

Представлены лучшие практики управления киберрисками цифровых предприятий. Введены понятия «система обеспечения кибербезопасности цифрового предприятия» и «корпоративная система управления киберрисками». Раскрыта природа киберрисков предприятий цифровой экономики Российской Федерации. Показана актуальность задачи построения корпоративной системы управления киберрисками цифрового предприятия и особенности ее решения на практике. Рассмотрены основные этапы жизненного цикла управления киберрисками. Показана необходимость автоматизации управления киберрисками. Представлена лучшая практика разработки корпоративной программы управления рисками в условиях роста угроз кибербезопасности. Рассмотрены тенденции и перспективы развития известных методологий управления киберрисками и приведены соответствующие примеры.

Введение

Глава 1. Роль и место управления киберрисками

Глава 2. Сравнительный анализ известных подходов управления рисками

- 2.1. Рекомендации NIST SP 800-30
- 2.2. Рекомендации OCTAVE
- 2.3. Рекомендации MG-2
- 2.4. Рекомендации COBIT
- 2.5. Рекомендации SA-CMM

Глава 3. Природа рисков цифровой экономики Российской Федерации

Глава 4. Роль и место управления киберрисками в системе управления рисками организации

- 4.1. Механизмы, процедуры, цели, задачи и принципы управления рисками
- 4.2. Жизненный цикл управления информационными рисками
- 4.3. Идентификация рисков и оценка их существенности
- 4.4. Ведение отчетности

Глава 5. Аудит системы управления рисками

- 5.1. Особенности жизненного цикла управления киберрисками
- 5.2. Технология оценки угроз и уязвимостей
- 5.3. Классы контрмер CRAMM (фрагмент)

Глава 6. Автоматизация управления рисками

- 6.1. История вопроса
- 6.2. Правила аттестации
- 6.3. Соответствие РСАОВ
- 6.4. Усиление корпоративной финансовой ответственности
- 6.5. Требования Закона Сарбейнса-Оксли, предъявляемые к руководству
 - 6.5.1. Требования к руководству из статьи 302
 - 6.5.2. Меры контроля и процедуры раскрытия информации
 - 6.5.3. Требования к руководству компании из статьи 404
 - 6.5.4. Внутренний контроль финансовой отчетности
 - 6.5.5. Свидетельства аудиторов
 - 6.5.6. Обязанности оценки аудиторов
 - 6.5.7. Основание для достоверной финансовой отчетности
 - 6.5.8. Контроль ИТ – уникальная задача
 - 6.5.9. Меры контроля над системами информационных технологий
 - 6.5.10. Среда контроля ИТ

Глава 7. Разработка корпоративной методик анализа киберрисков

7.1. Этапы и методы

- 7.1.1. Этапы анализа киберрисков
- 7.1.2. Методы оценивания информационных рисков
- 7.1.3. Табличные методы оценки рисков
- 7.1.4. Разделение рисков на приемлемые и не приемлемые

7.2. Пример: методика анализа киберрисков Microsoft

Глава 8. Автоматизация управления киберрисками

- 8.1. Инструментальные средства анализа рисков
- 8.2. Экспертная система АванГард
- 8.3. Система RiskWatch
- 8.4. CYTEGIC

Глава 9. Примеры из лучших практик управления рисками

- 9.1. Оценка субъективной вероятности
- 9.2. Классификация методов получения субъективной вероятности
- 9.3. Методы получения субъективной вероятности
- 9.4. Методы получения оценок непрерывных распределений
 - 9.4.1. Метод изменяющегося интервала
 - 9.4.2. Метод фиксированного интервала
 - 9.4.3. Графический метод
 - 9.4.4. Некоторые рекомендации
- 9.5. Агрегирование субъективных вероятностей
- 9.6. Методы теории полезности
 - 9.6.1. Постановка задачи выбора в условиях риска
 - 9.6.2. Необходимые сведения из теории полезности
 - 9.6.3. Применение методов теории полезности и классификация функций полезности по склонности к риску
 - 9.6.4. Многомерные функции полезности
 - 9.6.5. Методы и порядок построения многомерных функций полезности
 - 9.6.6. Проверка допущений о независимости, вычисление значений констант шкал и проверка согласованности
 - 9.6.7. Некоторые рекомендации
 - 9.6.8. Пример метода оценки рисков
 - 9.6.9. Описание логики работы и способа формирования результатов решения
 - 9.6.10. Метод анализа иерархий

Заключение

Приложение. Оценка киберриска ИТ-сервиса «Электронная почта»

Архитектура ИТ-сервиса «Электронная почта»

Целевая архитектура

Оценка киберрисков

Общая модель ресурсов сервиса

Анализ рисков и сценариев нарушения устойчивости сервиса

Некоррелированные сценарии выхода из строя ресурса

Некоррелированные сценарии выхода из строя сервиса

Коррелированные сценарии