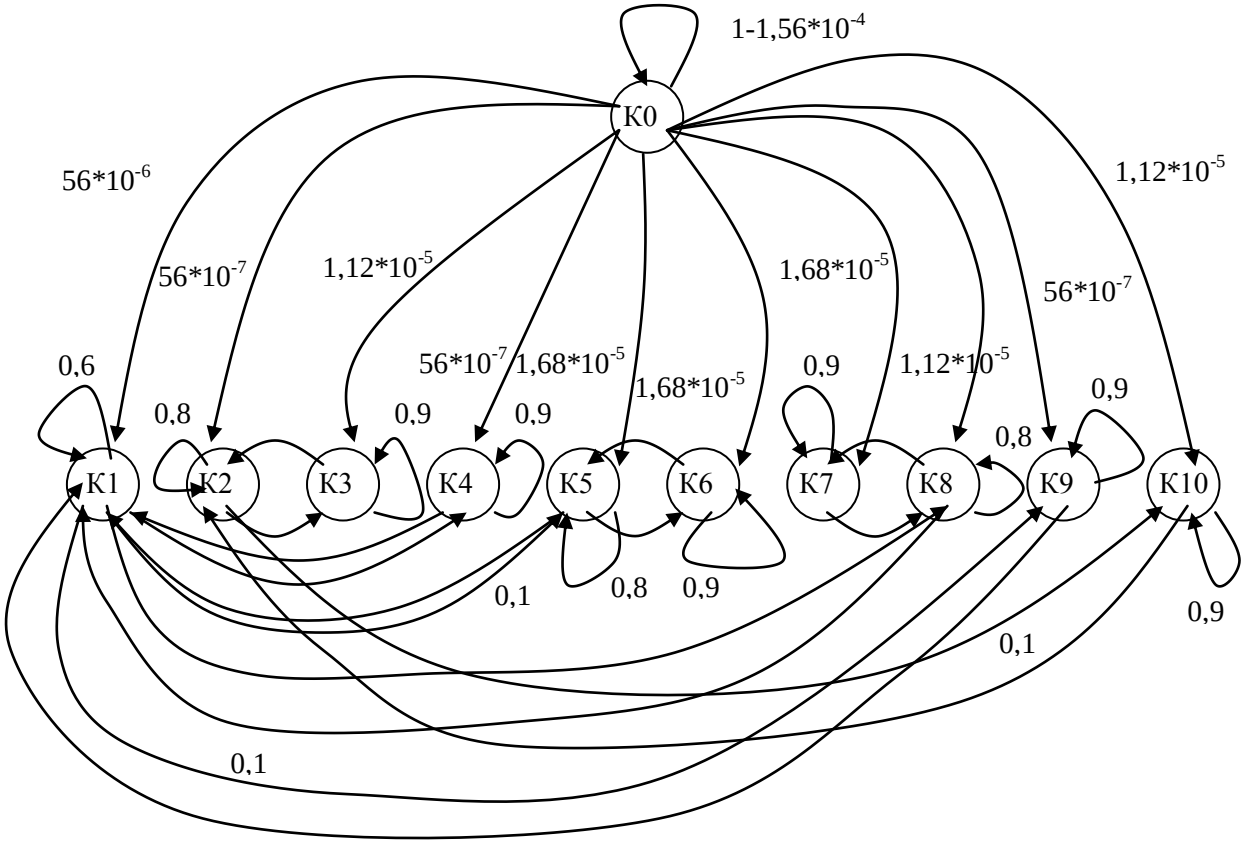

Если из одной вершины в другую ведут более одной дуги, все эти дуги можно заменить одной с весом, равным сумме весов этих дуг. Составим систему уравнений Колмогорова-Чепмена для определения вероятностей доступа в помещения. Для этого добавим в граф дуги, ведущие из каждой вершины в саму себя, с весом, равным:

$$v_i = 1 - \sum_{j=1}^{n} v_j \,, \qquad (2)$$

где $v_j$ – вес $j$-й дуги, входящей в данную вершину;

$n$ – количество дуг, входящих в вершину $i$.

