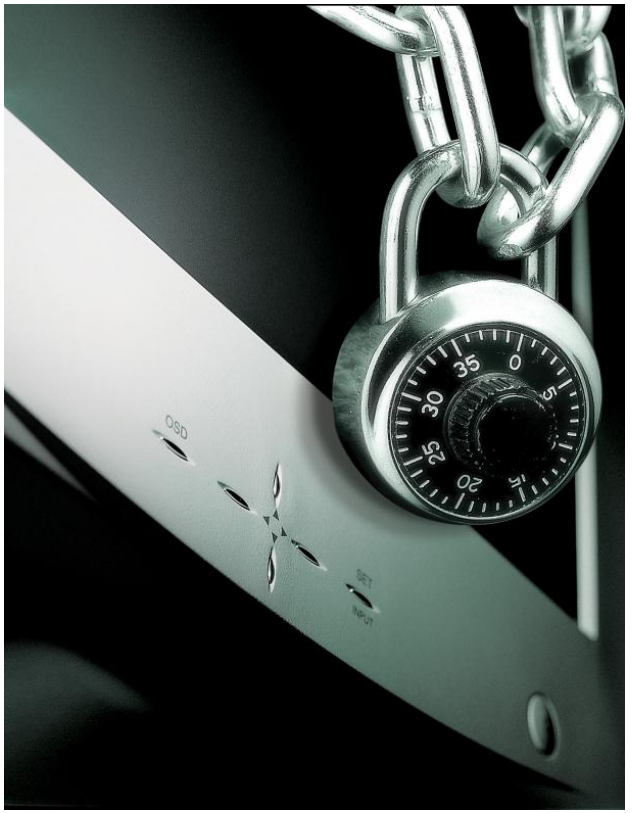
Научно-практическая конференция "Бизнес-образование как инструмент устойчивого развития экономики"

Управление рисками в IT безопасности

Подготовил: Суфианов Андрей

IT безопасность - состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.



А зачем оно надо?

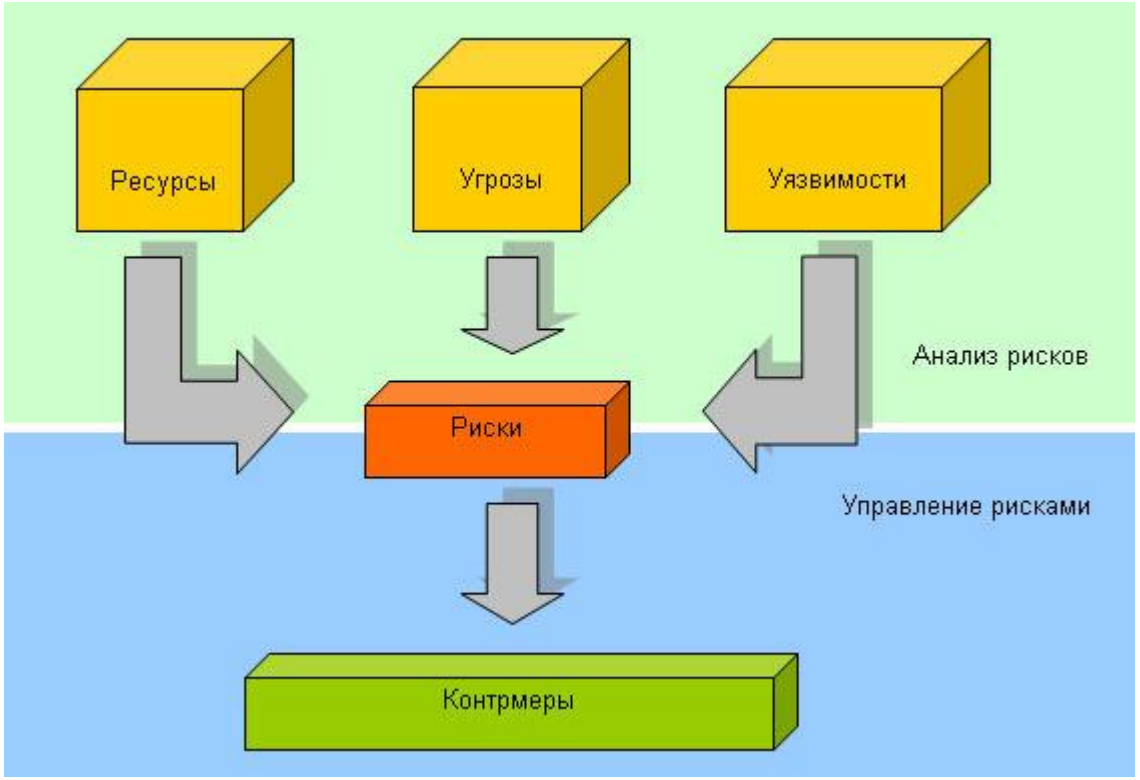
- Кража интеллектуальной собственности
- Информационные атаки
- Месть сотрудников
- Соответствие стандартам ISO

