**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования**

**«Юго-Западный государственный университет»**

**Кафедра ЗИиСС**

**Практическая работа №2**

**на тему: «Система аудита информационной безопасности ГИС».**

**Ст. преподаватель к.т.н., Волокитина Е.С.**

**2014 г.**

**Цель работы**

Изучение процесса создания политики информационной безопасности, ознакомление с методикой анализа рисков и международным стандартом ISO 17799.

# Теория

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.

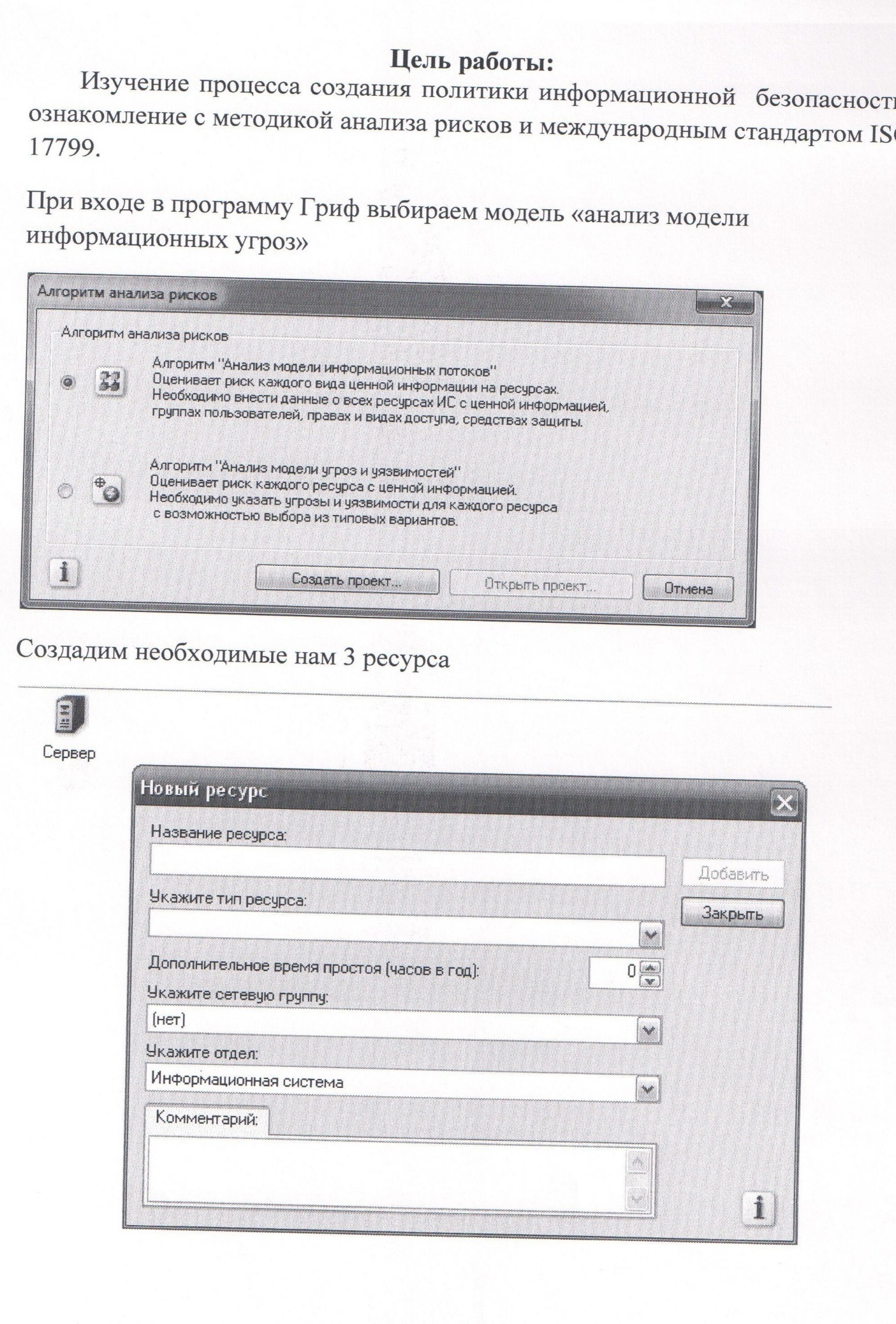
Угроза целостности - это угроза изменения информации.