В результате получим следующий граф:




Для данного графа матрица смежности будет иметь следующий вид:

| | К0 | К1 | К2 | К3 | К4 | К5 | К6 | К7 | К8 | К9 | К10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Из К0 | 0,999844 | $56*10^{-6}$ | $56*10^{-7}$ | $1,12*10^{-5}$ | $56*10^{-7}$ | $1,68*10^{-5}$ | $1,68*10^{-5}$ | $1,68*10^{-5}$ | $1,12*10^{-5}$ | $56*10^{-7}$ | $1,12*10^{-5}$ |
| Из К1 | 0 | 0,6 | 0 | 0 | 0,1 | 0,1 | 0 | 0 | 0,1 | 0,1 | 0 |
| Из К2 | 0 | 0 | 0,8 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0 | 0,1 |
| Из К3 | 0 | 0 | 0,1 | 0,9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Из К4 | 0 | 0,1 | 0 | 0 | 0,9 | 0 | 0 | 0 | 0 | 0 | 0 |
| Из К5 | 0 | 0,1 | 0 | 0 | 0 | 0,8 | 0,1 | 0 | 0 | 0 | 0 |
| Из К6 | 0 | 0 | 0 | 0 | 0 | 0,1 | 0,9 | 0 | 0 | 0 | 0 |
| Из К7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,9 | 0,1 | 0 | 0 |
| Из К8 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0,1 | 0,8 | 0 | 0 |
| Из К9 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,9 | 0 |
| Из К10 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,9 |

# Расчет вероятности доступа в помещения

$k := 0, 1 .. 126 \qquad A := (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$

$$B_k := \begin{pmatrix} 0.999844 & 0.000056 & 0.0000056 & 0.000112 & 0.0000056 & 0.0000168 & 0.0000168 & 0.0000168 & 0.000112 & 0.0000056 \\ 0 & 0.6 & 0 & 0 & 0.1 & 0.1 & 0 & 0 & 0.1 & 0.1 \\ 0 & 0 & 0.8 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.1 & 0.9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0.9 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0.8 & 0.1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.1 & 0.9 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0.1 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0.1 & 0.8 & 0 \\ 0 & 0 & 0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9 \end{pmatrix}^k$$

$$C1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C4 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C5 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

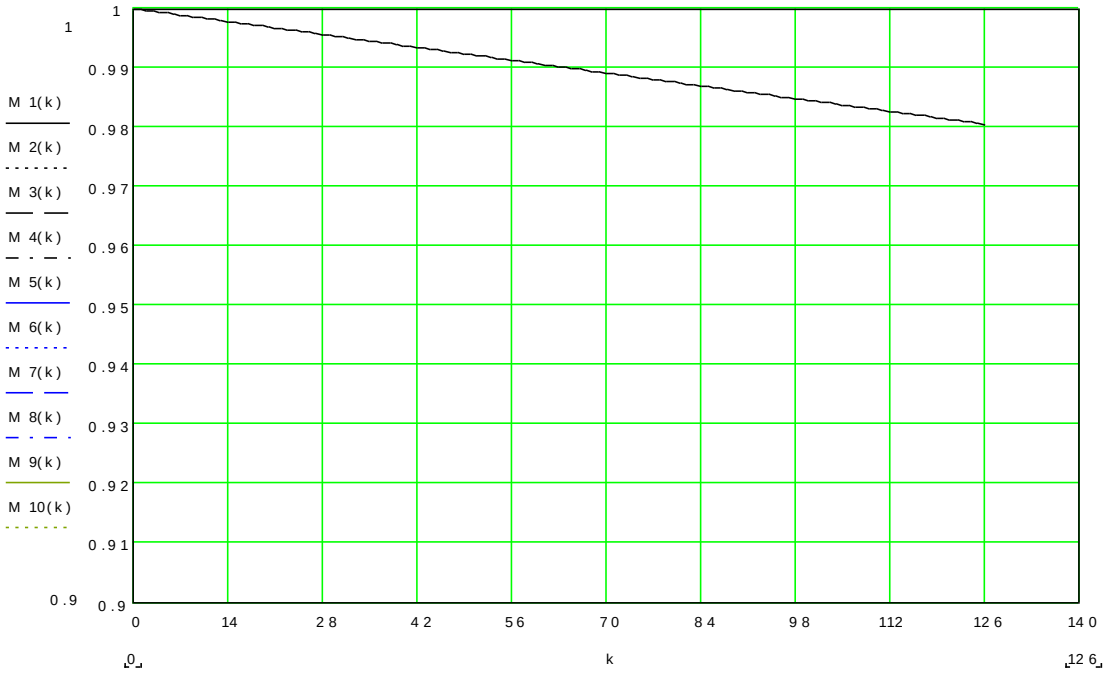
$$C6 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C7 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C8 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad C9 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad C10 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

