Deloitte.

Анализ информационных рисков.

Круглый стол, 12 апреля 2007 г.

Искандер Конеев

Аудит • Налоги • Консалтинг • Корпоративные финансы •

Важность управления рисками

Оценка и анализ рисков – основа построения СУИБ:

- Стандарты – ISO17799 и ISO27001
- Ответ на вопрос об экономической целесообразности безопасности

Известные формулы

- Количественное определение риска:
  - **ALE=SLE x ARO** – сколько тратить на безопасность
- Определение риска:
  - **R = f (I , P)** – I – размер ущерба, P – вероятность реализации ущерба
  - **$P = f_1 (T , V)$** – T – степень реализации угрозы, V – степень опасности уязвимости

Угрозы и уязвимости

Угрозы и уязвимости хорошо известны специалистам:

- Описаны в литературе
- Он-лайн базы данных
- Рассылки производителей

BS 7799:3 (приложение C.2) – около 80 примеров угроз

Cert.org (база уязвимостей) – более 300 в 2006 году

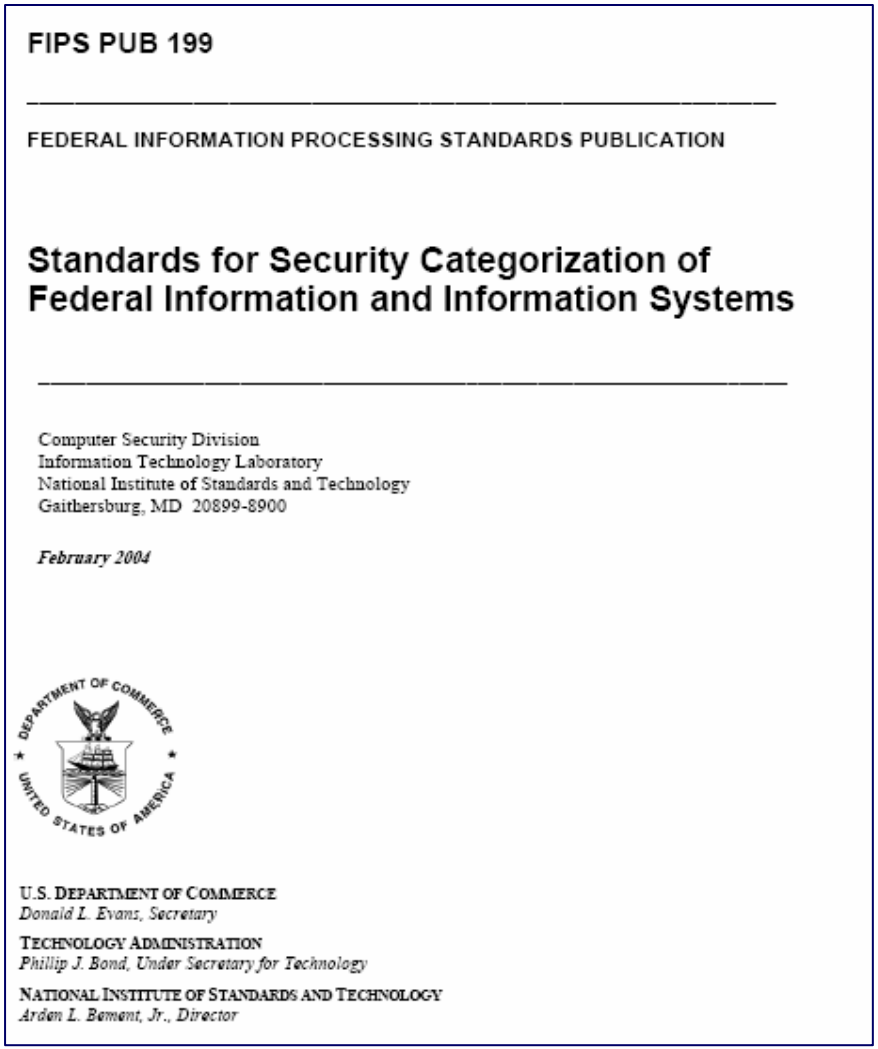
Наиболее сложные аспекты

- Навыки специалиста по оценке рисков (по BS7799:3):
  - Понимание бизнеса и риск-аппетита
  - Понимание концепции риска
  - Понимание ИТ угроз и уязвимостей
  - Понимание типов контролей ИБ
  - Навыки использования методик оценки рисков
  - Аналитические способности
  - Определение необходимых контактных лиц
  - Коммуникативные способности
- Наиболее сложные аспекты – определение размера ущерба:
  - Идентификация актива
  - Определение владельца актива
  - Оценка стоимости актива
  - Оценка ущерба актива

Имеющиеся инструменты

FIPS PUB 199

- Категории информации:
  - Конфиденциальность
  - Целостность
  - Доступность
- Степени:
  - Низкая
  - Средняя
  - Высокая



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

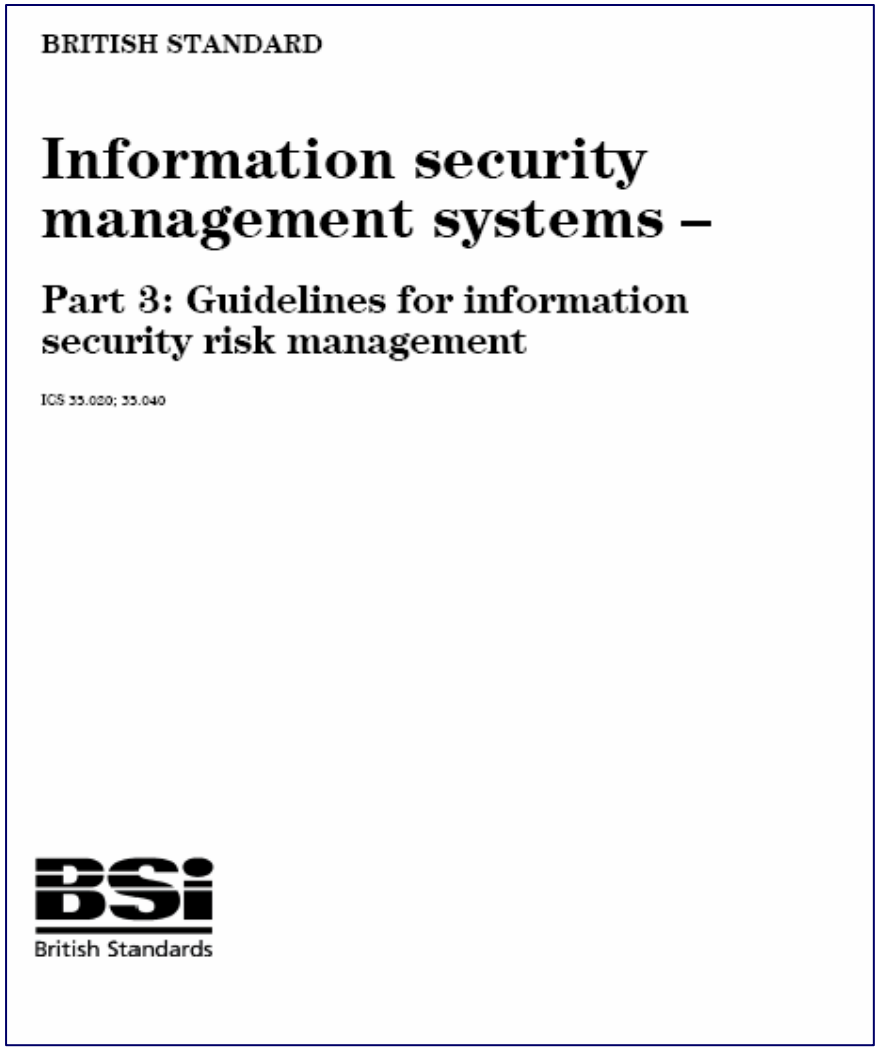
Имеющиеся инструменты

BS 7799:3 (платный)

