# RiskWatch

написано Александр Астахов | 11 июня, 2023

Метод *RiskWatch*, разработанный при участии Национального Института Стандартов и Технологий США (U.S. NIST), Министерства обороны США (U.S. DoD) и Министерства обороны Канады (Canadian Dept. of National Canadian Defence) в 1988 году, фактически является стандартом для американских государственных организаций. По заявлению разработчиков, этот метод используют в тысячах организаций не только в США, но и по всему миру.

К основным достоинствам программного продукта RiskWatch, помимо сравнительной простоты использования, можно отнести следующее:

- глубоко проработанная и хорошо зарекомендовавшая себя методология анализа рисков;
- сочетание количественной и качественной оценки рисков;
- обширная база знаний по угрозам, уязвимостям и контрмерам;
- возможности редактирования и совершенствования базы знаний;
- настраиваемые отчеты.

RiskWatch представляет собой семейство программных продуктов, построенных на общем программном ядре, которые предназначены для управления различными видами рисков и поддержки различных стандартов.

Продукты RiskWatch включают в себя следующее:

- HIPAA-Watch for Security;
- RiskWatch for Information Systems;
- RiskWatch 17799 (ISO 17799);
- RiskWatch for Physical & Homeland Security;

- RiskWatch for Seaport Security;
- RW-MEGA SHIP Security Version;
- RiskWatch for Force Protection;
- RiskWatch for Event Security;
- RiskWatch for Sarbanes-Oxley (SOX).

По заявлению разработчиков, в этих продуктах реализована поддержка многих стандартов и руководящих документов в области информационной безопасности, актуальных в основном для США:

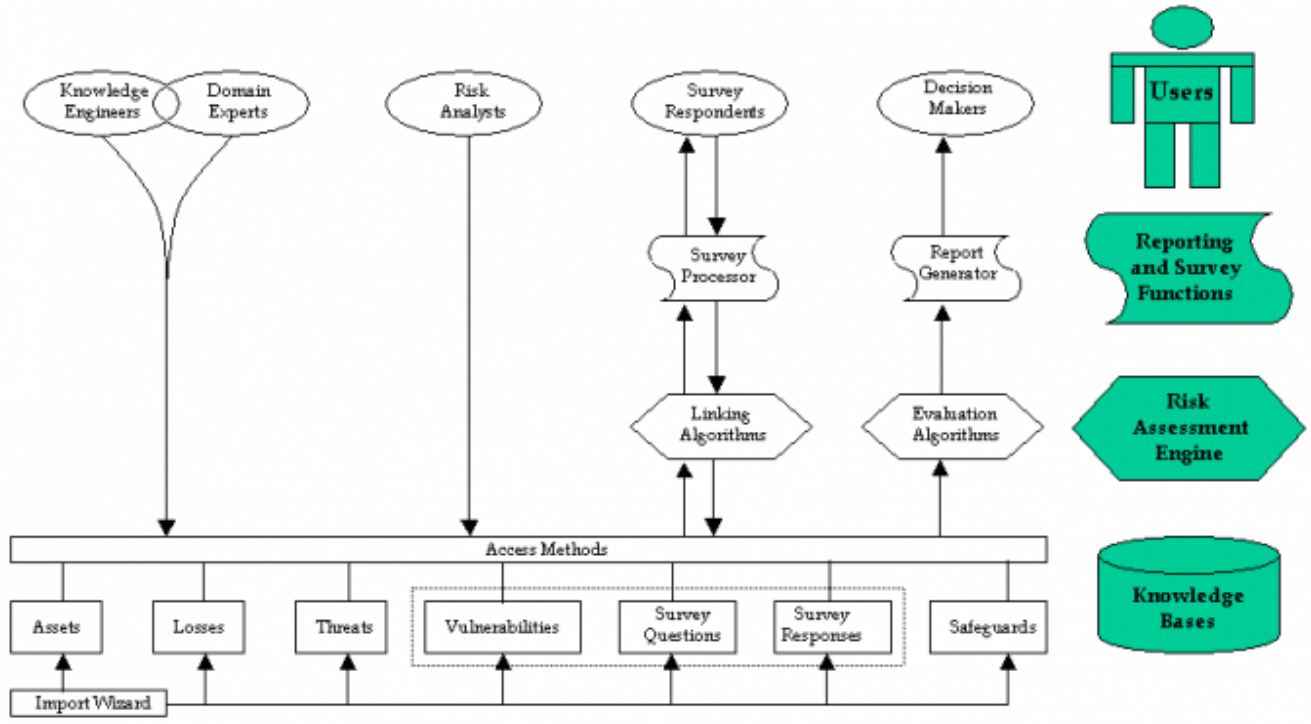
- ISACA Auditor’s Guideline for Risk Analysis;
- BS 7799 (ISO 17799);
- DoD TCSEC, DOD 5200.28-STD (Orange Book);
- OMB circulars on internal controls and management accountability A-123, A-124, A-127, and A-130;
- Computer Security Act of 1987;
- Privacy Act of 1974;
- Federal Manager’s Financial Integrity Act 1982;
- FIPS-Pub 65 Guidelines for ADP/EDP Risk Analysis;
- HIPAA;
- Army Field Manual 31 for Physical Security;
- Bioterrorism Preparedness and Response Act of 2002;
- Maritime Transport Security Act of 2002;
- International Maritime Organization Ship and Port Facility Security (ISPS) Code;
- Gramm Leach Bliley Act.