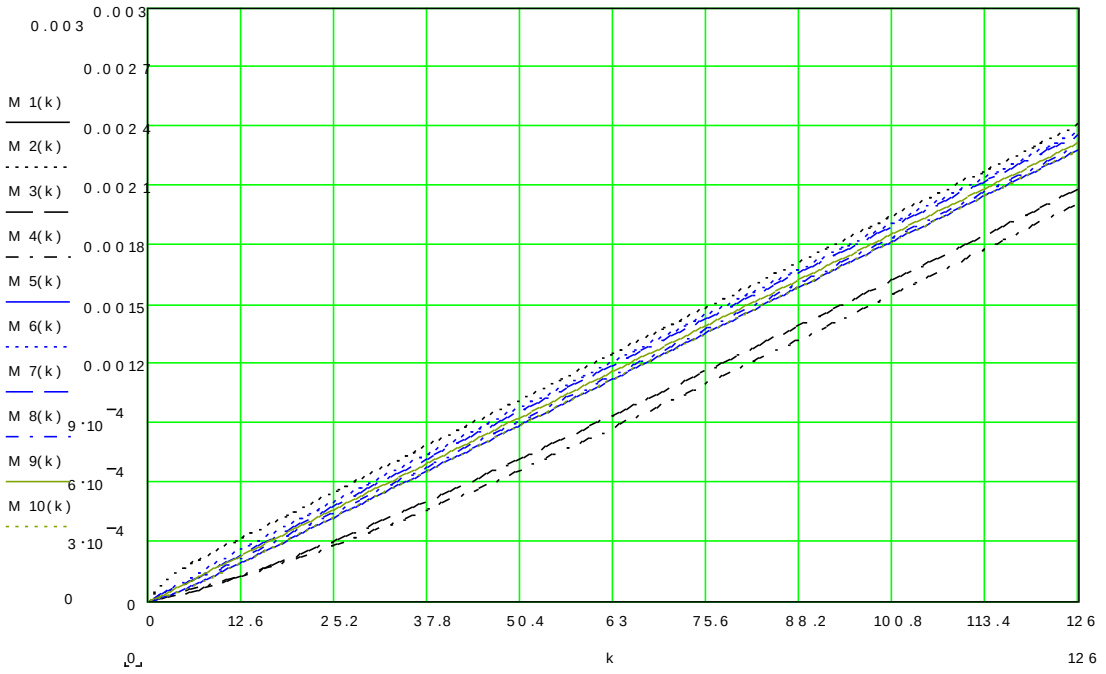
$P1_k := A \cdot B_k \cdot C1 \quad P2_k := A \cdot B_k \cdot C2 \quad P3_k := A \cdot B_k \cdot C3 \quad P4_k := A \cdot B_k \cdot C4 \quad P5_k := A \cdot B_k \cdot C5$

$P6_k := A \cdot B_k \cdot C6 \quad P7_k := A \cdot B_k \cdot C7 \quad P8_k := A \cdot B_k \cdot C8 \quad P9_k := A \cdot B_k \cdot C9 \quad P10_k := A \cdot B_k \cdot C10$

$M1(k) := (P1_k)_{0,0} \quad M2(k) := (P2_k)_{0,0} \quad M3(k) := (P3_k)_{0,0} \quad M4(k) := (P4_k)_{0,0} \quad M5(k) := (P5_k)_{0,0}$

$M6(k) := (P6_k)_{0,0} \quad M7(k) := (P7_k)_{0,0} \quad M8(k) := (P8_k)_{0,0} \quad M9(k) := (P9_k)_{0,0} \quad M10(k) := [(P10)_k]_{0,0}$