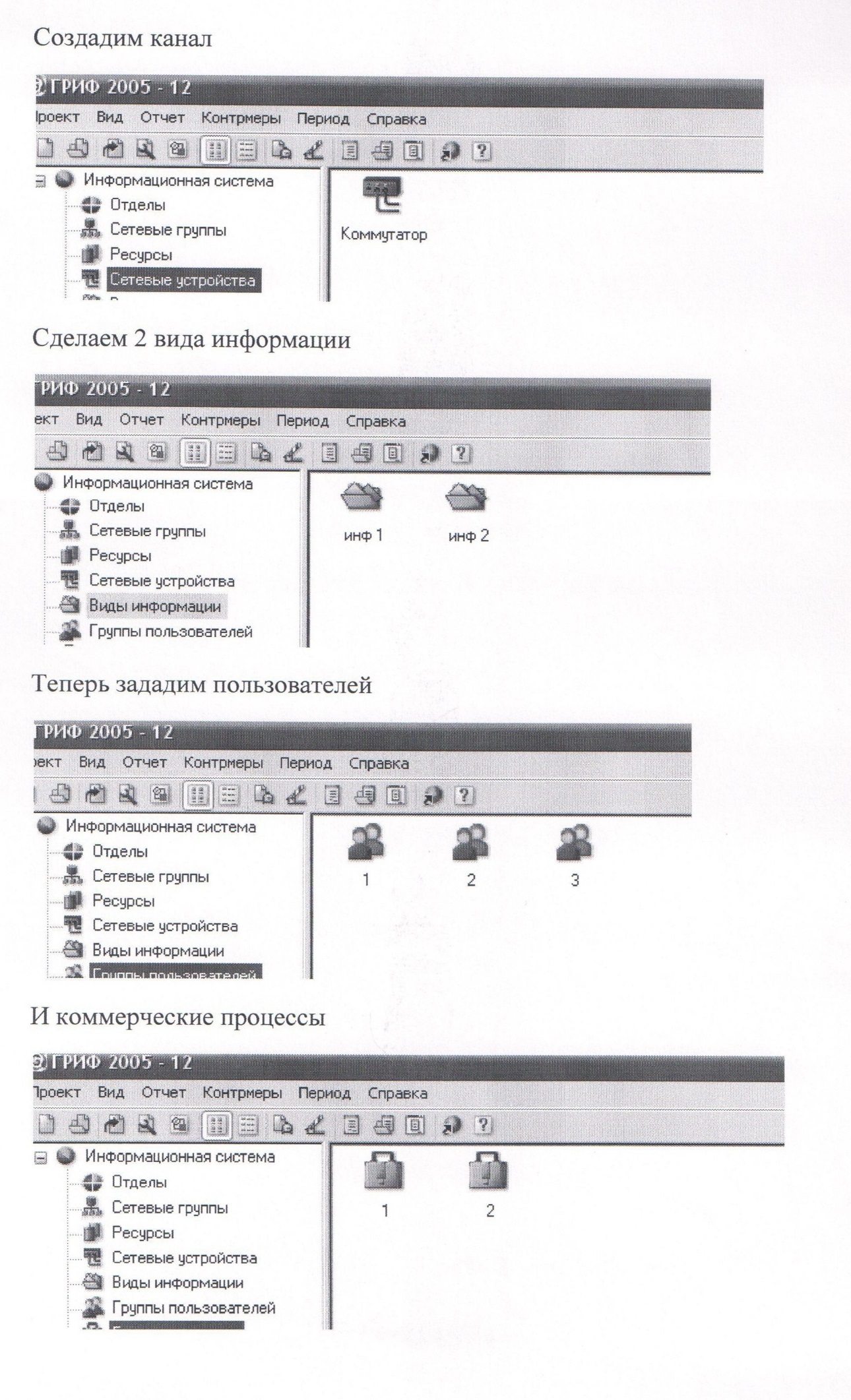
Угроза доступности - это угроза нарушения работоспособности системы при доступе к информации.