Управление информационными рисками - это

системный процесс идентификации, контроля и уменьшения информационных рисков компании в соответствии с нормативно-правовой базой в области защиты информации и собственной корпоративной политикой безопасности.

Тематические понятия

- Угроза
- Уязвимость ИС
- Риск

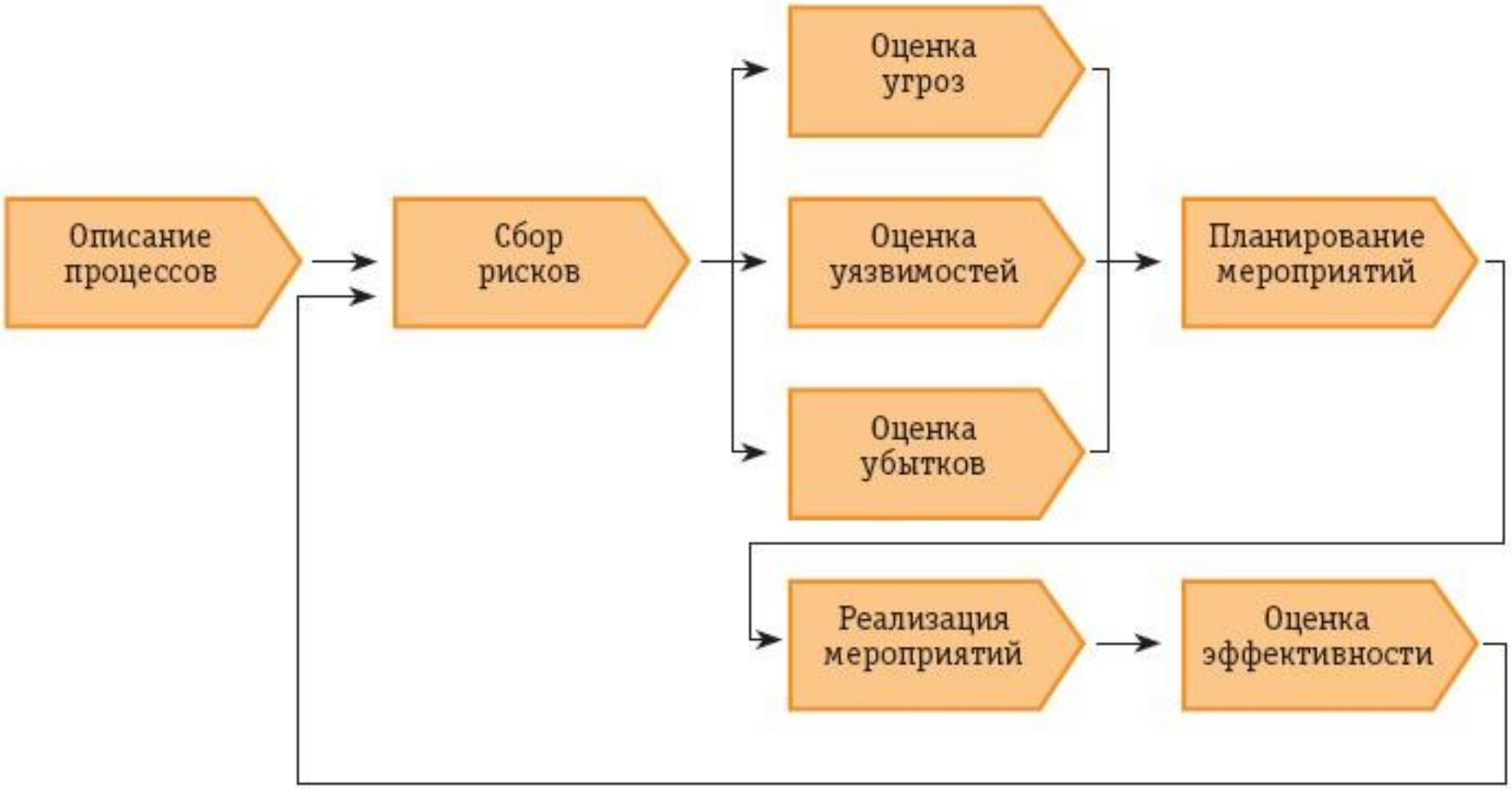


Для проектирования системы IT-безопасности в первую очередь необходимо:

- Обобщенно описать процессы деятельности