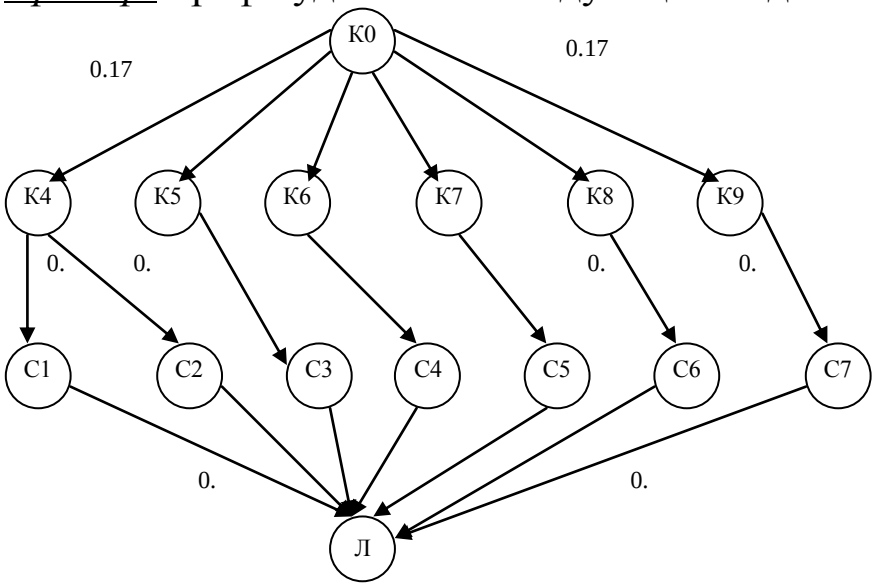

M 1(k)
M 2(k)
M 3(k)
M 4(k)
M 5(k)
M 6(k)
M 7(k)
M 8(k)
M 9(k)
M 10(k)
1
0.99
0.98
0.97
0.96
0.95
0.94
0.93
0.92
0.91
0.9
0
14
28
42
56
70
84
98
112
126
140
k
0
126


M 1(k)
M 2(k)
M 3(k)
M 4(k)
M 5(k)
M 6(k)
M 7(k)
M 8(k)
M 9(k)
M 10(k)
0.0003
0.00027
0.00024
0.00021
0.00018
0.00015
0.00012
9·10⁻⁴
6·10⁻⁴
3·10⁻⁴
0
12.6
25.2
37.8
50.4
63
75.6
88.2
100.8
113.4
126
k
0
126

**Расчет защищенности от НСД к локальной сети предприятия**

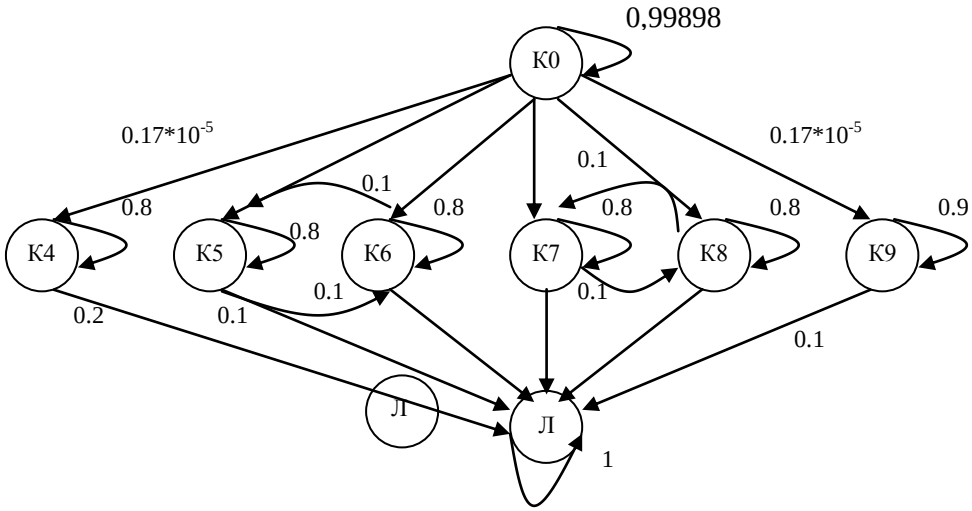
**Для поставленной задачи рассчитать защищенность от НСД ЛВС.**

*Пример.* Граф будет иметь следующий вид:




Будем считать: К0- внешняя среда, К4..К9 – комнаты, С- компьютеры, Л- локальная сеть предприятия.