Все продукты RiskWatch построены на одной унифицированной платформе, архитектура которой является достаточно типичной для подобных систем. Упрощенное представление такой архитектуры показано на рисунке и включает в себя следующее:

- *обширную базу знаний*, содержащую информацию по активам, угрозам, уязвимостям, видам ущерба, контрмерам, а также опросные листы для оценки факторов риска;
- *программный интерфейс (API*) для работы с базой знаний, а

также средства импорта информации, например данных по активам;

- *модуль оценки рисков*, реализующий алгоритмы анализа и оценивания рисков на основании данных из базы знаний и результатов опросов;
- *интерфейсные модули*, предназначенные для формирования и заполнения опросников пользователями продукта, а также для создания отчетов по результатам оценки рисков.




---

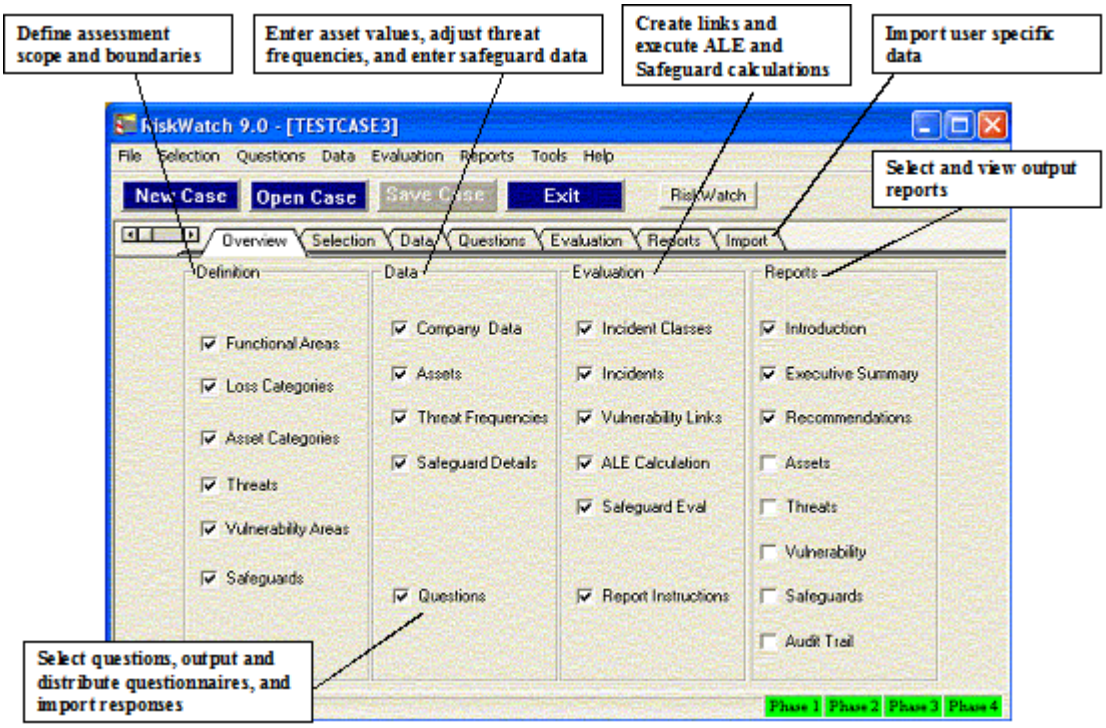
*Основные этапы оценки рисков по методу RiskWatch:*

1. *Определение параметров обследования.*
2. *Проведение интервью и ввод данных.*
3. *Расчет величины рисков.*
4. *Формирование отчетов.*

