Анализ рисков в области защиты информации

153 стр. | PDF | 2009 г.

Данное пособие позволит специалистам освоить лучшие мировые практики управления рисками в организации, приобрести знания практического использования техник оценки рисков и управления ими. В пособии подробно рассматриваются методы минимизации рисков до приемлемого уровня, выбор и использование адекватных инструментов контроля, дается обзор структуры стандартов управления информационной безопасностью. Пособие предназначено для руководителей и специалистов служб информационных технологий, информационной безопасности, управления рисками, внутреннего контроля и аудита, заинтересованных в совершенствовании управления рисками в ИТ и стремящихся к обеспечению защищенности информационных систем и их управляемости.

Введение

1. Анализ рисков в области защиты информации

1.1. Информационная безопасность бизнеса. Обоснование стоимости корпоративной системы защиты информации. Наукоемкий и практический подходы.

1.2. Развитие службы информационной безопасности. Организационная структура TOP-менеджмента компании. Тенденции развития службы ИБ. CISO, его задачи и функции.

1.3. Международная практика защиты информации. Основные этапы работы и требования по обеспечению режима информационной безопасности. Пошаговое определение политики безопасности. Модель Symantec LifeCycle Security.

1.4. Постановка задачи анализа рисков. Пять уровней зрелости компании с точки зрения информационной безопасности. Модель Cartner Group. Модель Carnegie Mellon University. Различные взгляды на защиту информации.

1.5. Национальные особенности защиты информации.Критерии оценки корпоративной системы защиты информации. Особенности отечественных нормативных документов. Учет остаточных рисков.

2. Управление рисками и международные стандарты

2.1. Международный стандарт ISO/IEC 27002:2005.Профессиональный авторский комментарий стандарта, применение методологических схем разбора аспектов организации режима ИБ:

- Политика безопасности и 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.
- Рекомендации по управлению ИБ на предприятии.
- Обзор стандарта ISO/IEC 27002:2005.
- Развитие стандарта ISO 17799

2.2. Германский стандарт BSI «Руководство по защите информационных технологий для базового уровня защищенности». Общая структура документа. Сравнение стандартов ISO 17799 и BSI

2.3. Стандарт США NIST 800-30. Стадии технологии управления информационными рисками. Алгоритм описания ИС. Идентификация угроз и уязвимостей. Формирование списка управляющих воздействий организации. Анализ системы управления ИС. Выбор шкалы для оценки параметров рисков. Анализ возможных последствий нарушения режима ИБ. Оценка рисков. Выработка рекомендаций по управлению рисками.

2.4. Ведомственные и корпоративные стандарты управления ИБ. XBSS – спецификации сервисов безопасности X/Open. Стандарт NASA «Безопасность информационных технологий». Концепция управления рисками MITRE.

3. Технологии анализа рисков

Необходимость адаптации общей методики анализа и управления рисками под конкретные нужды с учетом специфики функционирования предприятия и ведения бизнеса.

3.1. Вопросы анализа и управления рисками.

3.1.1. Идентификация рисков. Составляющие рисков (угрозы и уязвимости), требования к списку, полнота списков – их достоинства и недостатки.

3.1.2. Оценивание рисков. Шкалы и критерии измерения, прямые и косвенные. Ценность информационного ресурса. Объективные и субъективные критерии. Количественные и качественные шкалы. Вероятности.

3.1.3. Измерение рисков. Оценка риска по двум и по трем факторам. Общие идеи, математическое ожидание потерь, зависимости, математические оценки, таблицы уровней уязвимостей.

3.1.4. Технология оценки угроз и уязвимостей. Методы оценки угроз и уязвимостей. Практические сложности в реализации. Пример реализации подхода, основанного на учете различных факторов, используемого в методе CRAMM 4.0 для одного из класса рисков.

3.1.5. Выбор допустимого уровня риска. Затраты на реализацию подсистемы ИБ. Два подхода к выбору допустимого уровня рисков.