Граф, преобразованный с учетом исключения вершин с одной входной и одной выходной дугой, имеет вид:



Матрица смежности будет иметь следующий вид:

| | К0 | К4 | К5 | К6 | К7 | К8 | К9 | Л |
|---|---|---|---|---|---|---|---|---|
| из К0 | 0.99898 | $0.17*10^{-5}$ | $0.17*10^{-5}$ | $0.17*10^{-5}$ | $0.17*10^{-5}$ | $0.17*10^{-5}$ | $0.17*10^{-5}$ | 0 |
| из К4 | 0 | 0.8 | 0 | 0 | 0 | 0 | 0 | 0.2 |
| из К5 | 0 | 0 | 0.8 | 0.1 | 0 | 0 | 0 | 0.1 |
| из К6 | 0 | 0 | 0.1 | 0.8 | 0 | 0 | 0 | 0.1 |
| из К7 | 0 | 0 | 0 | 0 | 0.8 | 0.1 | 0 | 0.1 |
| из К8 | 0 | 0 | 0 | 0 | 0.1 | 0.8 | 0 | 0.1 |
| из К9 | 0 | 0 | 0 | 0 | 0 | 0 | 0.9 | 0.1 |
| из Л | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

# Расчет вероятности НСД к локальной сети предприятия

$k := 0, 1 .. 126 \qquad A := (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$

$$B_k := \begin{pmatrix} 0.99898 & 0.00017 & 0.00017 & 0.00017 & 0.00017 & 0.00017 & 0.00017 & 0 \\ 0 & 0.8 & 0 & 0 & 0 & 0 & 0 & 0.2 \\ 0 & 0 & 0.8 & 0.1 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0.1 & 0.8 & 0 & 0 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.8 & 0.1 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0.1 & 0.8 & 0 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}^k$$

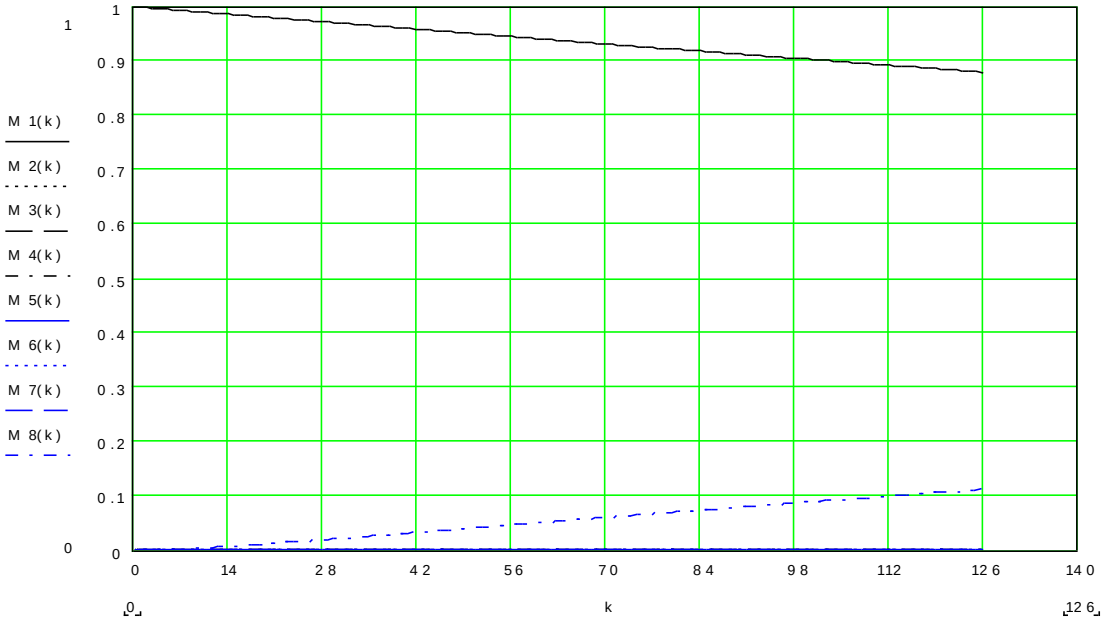
$$C1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C4 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C5 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad C6 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad C7 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad C8 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