- Выделить риски
- Определить порог риска

Цель:

Минимизация внешних и внутренних угроз при учете ограничений на ресурсы и время


Описание процессов
Сбор рисков
Оценка угроз
Оценка уязвимостей
Оценка убытков
Планирование мероприятий
Реализация мероприятий
Оценка эффективности

Качественные методики

- методики, разработанные на основе ISO 17799 (международный стандарт в области ИБ, с 1993г)

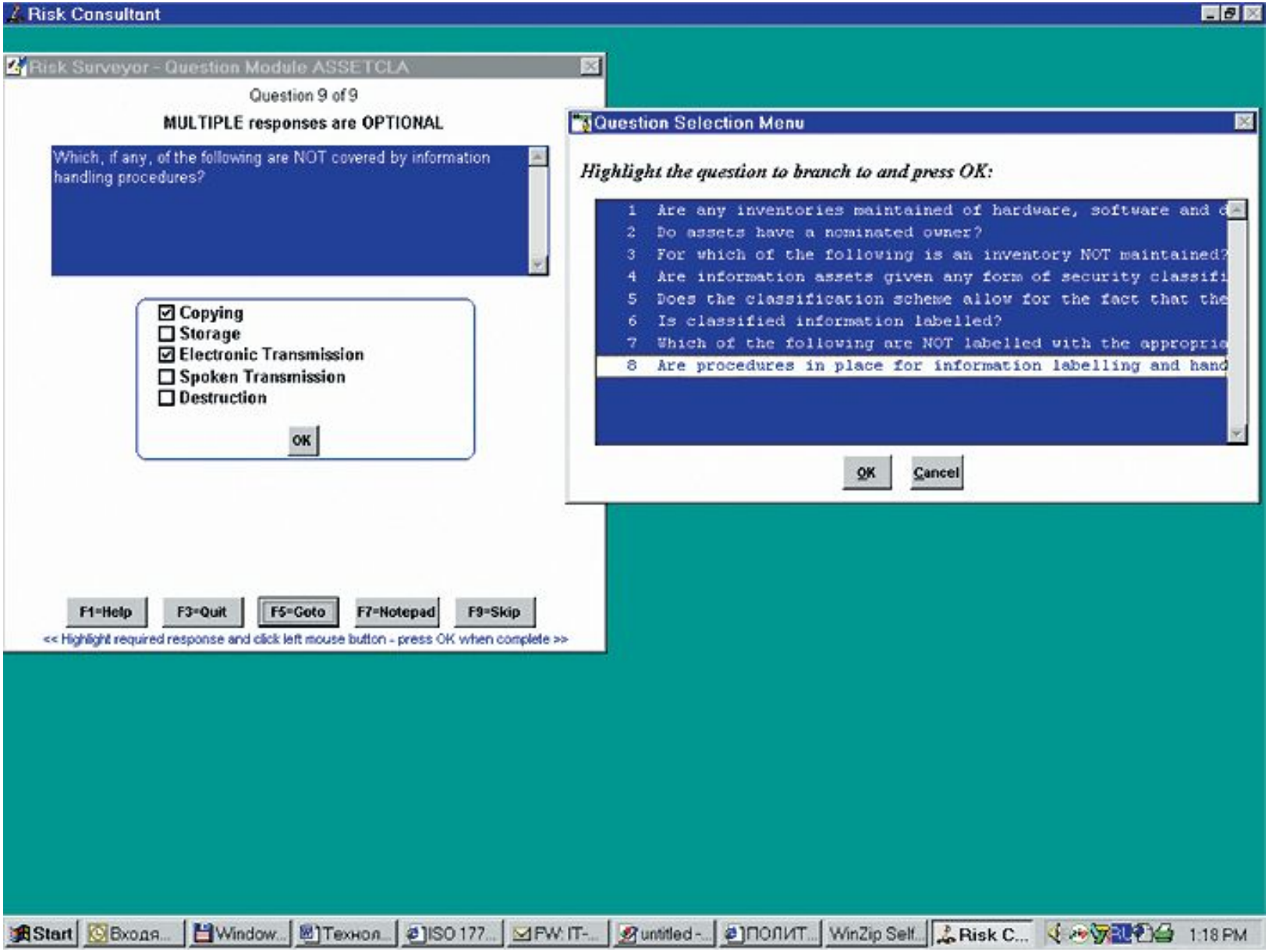
Представители:

COBRA by Systems Security Ltd

RA Software Tool. By RA Software

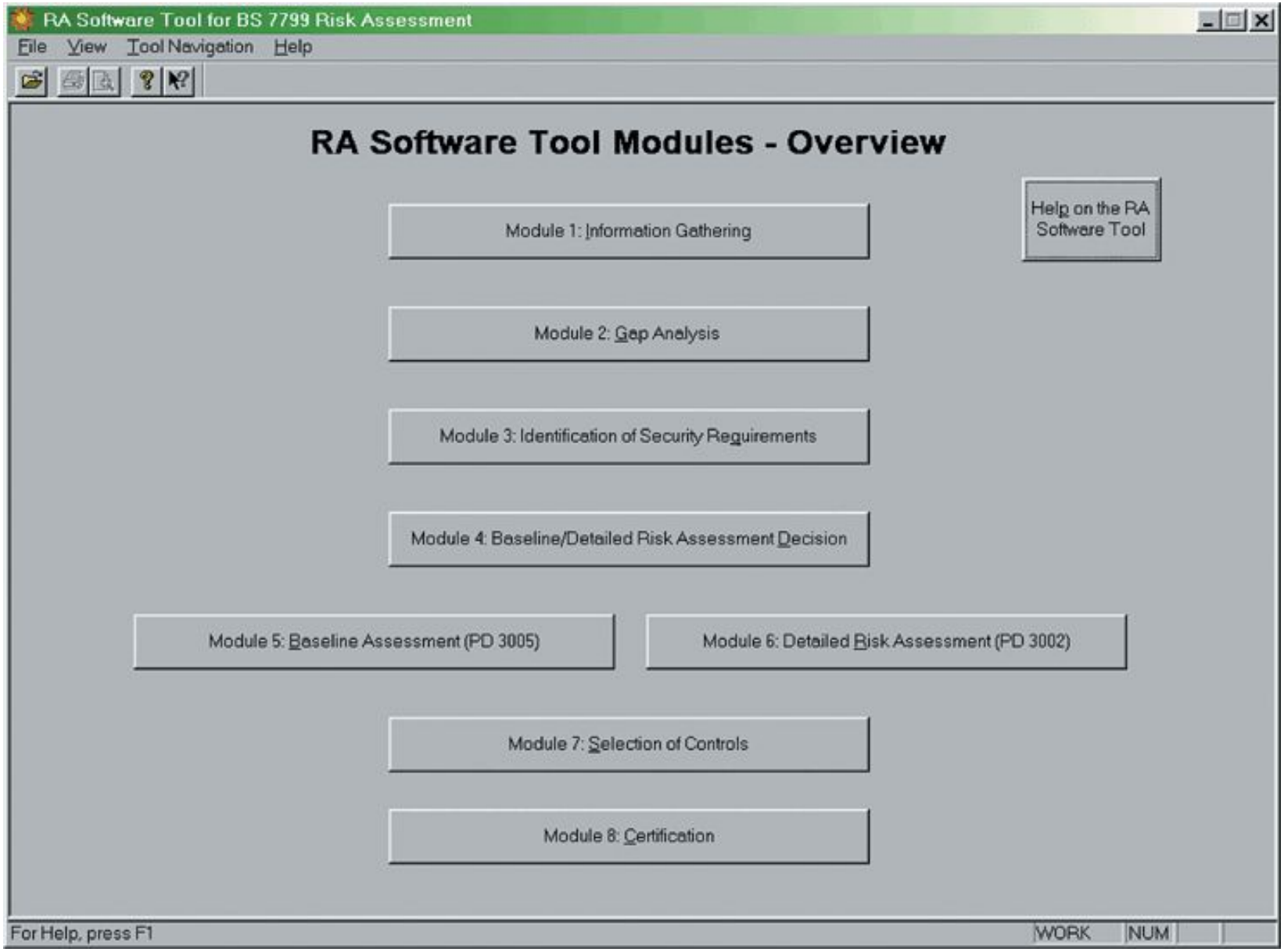
COBRA by Systems Security Ltd

требования стандарта ISO 17799 в виде тематических вопросников (check list's), на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнестранзакций компании.


Risk Consultant
Risk Surveyor - Question Module ASSETCLA
Question 9 of 9
MULTIPLE responses are OPTIONAL
Which, if any, of the following are NOT covered by information handling procedures?
Copying
Storage
Electronic Transmission
Spoken Transmission
Destruction
OK
F1=Help
F3=Quit
F5=Goto
F7=Notepad
F9=Skip
<< Highlight required response and click left mouse button - press OK when complete >>
Question Selection Menu
Highlight the question to branch to and press OK:
1 Are any inventories maintained of hardware, software and
2 Do assets have a nominated owner?
3 For which of the following is an inventory NOT maintained?
4 Are information assets given any form of security classifi
5 Does the classification scheme allow for the fact that the
6 Is classified information labelled?
7 Which of the following are NOT labelled with the appropria
8 Are procedures in place for information labelling and hand
OK
Cancel
Start
Входя...
Window...
Технол...
ISO 177...
FW: IT-...
untitled -...
ПОЛИТ...
WinZip Self...
Risk C...
1:18 PM

RA Software Tool

Эта методика позволяет выполнять оценку информационных рисков в соответствии с требованиями ISO 17799


RA Software Tool for BS 7799 Risk Assessment
File View Tool Navigation Help
RA Software Tool Modules - Overview
Help on the RA Software Tool
Module 1: Information Gathering
Module 2: Gap Analysis
Module 3: Identification of Security Requirements
Module 4: Baseline/Detailed Risk Assessment Decision
Module 5: Baseline Assessment (PD 3005)
Module 6: Detailed Risk Assessment (PD 3002)
Module 7: Selection of Controls
Module 8: Certification
For Help, press F1
WORK
NUM

Количественные методики

Решение оптимизационных задач, которые часто возникают в реальной жизни. Суть этих задач сводится к поиску единственного оптимального решения, из множества существующих.

