Методики управления информационными рисками

Презентация студентки
1 курса факультета ИКВО
Группы N3100
Кирилловой Елизаветы

- **Оценка информационных рисков** – процедура ранжирования приоритета конкретных условий и факторов, которые могут стать причиной нарушения целостности системы.

- *Оценка риска* должна обеспечить понимание возможного масштаба проблем, событий и принятие решений о том, каким образом надо обрабатывать тот или иной риск.

Методики управления

- Методики международных стандартов: ISO 15408, ISO 17799 (BS7799), BSI
- Методики национальных стандартов: NIST 80030, SAC, COSO, SAS 55/78

Управление информационными рисками любой компании предполагает:

- определение основных целей и задач защиты информационных активов компании
- создание эффективной системы оценки и управления информационными рисками
- расчет совокупности детализированных оценок рисков
- применение специального инструментария оценивания и управления рисками

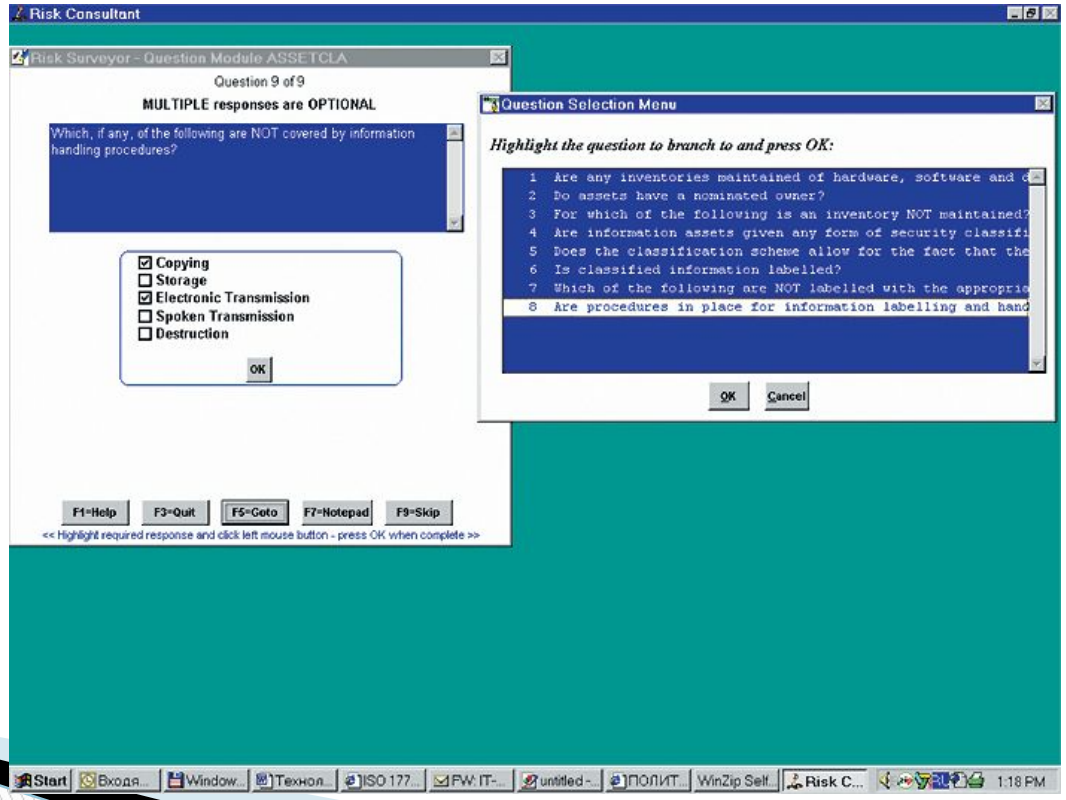
Качественные методики управления рисками. Стандарт ISO 17799.

- Часть 1. Основные аспекты организации режима информационной безопасности в компании:
  - Политика безопасности.
  - Организация защиты.
  - Классификация и управление информационными ресурсами.
  - Управление персоналом.
  - Физическая безопасность.
  - Администрирование компьютерных систем и сетей.
  - Управление доступом к системам.
  - Разработка и сопровождение систем.
  - Планирование бесперебойной работы организации.
  - Проверка системы на соответствие требованиям ИБ.