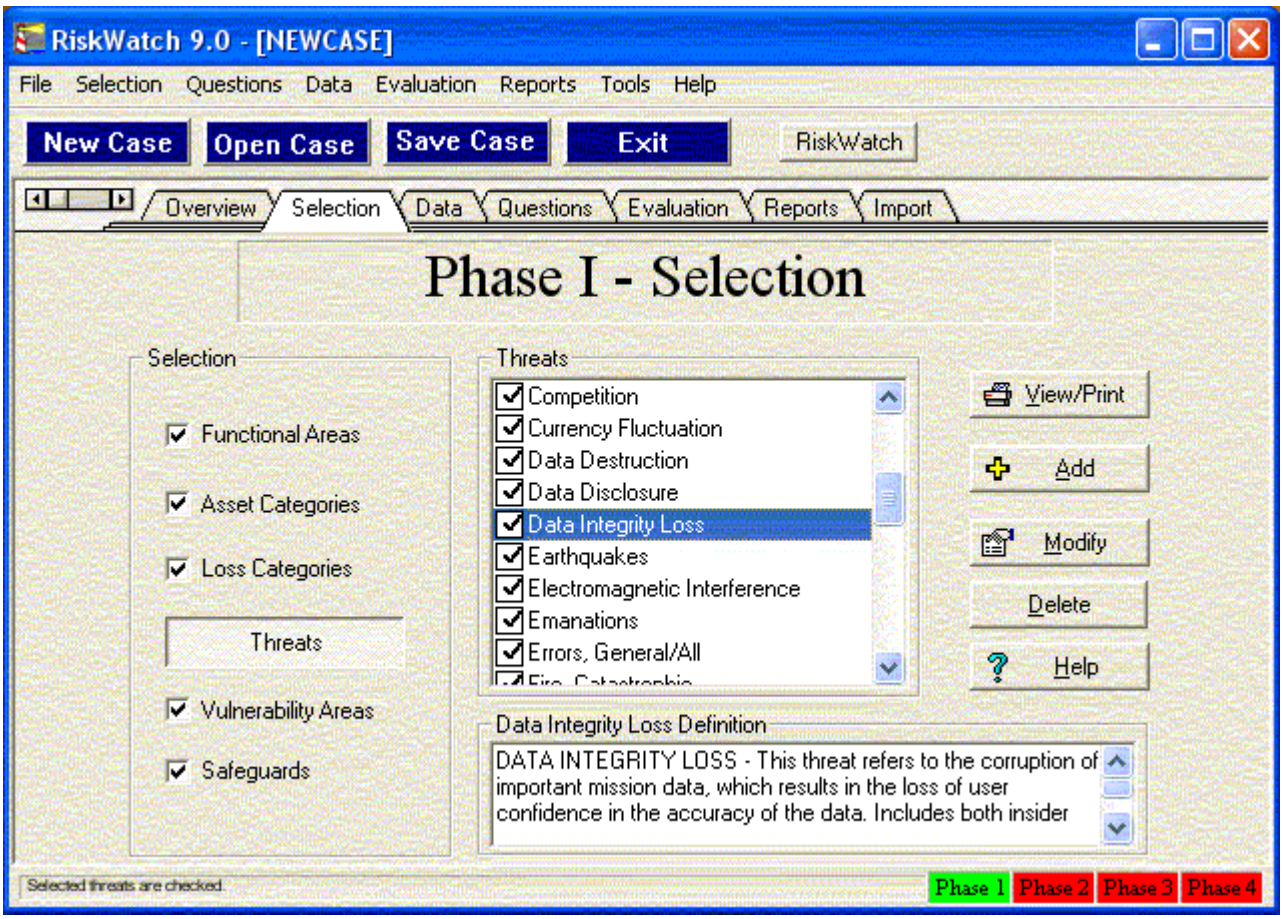
---

*Четыре стадии оценки рисков*(Определение параметров (Definition), Ввод данных (Data), Оценка рисков (Evaluation), Формирование отчетов (Reports)) и *степень*

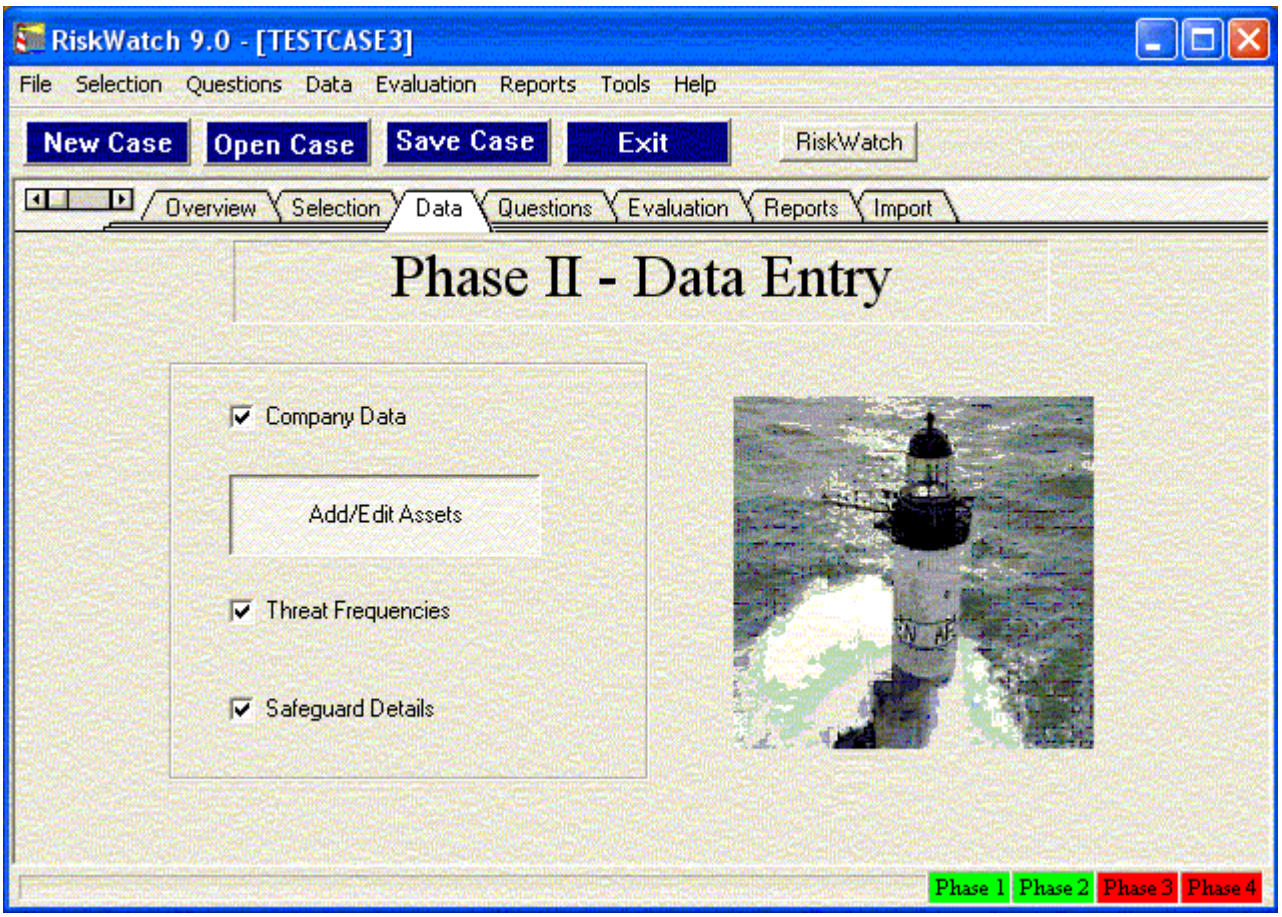
*их завершенности* представлены в наглядной форме на первом экране программы.