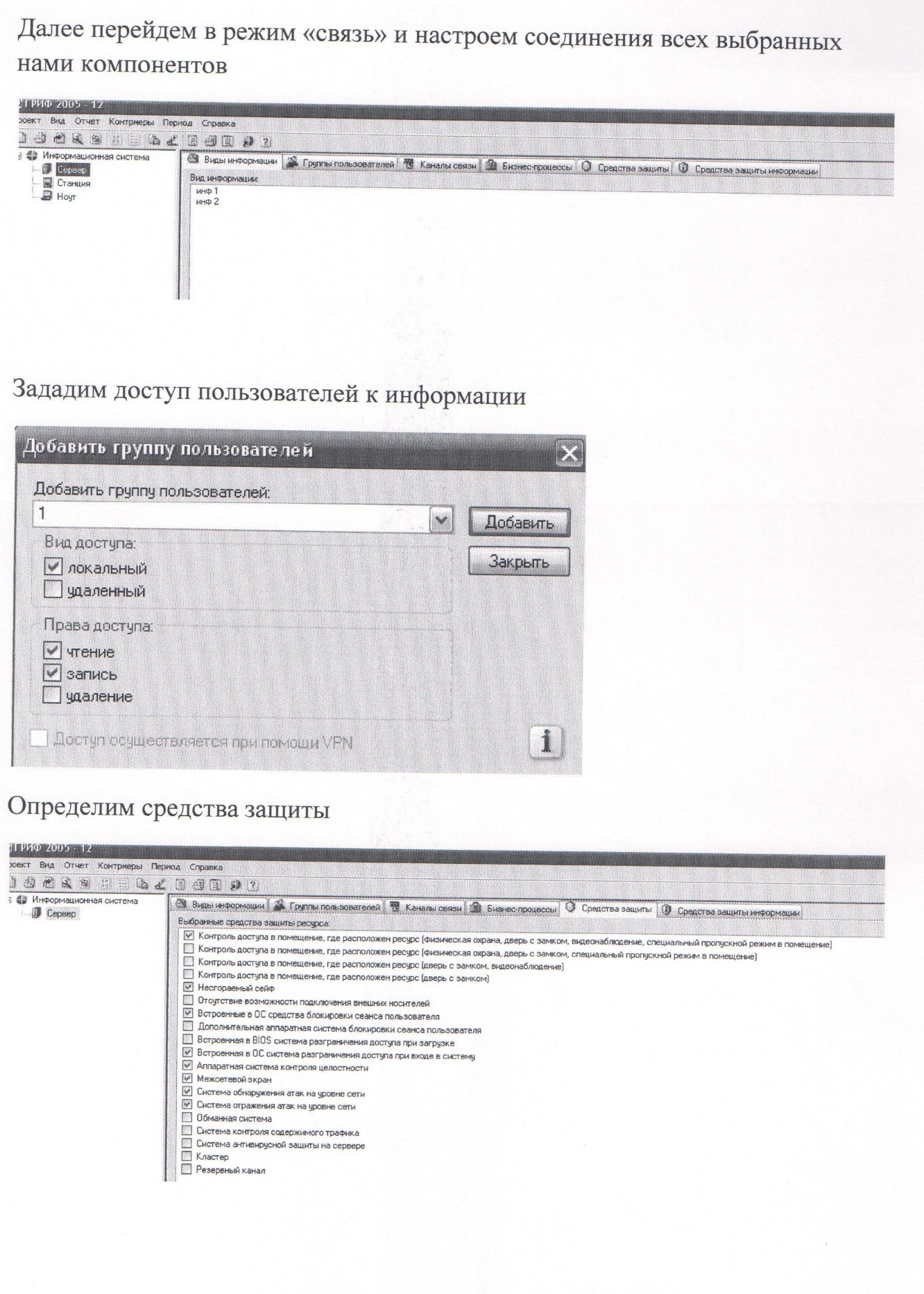
Ущерб - это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в информационной системе. Ущерб является характеристикой информационной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