- Часть 2: Спецификации, 2002 г., рассматривает эти же аспекты с точки зрения сертификации режима информационной безопасности компании на соответствие требованиям стандарта.

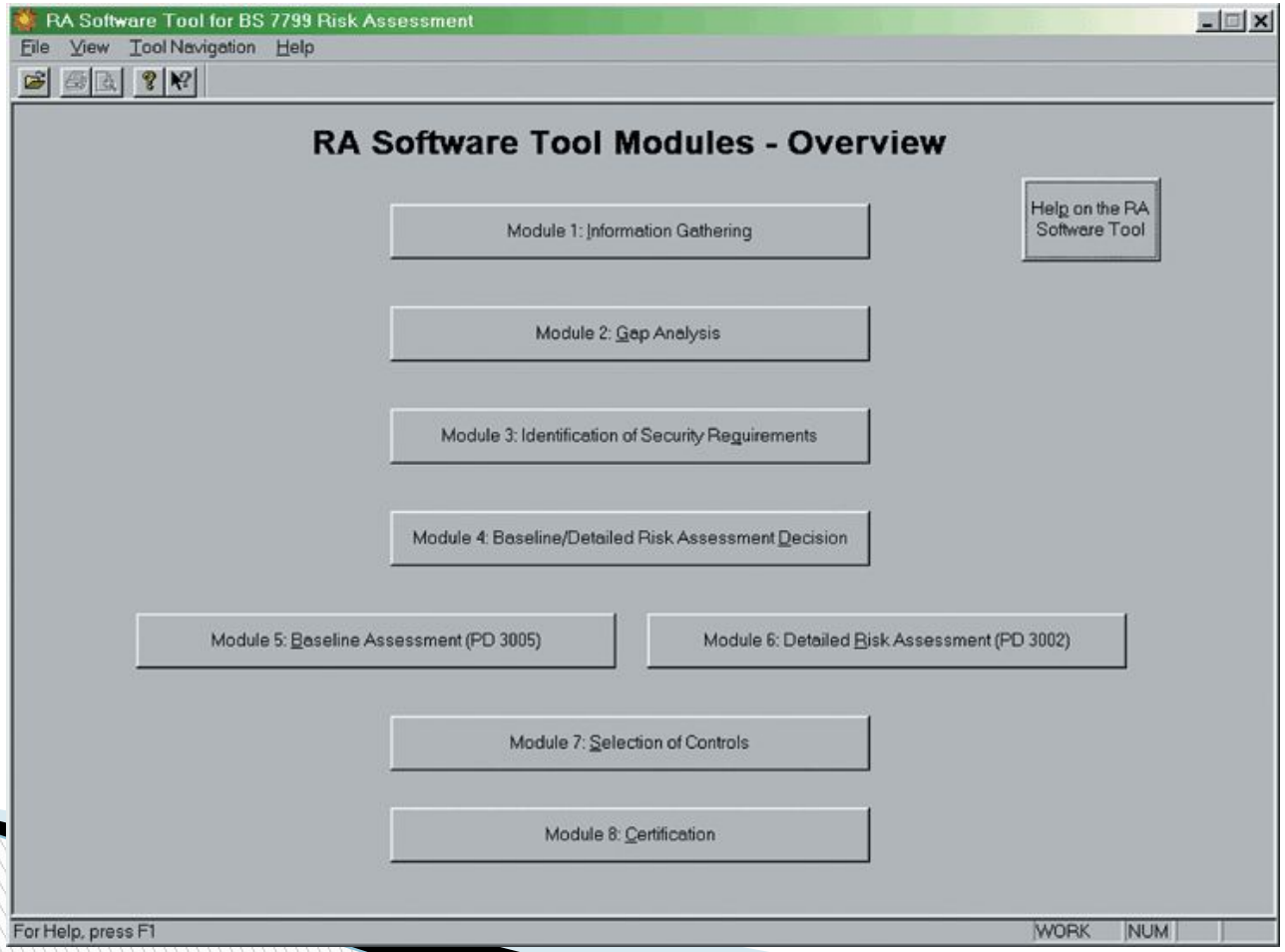
COBRA

- Методика COBRA представляет 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.