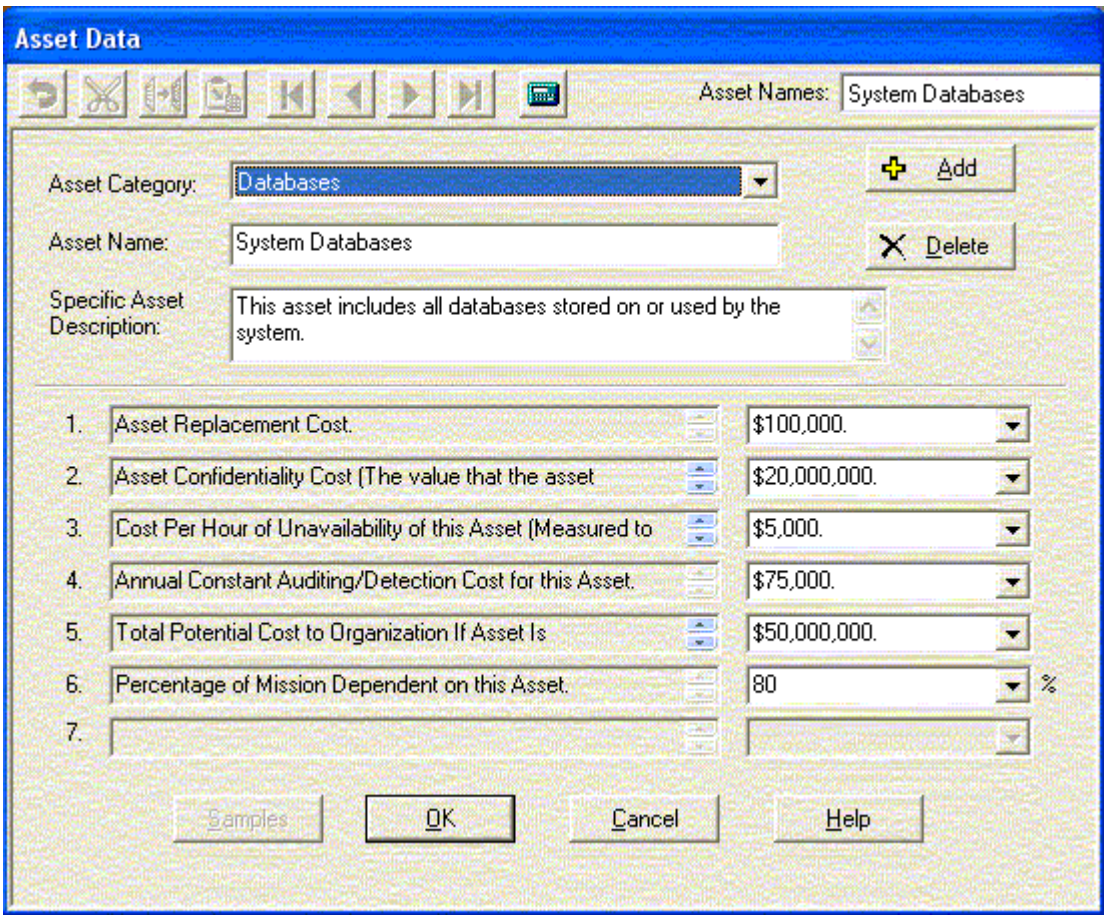

На этапе *определения параметров (Definition)* задаются область оценки, категории ущерба, категории активов, рассматриваемые угрозы, уязвимости и применяемые контрмеры. Можно использовать стандартные параметры и добавлять свои собственные.