Представители:

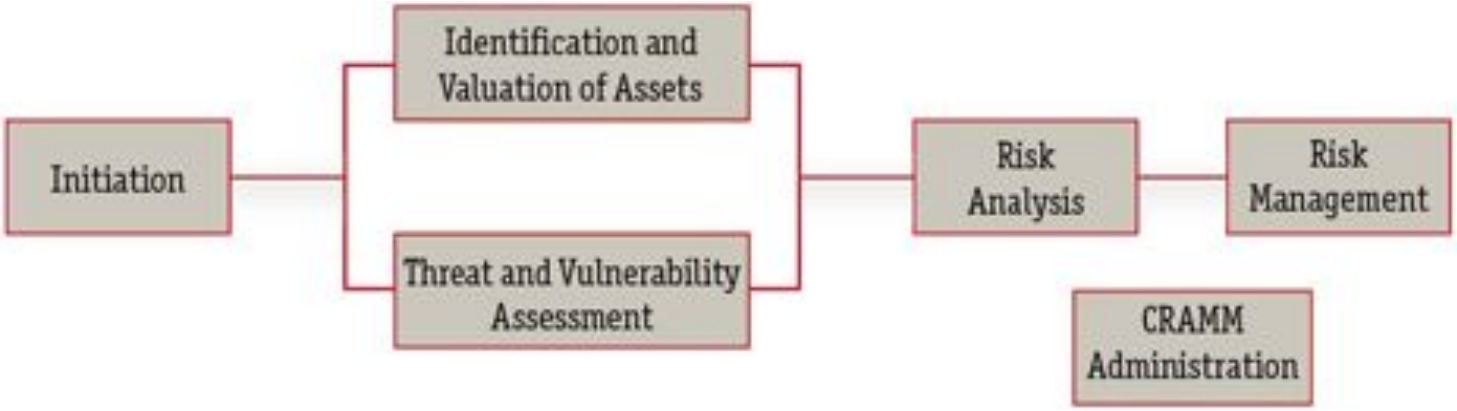
CRAMM by CCTA

ГРИФ by Digital Security Office

CRAMM ((CCTA Risk Analysis and Management Method)

- Формализация и автоматизация процедур анализа и управления рисками;
- Оптимизация расходов на средства контроля и защиты;
- Комплексное планирование и управление рисками на всех стадиях жизненного цикла информационных систем;
- Сокращение времени на разработку и сопровождение корпоративной системы защиты информации;
- Обоснование эффективности предлагаемых мер защиты и средств контроля;
- Управление изменениями и инцидентами;
- Поддержка непрерывности бизнеса;
- Оперативное принятие решений по вопросам управления безопасностью

Этапы управления рисками по CRAMM



«Initiation» — определяются границы исследуемой информационной системы компании

«Identification and Valuation of Assets» — четко идентифицируются активы и определяется их стоимость.

«Threat and Vulnerability Assessment» — идентифицируются и оцениваются угрозы и уязвимости

«Risk Analysis» — позволяет получить качественные и количественные оценки рисков.

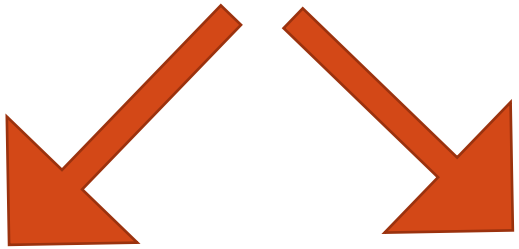
«Risk management» — предлагаются меры и средства уменьшения или уклонения от риска.

Недостатки CRAMM

- метод требует специальной подготовки и высокой квалификации аудитора;
- аудит по методу CRAMM - процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;
- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;
- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся;
- возможность внесения дополнений в базу знаний CRAMM недоступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации;
- ПО CRAMM не локализовано, существует только на английском языке;
- высокая стоимость лицензии - от 2000 до 5000 долл.

ГРИФ 2005

Дает картину защищенности информационных ресурсов в системе и позволяет выбрать оптимальную модель защиты корпоративной информации.