RA Software Tool

- Эта методика позволяет выполнять оценку информационных рисков в соответствии с требованиями ISO 17799, а при желании в соответствии с более детальными спецификациями руководства PD 3002 Британского института стандартов.



Количественные методики управления рисками

- На практике такие методики управления рискамипозволяют:

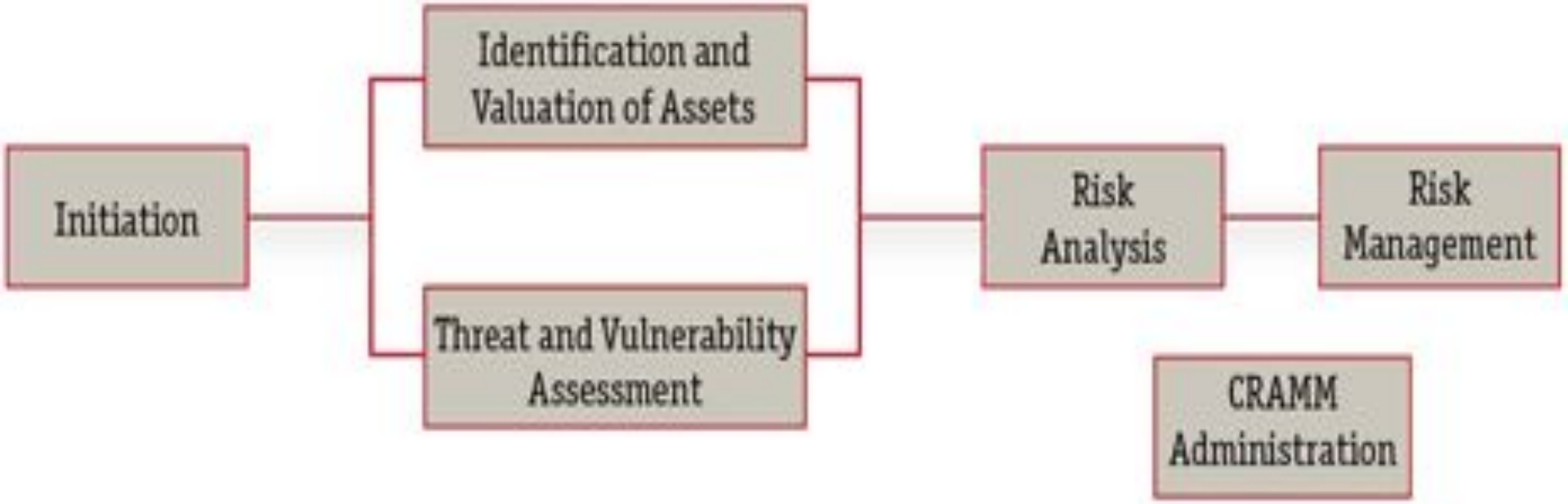
- Создавать модели информационных активов компании с точки зрения безопасности;
  - Классифицировать и оценивать ценности активов;
  - Составлять списки наиболее значимых угроз и уязвимостей безопасности;
  - Ранжировать угрозы и уязвимости безопасности;
  - Обосновывать средства и меры контроля рисков;
  - Оценивать эффективность/стоимость различных вариантов защиты;
  - Формализовать и автоматизировать процедуры оценивания и управления рисками.

- Одной из наиболее известных методик этого класса является методика CRAMM.