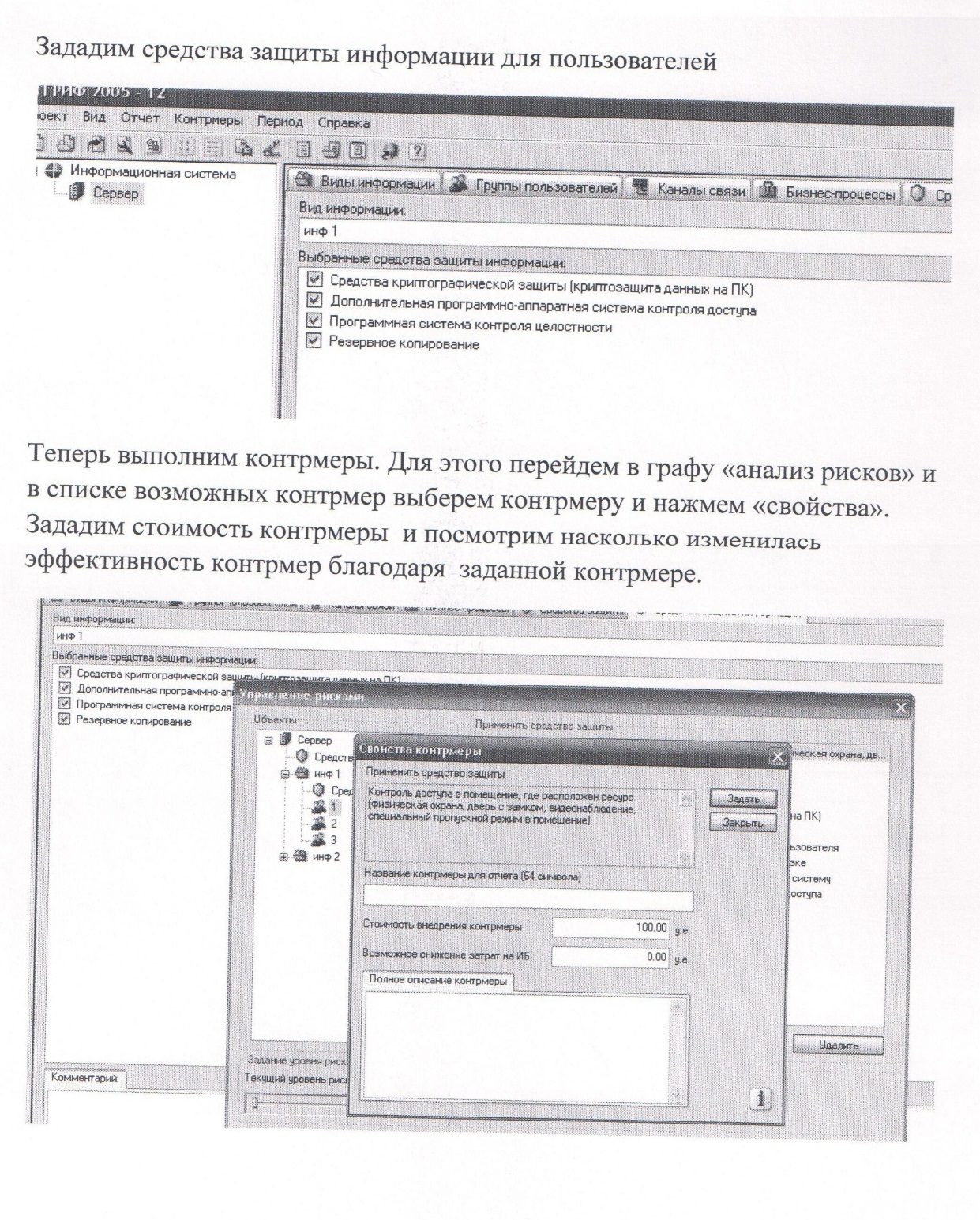
Риск - это вероятный ущерб, который зависит от защищенности системы.