Модель информационных потоков

Модель угроз и уязвимостей

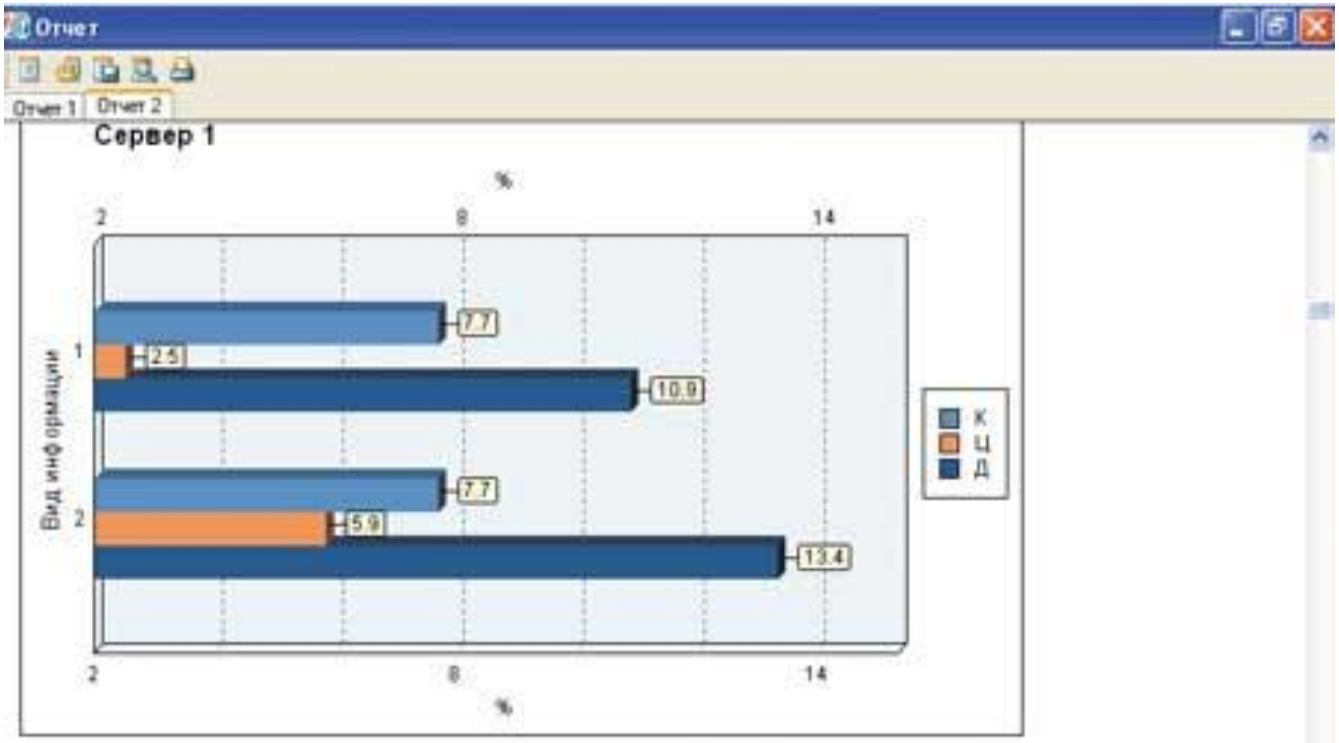
Модель информационных потоков

1. Пользователь вносит все объекты своей информационной системы: отделы и ресурсы.
2. Пользователь проставляет связи.
3. Пользователь отвечает на список вопросов по политике безопасности, реализованной в системе.
4. Пользователь доволен.

Модель угроз и уязвимостей

1. Пользователь вносит в систему объекты своей ИС.
2. Пользователь вносит угрозы и уязвимости, относящиеся к его ИС.
3. Пользователь проставляет связи.
4. Пользователь счастлив.

В результате работы с системой ГРИФ строится подробный отчет об уровне риска каждого ценного ресурса информационной системы компании



№	Вид информации	Конфиденциальность, ур.	Целостность, ур.	Доступность, ур.
1	Годовой отчет	Низкий	Низкий	Низкий
2	Информация о ценах	Низкий	Низкий	Низкий

Анализ и управление информационными рисками - ключевой фактор для построения эффективной защиты информационной системы.

Спасибо за внимание.