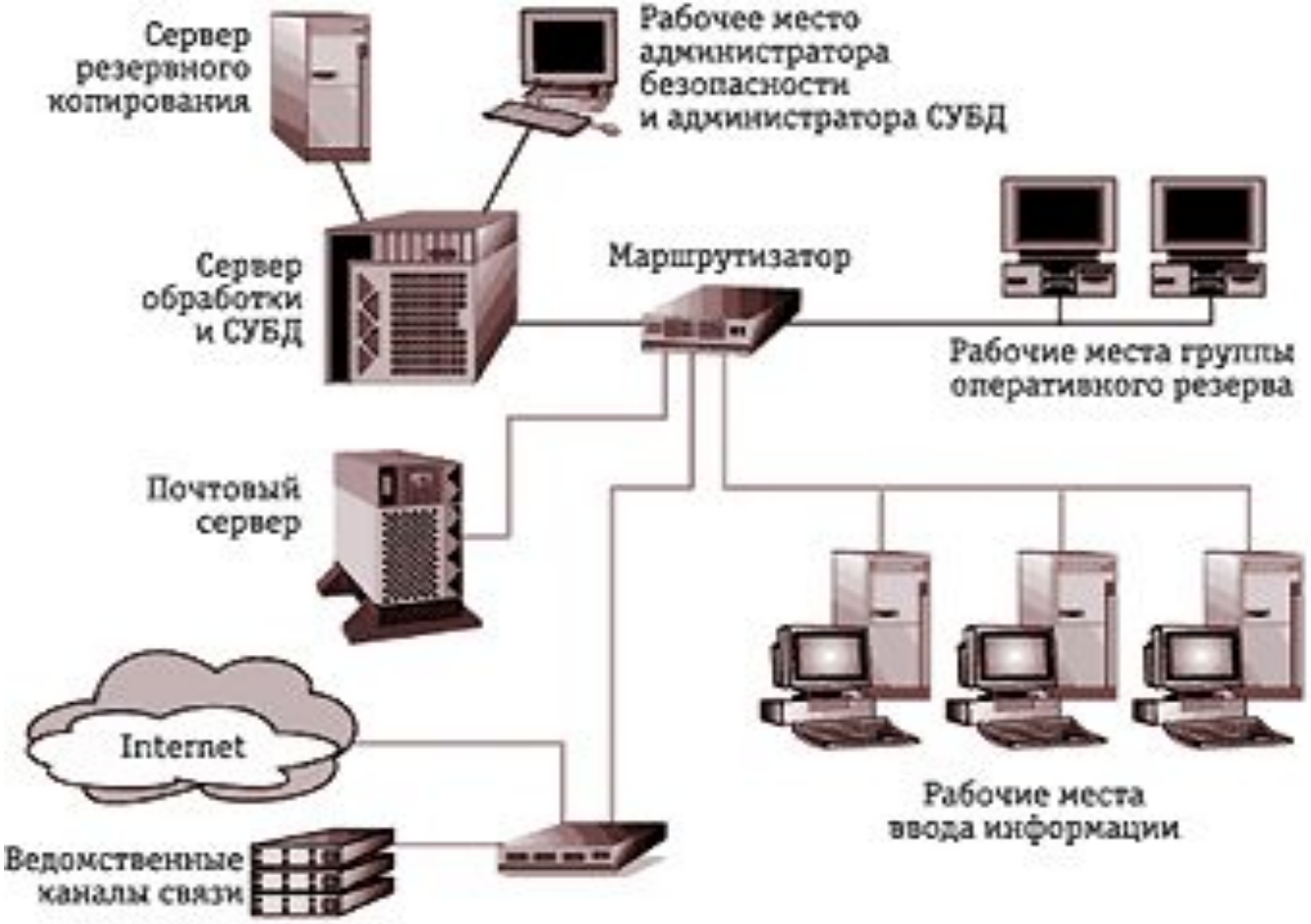
CRAMM

Основными целями методики CRAMM являются:

- 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 и пр.


Initiation
Identification and Valuation of Assets
Threat and Vulnerability Assessment
Risk Analysis
Risk Management
CRAMM Administration

Пусть проводится оценка информационных рисков следующей корпоративной информационной системы

