

# Оглавление

Предисловие.....	3
Введение .....	6
1. Нормативное обеспечение проверки и оценки деятельности по управлению иб.....	9
1.1. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – оценка функционирования СУИБ.....	10
1.2. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ.....	12
1.3. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ....	14
1.4. ISO 19011:2002 и ГОСТ Р ИСО 19011–2003 – рекомендации по аудиту систем менеджмента качества и/или окружающей среды .....	16
Выводы.....	17
Вопросы для самоконтроля .....	18
2. Процессы проверки системы управления ИБ.....	19
2.1. Виды проверок СУИБ .....	19
2.2. Мониторинг ИБ .....	22
2.3. Самооценка ИБ .....	31
2.4. Внутренний аудит ИБ .....	36
2.4.1. Цели и задачи внутренних аудитов ИБ.....	38
2.4.2. Организационные принципы внутреннего аудита ИБ .....	39
2.4.3. Принципы обеспечения эффективности внутреннего аудита ИБ .....	40
2.4.4. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации .....	41
2.5. Внешний аудит ИБ.....	43
2.5.1. Принципы проведения внешнего аудита ИБ.....	46
2.5.2. Управление программой внешнего аудита ИБ .....	48
2.5.3. Этапы проведения внешнего аудита ИБ.....	53
2.5.4. Компетентность аудиторов ИБ.....	67
2.5.5. Взаимоотношения представителей аудиторской группы и проверяемых организаций .....	72
2.6. Анализ СУИБ со стороны высшего руководства организации .....	74
2.7. Инструментальные средства проверки ИБ .....	77
Выводы.....	85
Вопросы для самоконтроля .....	86

3. Оценка деятельности по управлению ИБ .....	88
3.1. Оценка эффективности и результативности деятельности по управлению ИБ.....	89
3.2. Измерение, мера измерения, показатель и метрика .....	92
3.2.1. Метрики безопасности .....	96
3.2.2. Измерения, связанные с ИБ .....	108
3.3. Зрелость процессов СУИБ.....	122
3.3.1. Capability Maturity Model .....	125
3.3.2. Модель компании Gartner Group .....	127
3.3.3. Information Security Management Maturity Model.....	128
Выводы.....	131
Вопросы для самоконтроля.....	132
Заключение.....	133
Приложения.....	135
П1. Выдержка из возможной программы аудита вопросов управления непрерывностью бизнеса .....	135
П2. Примеры систем анализа защищенности .....	139
П3. Примеры систем обнаружения и предотвращения вторжений .....	140
П4. Примеры описания конструктивных элементов измерений, связанных с ИБ .....	141
П4.1. Оценка обучения персонала по вопросам СУИБ.....	141
П4.2. Оценка обучения по вопросам ИБ.....	142
П4.3. Качество паролей, генерируемых вручную.....	144
П4.4. Качество паролей, генерируемых автоматизированным образом .....	146
П4.5. Проверка СУИБ .....	148
П4.6. Эффективность управления инцидентами ИБ .....	150
П4.7. Реализация корректирующих действий.....	151
П4.8. Защита от вредоносных программ .....	154
П4.9. Анализ журналов регистрации событий.....	155
П5. Пример описания модели зрелости для подпроцесса минимизации рисков ИБ в рамках процесса управления рисками ИБ .....	156
Принятые сокращения .....	160
Список литературы .....	161