3.1.6. Выбор контрмер и оценка их эффективности. Административные, организационные, программно-технические контрмеры. Пример классификатора контрмер. Классы контрмер CRAMM. Ориентировочная эффективность мероприятий по критерию Return of Investment.

3.2. Разработка корпоративной методики анализа рисков

3.2.1. Постановка задачи. Рекомендации по практике защиты. Разработка собственной методики анализа и управления информационными рисками компании. Сценарий анализа, конкретизация шести этапов анализа рисков.

3.2.2. Методы оценивания информационных рисков. План оценки информационных ресурсов компании. Определение характеристик рисков корпоративной ИС и ее ресурсов. Факторы реализации угроз.

3.2.3. Табличные методы оценки рисков. Примеры подобных методов оценивания рисков, которые рекомендованы стандартами и методическими рекомендациями. Ранжирование рисков. Разделение рисков на приемлемые и неприемлемые. Moderate.

3.2.4. Методика анализа рисков Microsoft. В качестве примера корпоративной защиты рассмотрена методика оценки анализа рисков компании Microsoft Стоимости оценки вероятностей, примеры матриц, группировки по областям, идентификации триггеров, контроль и отслеживание рисков.

4. Инструментальные средства анализа рисков

Автоматизация работы специалистов. «Бумажные» методики и специализированное ПО. Инструментарий специалиста.

4.1. Инструментарий базового уровня

4.1.1. Справочные и методические материалы

4.1.2. COBRA Пример программного продукта для анализа и управления рисками, производства C&A Systems Security Ltd. Позволяет представить требования стандартов в виде тематических «вопросников» по отдельным аспектам деятельности организации.

4.1.3. RA Software Tool

4.2. Средства повышенного уровня. Рассматривается несколько методов, которые относятся к нуждам организаций 4 и 5 уровня зрелостей. Программные средства с использованием структурных методов системного анализа и проектирования, относящиеся к категории CASE-средств.

4.2.1. Метод CRAMM. История создания метода, распространенность, концепция, этапы CRAMM

4.2.2. Пример использования CRAMM

4.2.3. Средства компании MethodWare

4.2.4. Экспертная система АванГард

4.2.5. RiskWatch

5. Возможные постановки задач

5.1. Разработка стратегии ИТ-безопасности компании. Результативные документы. Этапность реализации, уровни зрелости системы менеджмента ИБ, уровень доверия бизнеса к службе ИБ, состояние развития отечественных служб ИБ, система принятия решений по управлению ИБ.

5.2. Разработка модели управления рисками ИТ-безопасности. Единая методология управления рисками ИТ-безопасности, сформулированная концепция, реализация внутренних инициатив, пять этапов реализации. Модель ценообразования услуг ИБ, разработка портфеля услуг.

5.3. Подготовка системы управления информационной безопасностью к сертификации ISO 27001. Этап 1 – Оценка текущего состояния СУИБ. Рекомендуемый перечень разрабатываемых документов. Этап 2 – Оценка эффективности внедрения СУИБ. Этап 3 – Инспекции СУИБ.

5.4. Роль CISO в реализации проектов. Функциональные обязанности, востребованность знаний, CISSP, программы обучения

Заключение

Практические рекомендации по разработке и внедрению программ и методик управления информационными рисками. Стандарты и рекомендации, этапы процесса оценки и снижения рисков, расчет риска, OCTAVE-критерии, жизненный цикл управления рисками по MG-2, рекомендации Cobit 4.1

Список дополнительной литературы

Стандарты информационной безопасности

1. ISO/IEC FDIS 27001:2005 (англ.)
2. ISO/IEC FDIS 27001:2005 (перевод на русский язык)
3. BS ISO/IEC 17799:2005 (англ.)
4. ГОСТ Р ИСО/МЭК 27001
5. ГОСТ Р ИСО/МЭК 17799