

Оглавление

Предисловие	3
Введение	6
1. Нормативное обеспечение управления рисками информационной безопасности	8
1.1. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ	9
1.2. BS 7799–3:2006 – руководство по управлению рисками ИБ	11
Вопросы для самоконтроля	12
2. Основные определения	13
2.1. Риск ИБ	13
2.2. Управление рисками ИБ	17
2.3. Составляющие процесса управления рисками ИБ	20
2.4. Системный подход к управлению рисками ИБ	27
2.5. Установление контекста управления рисками ИБ	32
2.5.1. Базовые критерии принятия решений по управлению рисками ИБ	33
2.5.2. Область действия и границы управления рисками ИБ	34
2.5.3. Учет требований по ОИБ при управлении рисками ИБ	35
Вопросы для самоконтроля	37
3. Оценка рисков ИБ	38
3.1. Этап 1 – анализ рисков ИБ	41
3.1.1. Подэтап 1 анализа рисков ИБ – идентификация рисков ИБ	42
3.1.2. Шаг 1 подэтапа 1 – идентификация активов	43
3.1.3. Шаг 2 подэтапа 1 – идентификация угроз ИБ	47
3.1.4. Шаг 3 подэтапа 1 – идентификация существующих средств управления рисками ИБ	49
3.1.5. Шаг 4 подэтапа 1 – идентификация уязвимостей	50
3.1.6. Шаг 5 подэтапа 1 – идентификация последствий	52
3.1.7. Подэтап 2 анализа рисков ИБ – количественная оценка рисков ИБ	53
3.1.8. Шаг 1 подэтапа 2 – оценка последствий	55
3.1.9. Шаг 2 подэтапа 2 – оценка вероятностей	60
3.1.10. Шаг 3 подэтапа 2 – определение уровня (величины) рисков ИБ	63
3.2. Этап 2 – оценивание рисков ИБ	66
3.3. Подходы к оценке рисков ИБ	67

3.3.1. Базовый анализ рисков ИБ	70
3.3.2. Неформальный анализ рисков ИБ	72
3.3.3. Детальный анализ рисков ИБ	73
3.3.4. Комбинированный анализ рисков ИБ	75
3.3.5. Высокоуровневая оценка рисков ИБ	75
3.3.6. Детальная оценка рисков ИБ	77
3.3.7. Общий подход к оценке рисков ИБ РС БР ИББС-2.2–2009	84
Вопросы для самоконтроля	89
4. Обработка рисков ИБ	90
4.1. Снижение риска ИБ	93
4.2. Сохранение риска ИБ	95
4.3. Избежание риска ИБ	96
4.4. Передача риска ИБ	96
Вопросы для самоконтроля	98
5. Принятие, коммуникация, мониторинг и пересмотр рисков ИБ	99
5.1. Принятие рисков ИБ	99
5.2. Коммуникация рисков ИБ	100
5.3. Мониторинг и пересмотр рисков ИБ	102
5.3.1. Мониторинг и пересмотр показателей риска ИБ	102
5.3.2. Мониторинг, пересмотр и усовершенствование процесса управления рисками ИБ	103
Вопросы для самоконтроля	104
6. Обеспечение управления рисками ИБ	105
6.1. Документальное обеспечение управления рисками ИБ	105
6.2. Инструментальные средства управления рисками ИБ	107
Вопросы для самоконтроля	109
Заключение	110
Приложения	112
П1. Примеры угроз ИБ	112
П1.1. Физическая безопасность и безопасность окружающей среды	112
П1.2. Управление коммуникациями и операциями	113
П1.3. Аспекты ИБ в управлении непрерывностью бизнеса	114
П1.4. Соответствие	114
П2. Примеры уязвимостей	120
П3. Инструментальные средства управления рисками ИБ	123
Принятые сокращения	125
Список литературы	126