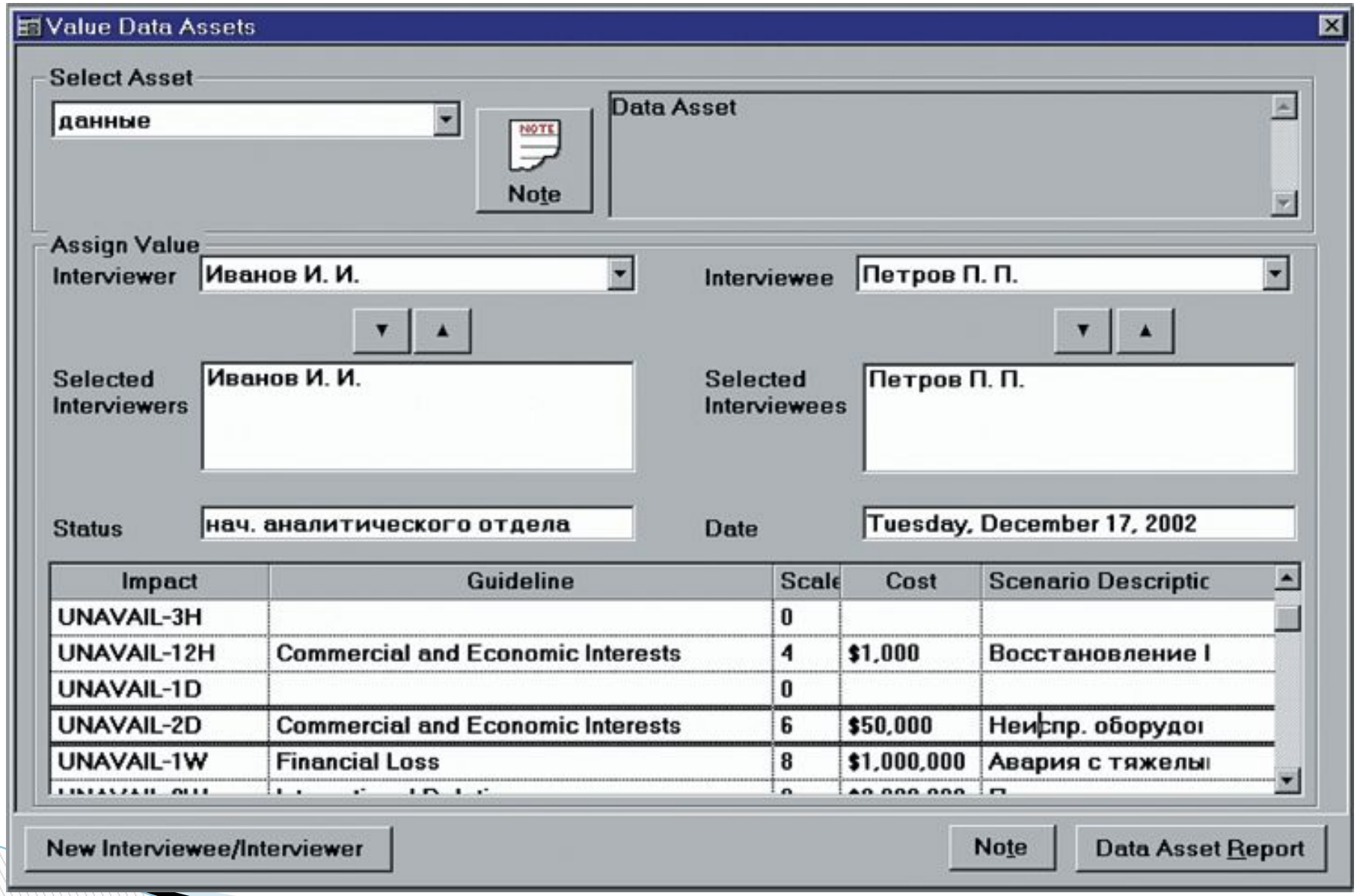


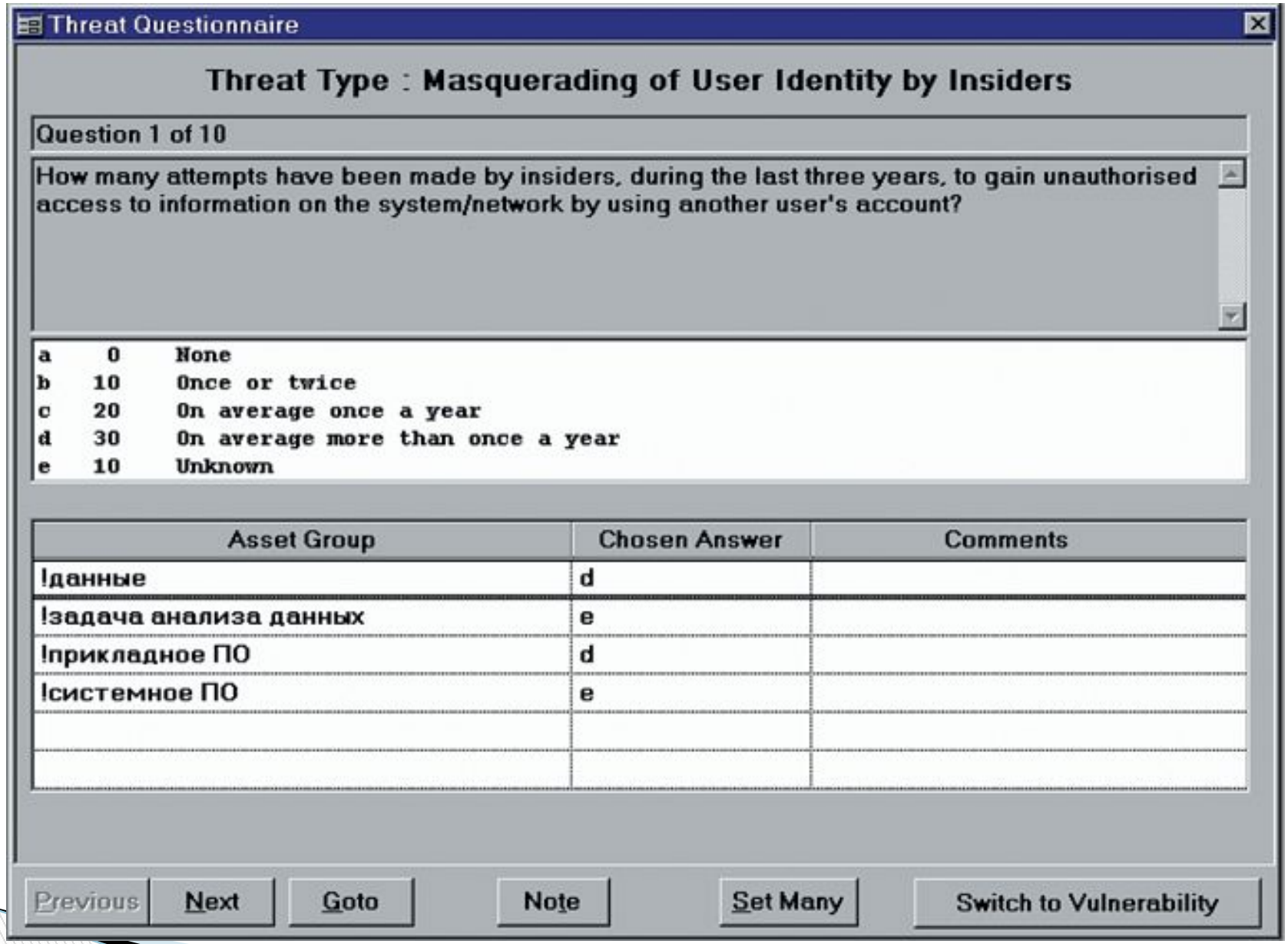
Ценность ресурсов

- Ценность данных и программного обеспечения определяется в следующих ситуациях:
  - недоступность ресурса в течение определенного периода времени;
  - разрушение ресурса — потеря информации, полученной со времени последнего резервного копирования или ее полное разрушение;
  - нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
  - модификация рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
  - ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

- Для оценки возможного ущерба предлагается использовать следующие критерии:
  - ущерб репутации организации;
  - нарушение действующего законодательства;
  - ущерб для здоровья персонала;
  - ущерб, связанный с разглашением персональных данных отдельных лиц;
  - финансовые потери от разглашения информации;
  - финансовые потери, связанные с восстановлением ресурсов;
  - потери, связанные с невозможностью выполнения обязательств;
  - дезорганизация деятельности.