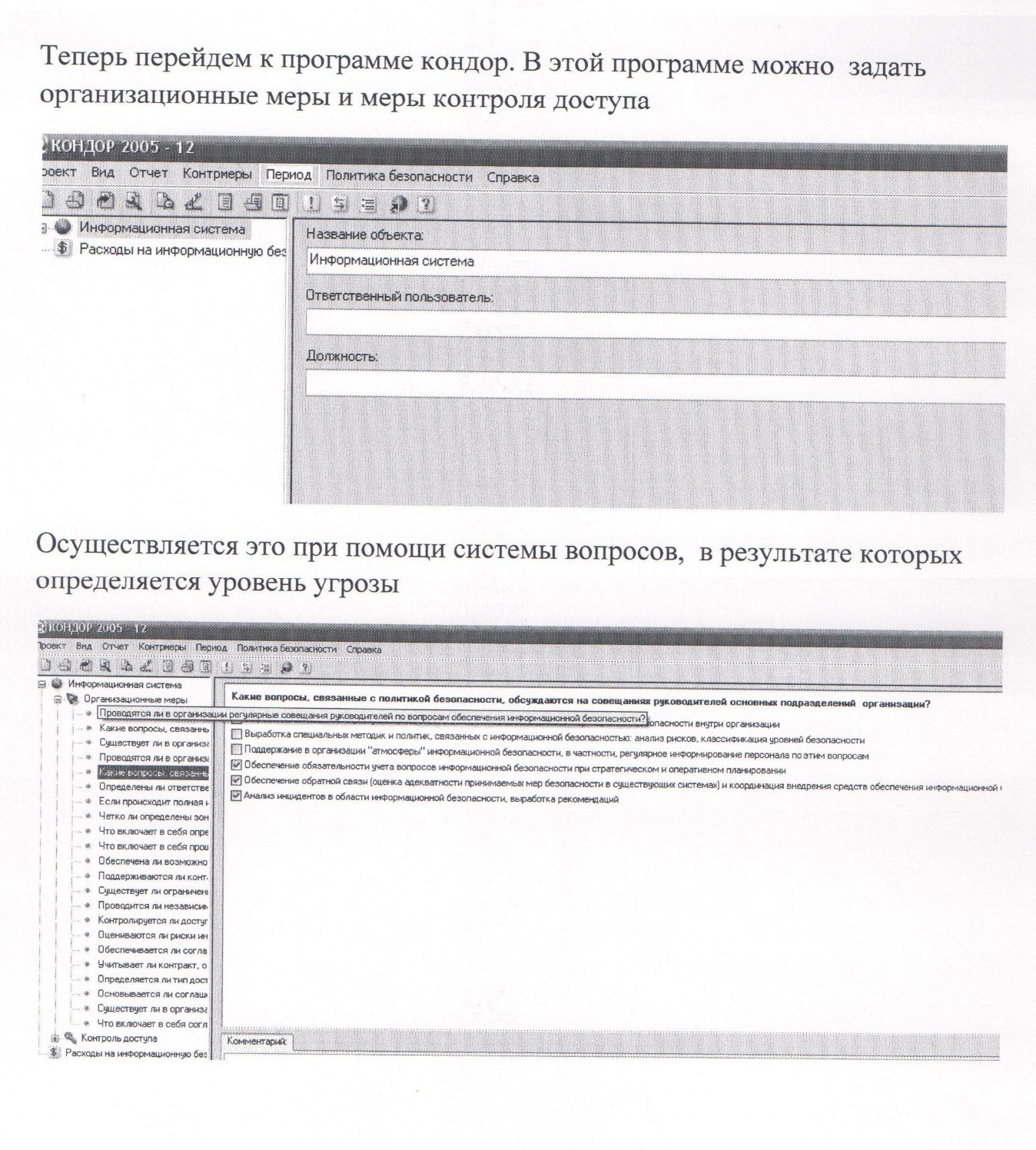
# Ход выполнения работы:

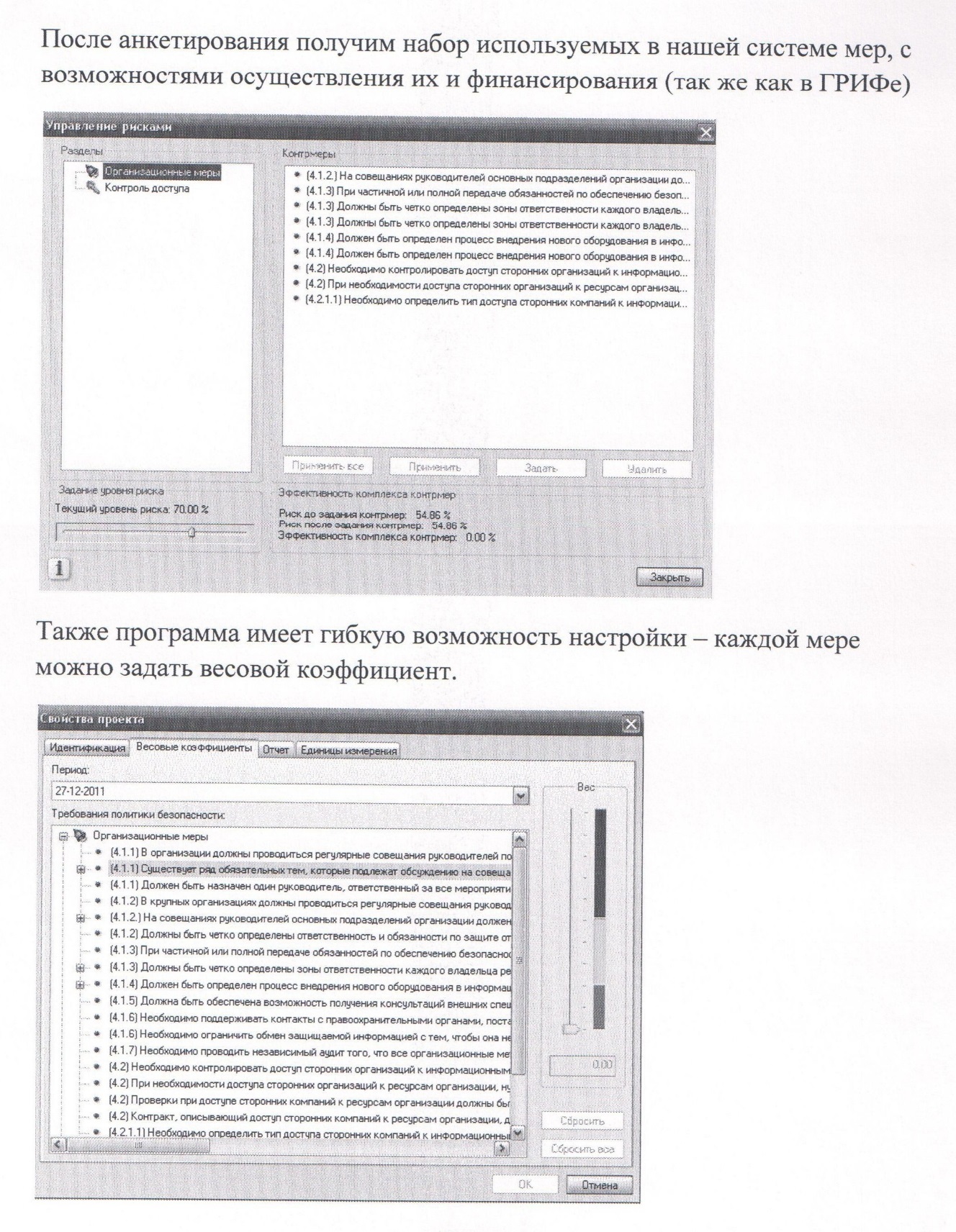












# Задание для лабораторной работы

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 |
| 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.

# Состав отчета по лабораторной работе

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

# Примерный перечень вопросов

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.

# Литература

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.