

Оглавление

Предисловие к серии учебных пособий «Вопросы управления информационной безопасностью»	3
Предисловие	8
Введение	11
1. Базовая терминология	13
1.1. Система	13
1.2. Системный подход	15
1.3. Процесс	16
1.4. Процессный подход	18
1.5. Управление	19
1.6. Циклическая модель улучшения процессов	25
1.7. Системный подход к управлению организацией	27
1.8. Процессный подход к управлению организацией	28
1.9. Информационная безопасность	28
Выводы	31
Вопросы для самоконтроля	32
2. Стандартизация систем и процессов управления информационной безопасностью	33
2.1. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности»	34
2.1.1. ISO/IEC 27000:2009 – СУИБ: определения и основные принципы	37
2.1.2. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006 – требования к СУИБ	39
2.1.3. ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799–2005 – практические правила управления ИБ	40
2.1.4. ISO/IEC 27003:2010 – руководство по внедрению СУИБ	42
2.1.5. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – оценка функционирования СУИБ	43
2.1.6. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ	45
2.1.7. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ	48
2.1.8. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ	50

2.1.9. ISO/IEC 27011:2008 – руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002	52
2.1.10. ISO/IEC 27013 – руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001	54
2.1.11. ISO/IEC 27014 – инфраструктура руководства ИБ.....	55
2.1.12. ISO/IEC 27015 – руководство по управлению ИБ для финансовых сервисов.....	56
2.1.13. ISO/IEC 27031:2011 – руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса	57
2.1.14. ISO/IEC 27033 – управление безопасностью сетей	60
2.1.15. ISO/IEC 27035:2011 – управление инцидентами ИБ.....	63
2.1.16. ISO/IEC 27037 – руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.....	65
2.2. Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ	66
2.2.1. ISO/IEC 13335 – методы и средства обеспечения безопасности информационных технологий	66
2.2.2. ISO/IEC 15408 и ISO/IEC 18045:2008 – общие критерии и методология оценки безопасности информационных технологий	69
2.2.3. ISO 19011:2011 и ГОСТ Р ИСО 19011–2003 – рекомендации по аудиту систем менеджмента	71
2.2.4. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса.....	73
2.3. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации	75
2.3.1. СТО БР ИББС-1.0 – общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации	77
2.3.2. СТО БР ИББС-1.1 – аудит ИБ	78
2.3.3. СТО БР ИББС-1.2 – методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0	80
Выводы	81
Вопросы для самоконтроля	82
3. Политика информационной безопасности	84
3.1. Понятия политики обеспечения ИБ и политики ИБ организации.....	84
3.2. Причины выработки политики ИБ.....	92
3.3. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ.....	97

3.4. Содержание политики ИБ.....	102
3.4.1. Содержание корпоративной политики ИБ.....	103
3.4.2. Содержание частных политик ИБ.....	108
3.5. Жизненный цикл политики ИБ.....	111
3.5.1. Разработка политики ИБ.....	114
3.5.2. Внедрение политики ИБ.....	116
3.5.3. Применение политики ИБ.....	118
3.5.4. Аннулирование политики ИБ.....	121
3.6. Ответственность за исполнение политики ИБ.....	121
Выводы.....	126
Вопросы для самоконтроля.....	127
4. Управление и система управления информационной безопасностью.....	128
4.1. Необходимость управления обеспечением ИБ организации.....	128
4.2. Деятельность по обеспечению ИБ организации как процесс.....	130
4.3. Определение управления ИБ организации.....	134
4.4. Управление ИБ информационно-телекоммуникационных технологий организации.....	139
4.5. Система управления ИБ организации.....	143
4.5.1. Область действия СУИБ.....	146
4.5.2. Документальное обеспечение СУИБ.....	149
4.5.3. Политика СУИБ.....	156
4.5.4. Поддержка СУИБ со стороны руководства организации.....	158
4.6. Процессный подход в рамках управления ИБ.....	160
4.6.1. Планирование СУИБ.....	163
4.6.2. Реализация СУИБ.....	167
4.6.3. Проверка СУИБ.....	171
4.6.4. Совершенствование СУИБ.....	172
4.7. Работа с процессами СУИБ организации.....	175
4.7.1. Задание процесса СУИБ.....	177
4.7.2. Идентификация процессов СУИБ организации.....	178
4.7.3. Документирование и описание процесса СУИБ.....	181
4.7.4. Мониторинг и измерение параметров процесса СУИБ.....	183
4.8. Стратегии построения и внедрения СУИБ.....	187
4.8.1. Построение и внедрение СУИБ в целом.....	190
4.8.2. Построение и внедрение процессов СУИБ по отдельности.....	192
Выводы.....	193
Вопросы для самоконтроля.....	193
Заключение.....	196
Приложения.....	199

Примеры частных политик информационной безопасности	199
П1. Политика использования компьютеров интранета.....	199
П2. Политика использования паролей.....	203
П3. Политика использования алгоритмов шифрования	207
П4. Политика антивирусной защиты.....	208
П5. Политика оценки рисков ИБ.....	209
П6. Политика аудита ИБ.....	210
П7. Политика для пограничных маршрутизаторов интранета.....	211
П8. Политика удаленного доступа к интранету	212
П9. Политика построения виртуальных частных сетей.....	214
П10. Политика для экстранета	216
П11. Политика для оборудования пограничной демилитаризованной зоны.....	218
П12. Политика подключения подразделений к интранету	221
П13. Политика подключения к интранету с применением модема	224
П14. Политика работы с конфиденциальной информацией.....	225
П15. Политика для веб-сервера.....	227
П16. Политика отправки электронной почты за пределы интранета	229
П17. Политика хранения сообщений электронной почты.....	230
П18. Политика для межсетевых экранов.....	231
П19. Политика подключения новых устройств к интранету.....	231
Принятые сокращения.....	232
Список литературы	234