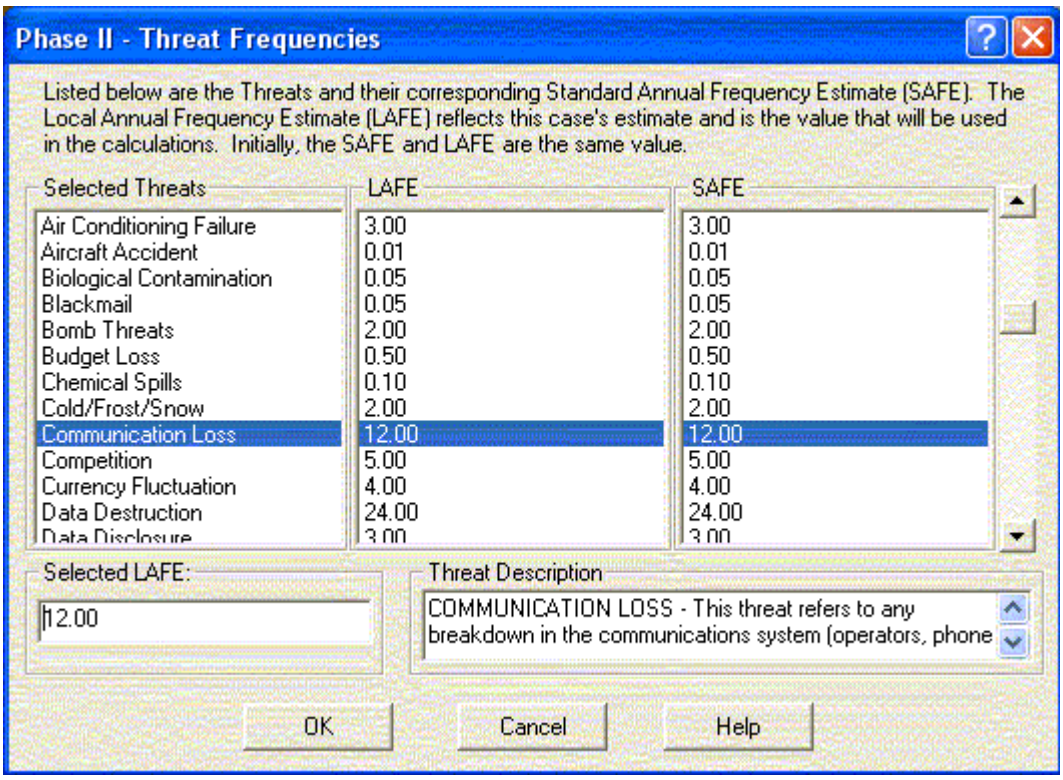

На этапе *ввода данных (Data)* в систему заносятся данные о ценности активов, вероятности угроз, величине уязвимостей и стоимости контрмер.



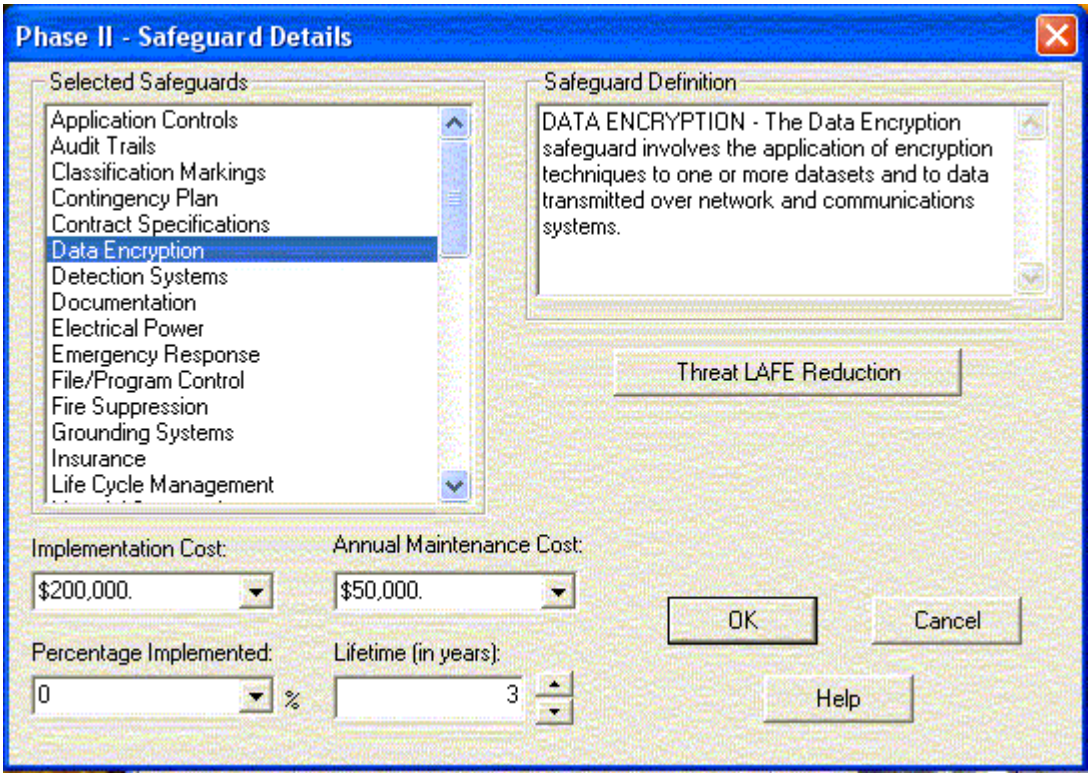

Ценности активов, определяемой величиной ущерба в результате нарушения конфиденциальности, целостности и доступности активов, соответствуют определенные оценочные денежные величины.