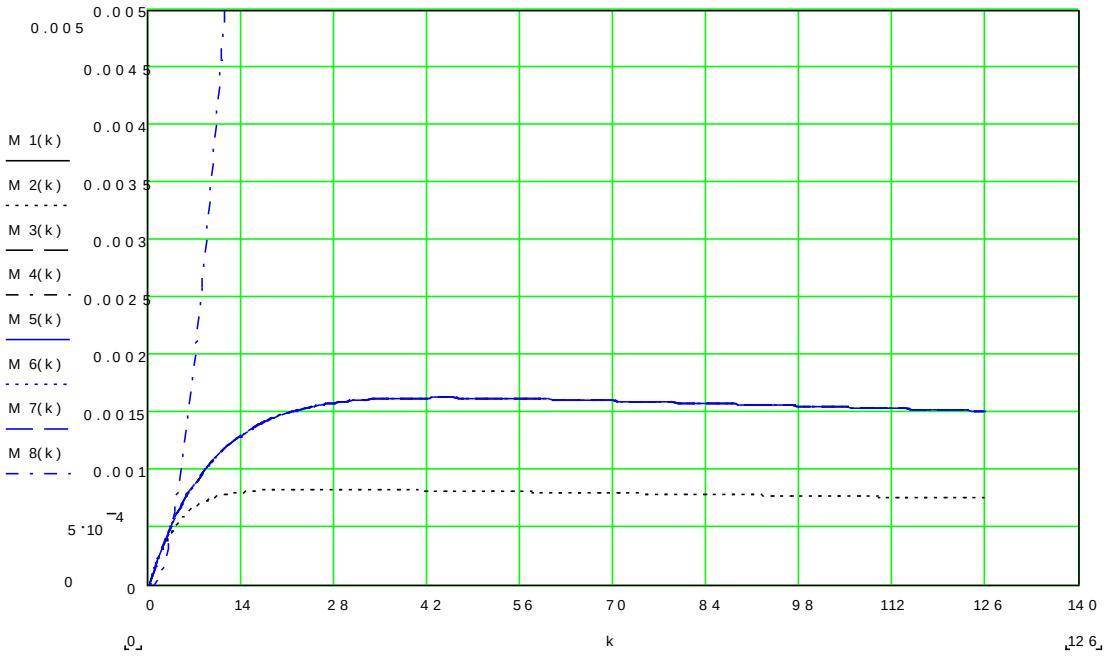
$P1_k := A \cdot B_k \cdot C1 \quad P2_k := A \cdot B_k \cdot C2 \quad P3_k := A \cdot B_k \cdot C3 \quad P4_k := A \cdot B_k \cdot C4$

$P5_k := A \cdot B_k \cdot C5 \quad P6_k := A \cdot B_k \cdot C6 \quad P7_k := A \cdot B_k \cdot C7 \quad P8_k := A \cdot B_k \cdot C8$

$M1(k) := (P1_k)_{0,0} \quad M2(k) := (P2_k)_{0,0} \quad M3(k) := (P3_k)_{0,0} \quad M4(k) := (P4_k)_{0,0}$

$M5(k) := (P5_k)_{0,0} \quad M6(k) := (P6_k)_{0,0} \quad M7(k) := (P7_k)_{0,0} \quad M8(k) := (P8_k)_{0,0}$


M 1(k)
M 2(k)
M 3(k)
M 4(k)
M 5(k)
M 6(k)
M 7(k)
M 8(k)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
14
28
42
56
70
84
98
112
126
140
0
k
126


M 1(k)
M 2(k)
M 3(k)
M 4(k)
M 5(k)
M 6(k)
M 7(k)
M 8(k)
0.005
0.0045
0.004
0.0035
0.003
0.0025
0.002
0.0015
0.001
5·10⁻⁴
0
0
14
28
42
56
70
84
98
112
126
140
0
k
126

## ЗАДАНИЕ:

**План предприятия и назначение помещений:**

1- проходная;
2- помещение охраны;
3- операторская;
4- операторская;
5- бухгалтерия;
6- кабинет директора;
7- приемная;
8- библиотека;
9- комната для переговоров.

В соответствии с описанием помещений составить собственную графическую схему.

## КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое политика информационной безопасности?
2. Какие организационные меры защиты существуют?
3. Назначение организационных мер?
4. Какие из них наиболее эффективны? Почему?
5. Перечислите основные нормативные документы, регламентирующие ИБ в России
6. Какой состав и организационная структура системы обеспечения информационной безопасности?
7. В чем заключается стандарт ISO 17799?
8. Опишите методику анализа рисков.

# СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ


1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоиздат, 1994. Кн. 1-2.
2. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. - Москва, 1992.
3. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.
4. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.
5. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. - Москва, 1992.
6. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Москва, 1992.
7. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М., Яхтсмен, 1996.
8. И.Н. Анисимова, Е.В. Стельмашонок. Защита информации.: Учебное пособие - СПб, СпбГИЭУ, 2002.