Категории данных (процессы)

- Внешне направленные:
  - Продажи и маркетинг
  - Производство и операции
  - Обслуживание клиентов

- Внутренние:
  - Управление персоналом
  - Исследование и развитие
  - Администрирование и ИТ
  - Финансы и учет

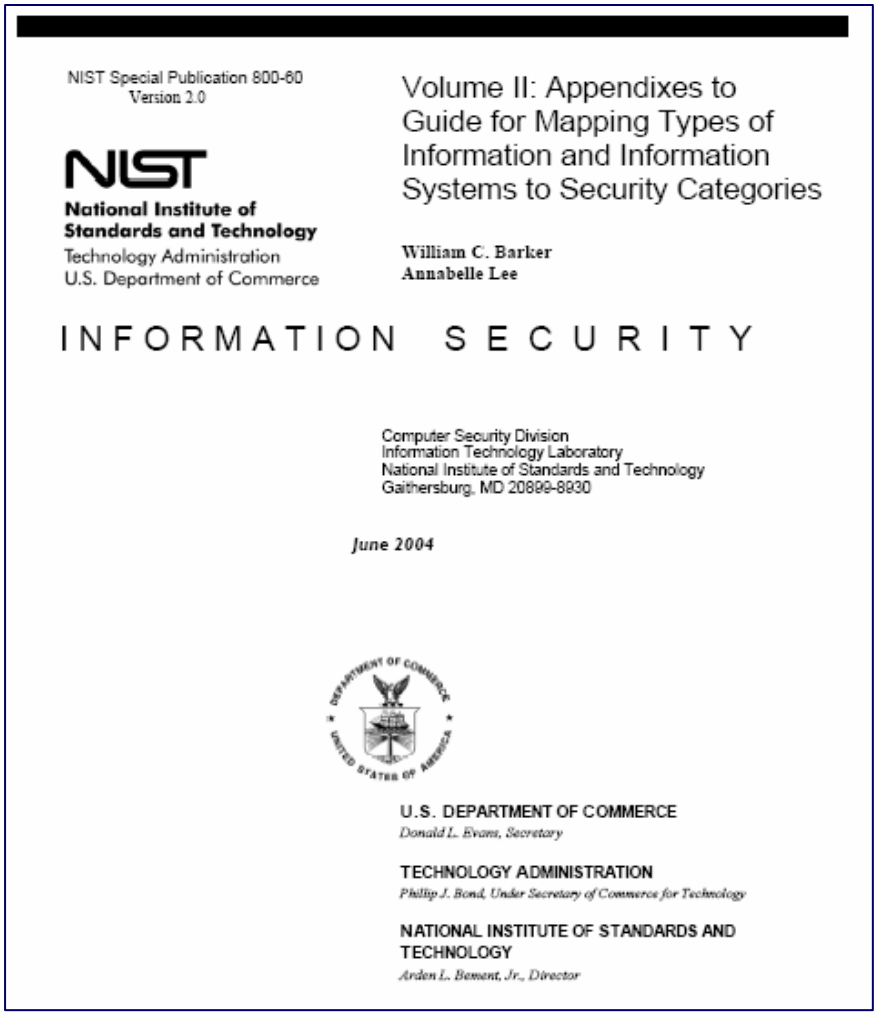


Имеющиеся инструменты

NIST SP 800-60

Соотнесение типов данных:

- Около 60 типов данных
- Описание каждого типа
- Соотнесение по 3 категориям



NIST Special Publication 800-60
Version 2.0

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories

William C. Barker
Annabelle Lee

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Советы по сбору данных

Первый вариант – какие данные в подразделении:

- Создаются
- Хранятся
- Обрабатываются
- Пересылаются
- Уничтожаются

Второй вариант – опора на бизнес-процесс:

- Входящая информация процесса
- Информация, используемая в процессе
- Выходная информация процесса

Дополнительная информация о данных:

– Жизненный цикл данных

– Агрегация данных

– Аналитичность данных

Вспомогательные вопросы по оценке ущерба:

- Что будет, если конкурент сможет ознакомиться с данными?
- Что будет, если злоумышленник изменит данные в свою пользу?
- Что будет, если данные станут недоступны в течении периода времени?