Ожидаемая частота реализации угроз определяется в терминах *среднегодовой оценочной частоты угрозы* (Annual Frequency Estimate). База знаний RiskWatch определяет для каждой угрозы *стандартную оценочную частоту* (StandardAnnualFrequencyEstimate, SAFE). Для вычисления рисков используется *локальная оценочная частота угрозы* (Local Annual Frequency Estimate, LAFE), которую пользователь определяет сам, используя в качестве базового значение SAFE.

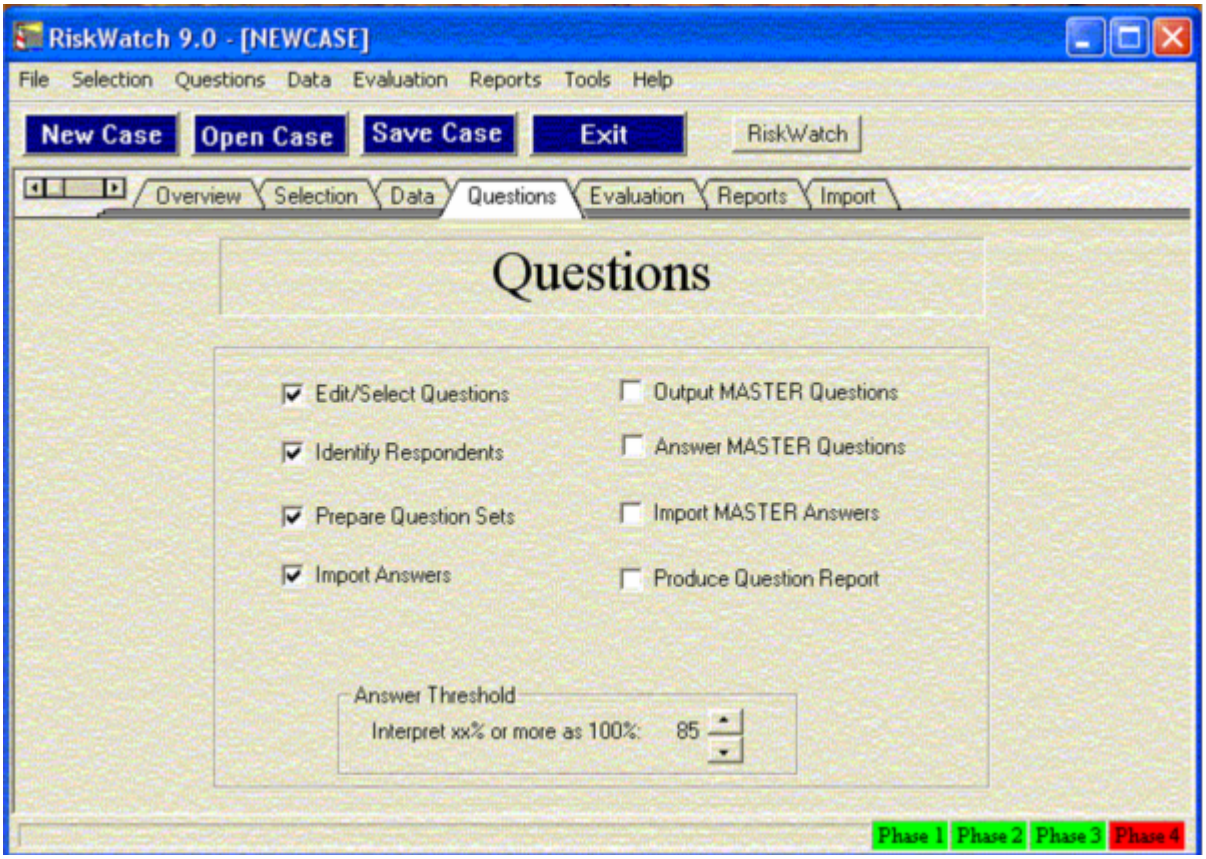



Для каждой контрмеры задается ее стоимость, которая определяется стоимостью внедрения и сопровождения. Также учитывается, на какой стадии находится реализация контрмеры, продолжительность ее жизненного цикла и насколько это контрмера уменьшает оценочную частоту реализации угрозы (LAFE).