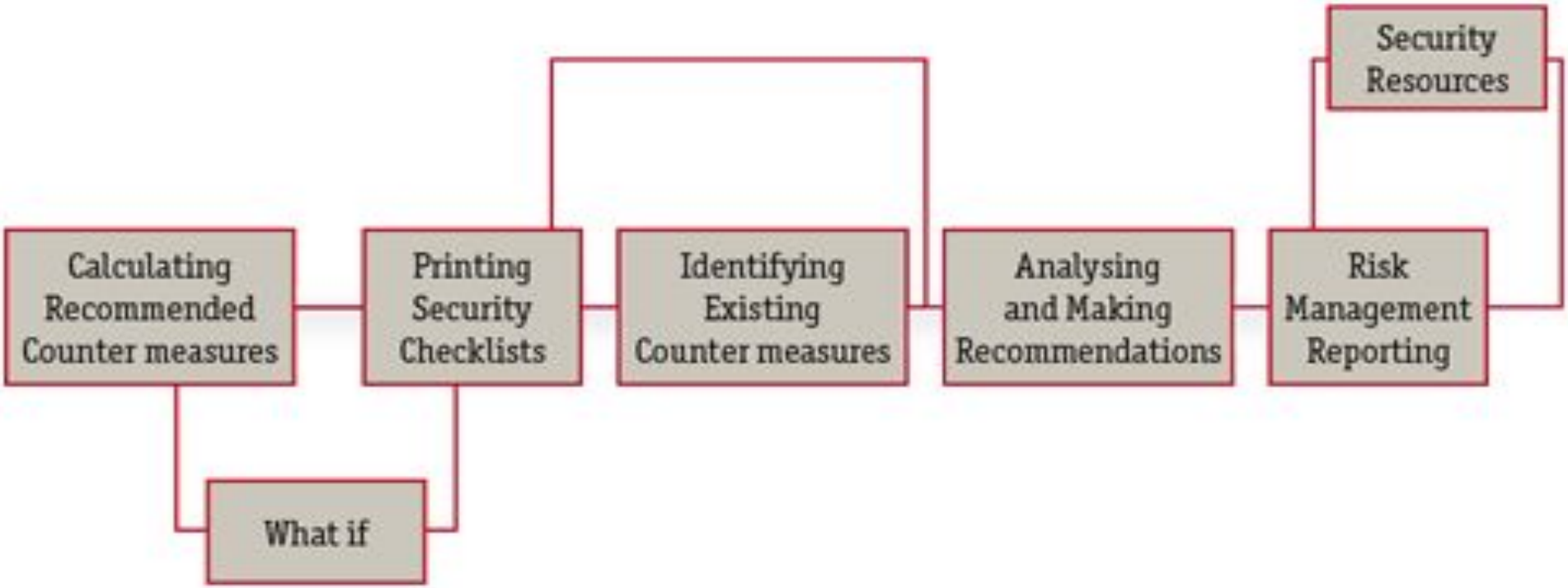
- Ущерб репутации организации:
  2 – негативная реакция отдельных чиновников, общественных деятелей;
  4 – критика в средствах массовой информации, не имеющая широкого общественного резонанса;
  6 – негативная реакция отдельных депутатов Думы, Совета Федерации;
  8 – критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т. п.;
  10 – негативная реакция на уровне Президента и Правительства.
- Ущерб для здоровья персонала:
  2 – минимальный ущерб (последствия не связаны с госпитализаций или длительным лечением);
  4 – ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);
  6 – серьезные последствия (длительная госпитализация, инвалидность одного или нескольких сотрудников);
  10 – гибель людей.
- Финансовые потери, связанные с восстановлением ресурсов:
  2 – менее $1000;
  6 – от $1000 до $10 000;
  8 – от $10 000 до $100 000;
  10 – свыше $100 000.
- Дезорганизация деятельности в связи с недоступностью данных:
  2 – отсутствие доступа к информации до 15 минут;
  4 – отсутствие доступа к информации до 1 часа;
  6 – отсутствие доступа к информации до 3 часов;
  8 – отсутствие доступа к информации от 12 часов;
  10 – отсутствие доступа к информации более суток.


Value Data Assets
Select Asset
данные
Note
Data Asset
Assign Value
Interviewer
Иванов И. И.
Interviewee
Петров П. П.
Selected Interviewers
Иванов И. И.
Selected Interviewees
Петров П. П.
Status
нач. аналитического отдела
Date
Tuesday, December 17, 2002
Impact
Guideline
Scale
Cost
Scenario Descriptic
UNAVAIL-3H
0
UNAVAIL-12H
Commercial and Economic Interests
4
$1,000
Восстановление I
UNAVAIL-1D
0
UNAVAIL-2D
Commercial and Economic Interests
6
$50,000
Неиспр. оборудо
UNAVAIL-1W
Financial Loss
8
$1,000,000
Авария с тяжелы
New Interviewee/Interviewer
Note
Data Asset Report


Threat Questionnaire
Threat Type : Masquerading of User Identity by Insiders
Question 1 of 10
How many attempts have been made by insiders, during the last three years, to gain unauthorised access to information on the system/network by using another user's account?
a 0 None
b 10 Once or twice
c 20 On average once a year
d 30 On average more than once a year
e 10 Unknown
Asset Group
Chosen Answer
Comments
!данные
d
!задача анализа данных
e
!прикладное ПО
d
!системное ПО
e
Previous
Next
Goto
Note
Set Many
Switch to Vulnerability

- Уровень угроз оценивается, в зависимости от ответов, как:
  - очень высокий;
  - высокий;
  - средний;
  - низкий;
  - очень низкий.