На что обратить внимание

Представители бизнеса склонны:

- Преувеличивать значимость своих данных
- Недооценивать опасность внутреннего злоумышленника

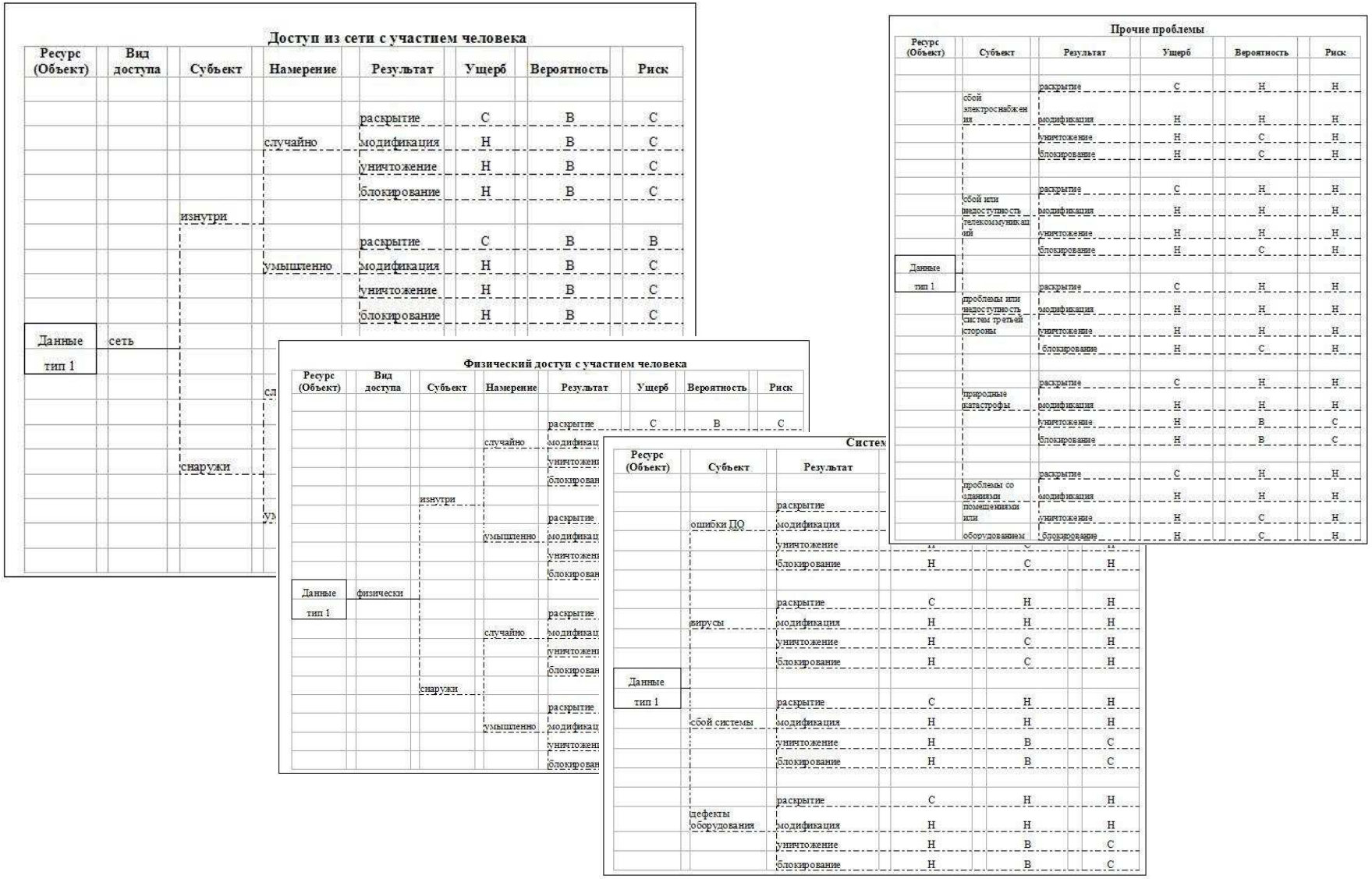
При окончательной оценке учитывать:

- Мнение владельца данных
- Общепринятые практики (в том числе NIST 800-60)
- Собственный экспертный опыт

Дальнейшая работа

- После определения стоимости активов, необходимо сформировать Классификатор данных:
  - Владелец данных
  - Тип данных
  - Категории важности
  - Дополнения (жизненный цикл, агрегация, аналитичность)
- Анализ угроз
  - Стандартная анкета ISO 27001
- При расчете рисков учитывать
  - Остаточные риски
  - Вторичные риски

Отчет (OCTAVE)



Доступ из сети с участием человека

Ресурс (Объект)	Вид доступа	Субъект	Намерение	Результат	Ущерб	Вероятность	Риск
				раскрытие	С	В	С
			случайно	модификация	Н	В	С
				уничтожение	Н	В	С
				блокирование	Н	В	С
		изнутри					
				раскрытие	С	В	В
			умышленно	модификация	Н	В	С
				уничтожение	Н	В	С
				блокирование	Н	В	С
Данные тип 1	сеть						

Физический доступ с участием человека

Ресурс (Объект)	Вид доступа	Субъект	Намерение	Результат	Ущерб	Вероятность	Риск
				раскрытие	С	В	С
			случайно	модификац			
				уничтожени			
				блокирован			
		изнутри					
				раскрытие			
			умышленно	модификац			
				уничтожени			
				блокирован			
Данные тип 1	физически						
				раскрытие			
			случайно	модификац			
				уничтожени			
				блокирован			
		снаружи					
				раскрытие			
			умышленно	модификац			
				уничтожени			
				блокирован			

Систем

Ресурс (Объект)	Субъект	Результат			
		раскрытие			
	ошибки ПО	модификация			
		уничтожение			
		блокирование	Н	С	Н
		раскрытие	С	Н	Н
	вирусы	модификация	Н	Н	Н
		уничтожение	Н	С	Н
		блокирование	Н	С	Н
Данные тип 1					
		раскрытие	С	Н	Н
	сбой системы	модификация	Н	Н	Н
		уничтожение	Н	В	С
		блокирование	Н	В	С
		раскрытие	С	Н	Н
	дефекты оборудования	модификация	Н	Н	Н
		уничтожение	Н	В	С
		блокирование	Н	В	С

Прочие проблемы

Ресурс (Объект)	Субъект	Результат	Ущерб	Вероятность	Риск
		раскрытие	С	Н	Н
	сбой электроснабжения	модификация	Н	Н	Н
		уничтожение	Н	С	Н
		блокирование	Н	С	Н
		раскрытие	С	Н	Н
	сбои или недоступность телекоммуникаций	модификация	Н	Н	Н
		уничтожение	Н	Н	Н
		блокирование	Н	С	Н
Данные тип 1					
		раскрытие	С	Н	Н
	проблемы или недоступность систем третьей стороны	модификация	Н	Н	Н
		уничтожение	Н	Н	Н
		блокирование	Н	С	Н
		раскрытие	С	Н	Н
	природные катастрофы	модификация	Н	Н	Н
		уничтожение	Н	В	С
		блокирование	Н	В	С
		раскрытие	С	Н	Н
	проблемы со зданиями помещениями или	модификация	Н	Н	Н
		уничтожение	Н	С	Н
	оборудованием	блокирование	Н	С	Н

Дополнительные материалы

NIST SP 800-30:

- Руководство по управлению рисками для ИТ систем

Microsoft Solutions for Security, Security Center of Excellence

- Руководство по управлению рисками безопасности

Member of
Deloitte Touche Tohmatsu