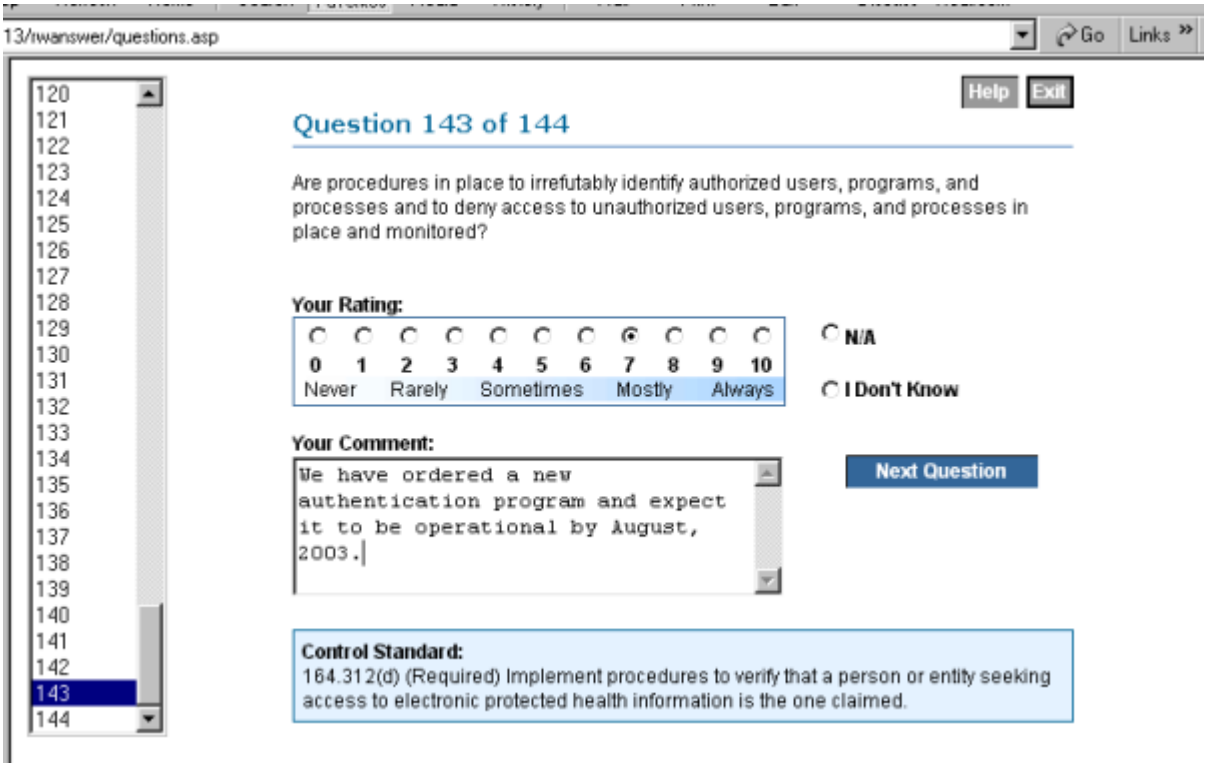



На данном этапе также осуществляется формирование опросных

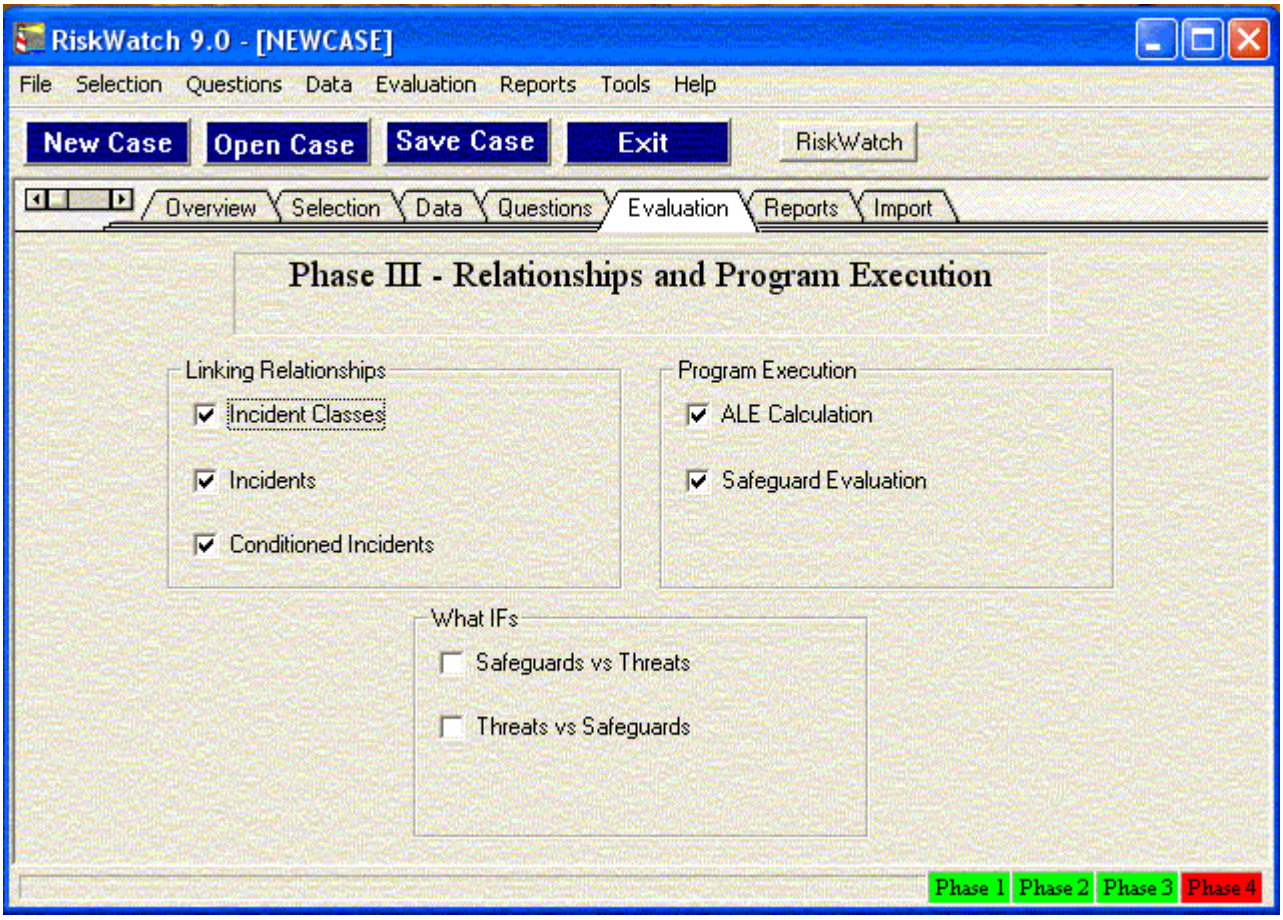
листов, используемых для получения информации от владельцев активов, представителей бизнеса и экспертов предметной области.