- Уровень уязвимости оценивается, в зависимости от ответов, как:
  - высокий;
  - средний;
  - низкий;
  - отсутствует.



- Обеспечение безопасности на сетевом уровне.
- Обеспечение физической безопасности.
- Обеспечение безопасности поддерживающей инфраструктуры.
- Меры безопасности на уровне системного администратора.

MethodWare

Компания MethodWare разработала свою собственную методику оценки и управления рисками и выпустила ряд соответствующих инструментальных средств. К этим средствам относятся:

- ПО анализа и управления рисками Operational Risk Builder и Risk Advisor. Методика соответствует австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и стандарту ISO17799.
- ПО управления жизненным циклом информационной технологии в соответствии с CobiT Advisor 3rd Edition (Audit) и CobiT 3rd Edition Management Advisor. В руководствах CobiT существенное место уделяется анализу и управлению рисками.
- ПО для автоматизации построения разнообразных опросных листов Questionnaire Builder.

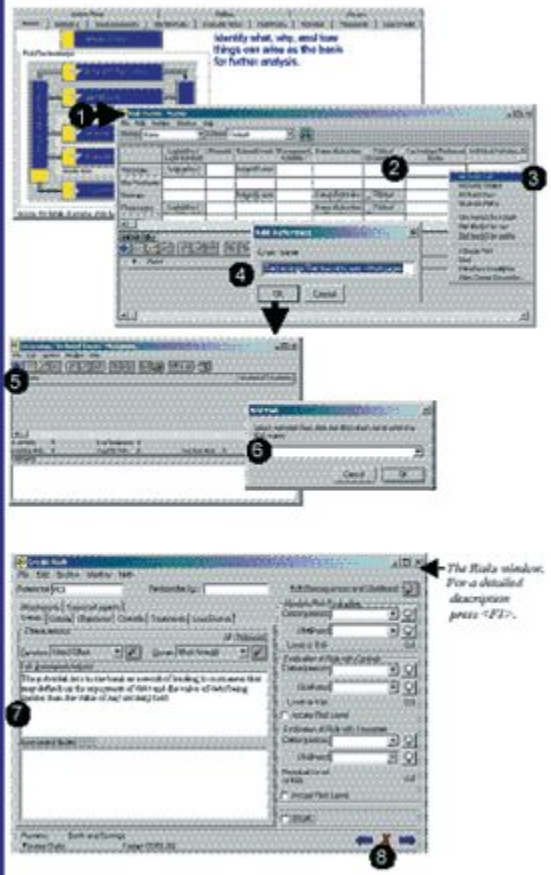
Описание рисков

To add a risk to a source of risk/area of impact:

1. Click the Identify Risks button on the **Model tab** on the **Home window**.
2. Select the source of risk/area of impact cell for which you want to add a risk.
3. Click the right mouse button and click the option **Activate Cell**.
4. Type a name for the activated cell and click the **OK** button.

   A dialog displaying information unique to that source of risk/area of impact relationship displays.

   NOTE: This dialog contains the same information as, if you select the activated cell, the context sensitive **Linked Risks pane**, located directly under the matrix.
5. On the resulting dialog click the button.
6. Type a name for the risk and click the **OK** button. The **Risks window** displays with the new risk in view.
7. Complete the appropriate fields and tabs.



Performing an assessment of absolute risk

To conduct an absolute risk assessment:

1. Double click the first risk on the **Evaluate Risks tab** on the **Home** window.
2. Select a consequence rating for the risk in the **Consequence** field of the **Absolute Risk Evaluation** section.
3. Select a likelihood rating for the risk in the **Likelihood** field of the **Absolute Risk Evaluation** section.
4. Click the button when complete.