Для проведения интервью используется веб-ориентированный интерфейс, позволяющий опрашивать любое количество экспертов в удаленном режиме.

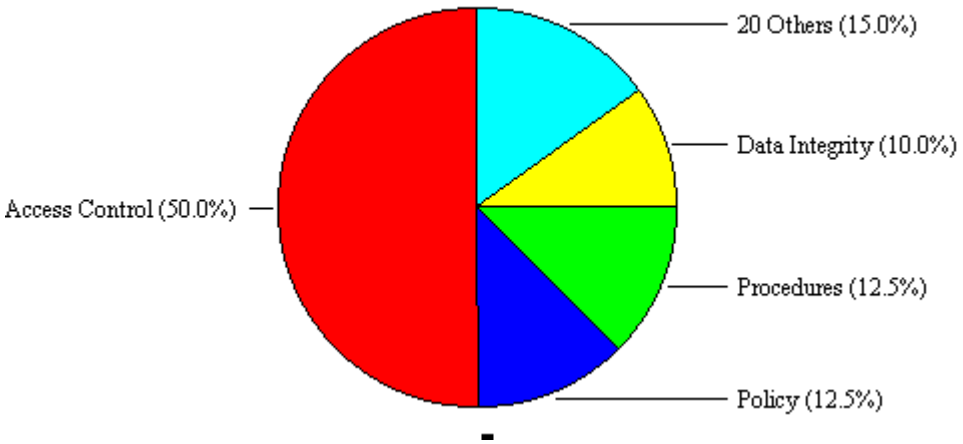



На этапе *оценки рисков (Evaluation)* производится связывание между собой данных о ценности активов, частоте угроз и величине уязвимостей. В результате производится расчет *количественных значений ожидаемого среднегодового ущерба* (Annual Loss Expectancy, ALE) для каждой комбинации актив–угроза–уязвимость. На данном этапе также производится расчет ROI для контрмер и рассмотрение сценариев «А что если?» (What Ifs), позволяющих выбрать для уменьшения рисков оптимальную комбинацию контрмер.



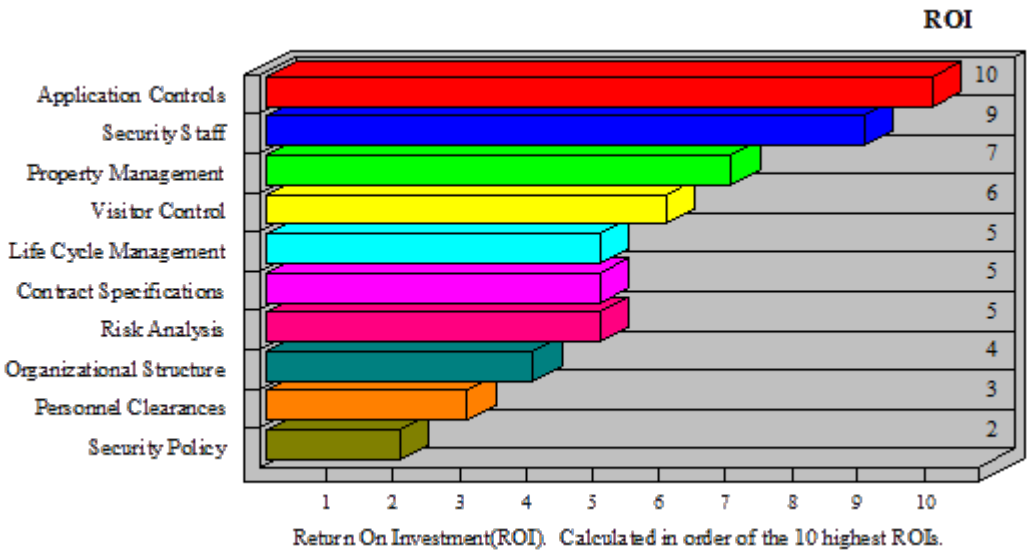

На этапе *формирования отчетов (Reports)* распечатывается предопределенный набор отчетов по результатам оценки рисков.


Используемые в отчетах графики представляют статистическую информацию, например о распределении уязвимостей информационной системы по областям контроля.




-

Рекомендуемые контрмеры могут быть отсортированы в порядке убывания значения ROI, что является одним из основных показателей для принятия решения относительно реализации контрмер и соответствующих приоритетах их реализации.


ROI
Application Controls
Security Staff
Property Management
Visitor Control
Life Cycle Management
Contract Specifications
Risk Analysis
Organizational Structure
Personnel Clearances
Security Policy
10
9
7
6
5
5
5
4
3
2
1
2
3
4
5
6
7
8
9
10
Return On Investment(ROI). Calculated in order of the 10 highest ROIs.