

Оглавление

Предисловие	3
Введение	6
1. Нормативное обеспечение управления рисками информационной безопасности	9
1.1. Стандарты, посвященные рискам без указания конкретной предметной области	9
1.1.1. ГОСТ Р 51897–2011/Руководство ИСО 73:2009 — термины и определения в области рисков	10
1.1.2. ГОСТ Р 51901.23–2012 — реестр рисков	12
1.1.3. NIST SP 800-30 — руководство по проведению оценок рисков	19
1.1.4. ГОСТ Р ИСО 31000–2019 — принципы и руководство по управлению рисками	26
1.1.5. ГОСТ Р 58771–2019 — технологии оценки рисков	32
1.2. Документы, посвященные рискам информационной безопасности	52
1.2.1. PC BP ИВВС-2.2–2009 — управление рисками нарушения ИБ для организации банковской системы	53
1.2.2. NIST SP 800-39 — управление рисками ИБ с точки зрения организации миссии и информационных систем	56
1.2.3. ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001–2006 — риск-ориентированный подход к управлению ИБ	60
1.2.4. BS 7799–3:2017 — руководство по управлению рисками ИБ	63
1.2.5. NIST SP 800-37 — инфраструктура управления рисками для информационных систем и организаций для обеспечения безопасности	65
1.2.6. ISO/IEC 27005:2018 и ГОСТ Р ИСО/МЭК 27005–2010 — управление рисками	70
Вопросы для самоконтроля	74
2. Основные определения	76
2.1. Риск нарушения ИБ, или риск ИБ	76
2.2. Управление рисками ИБ	81
2.3. Составляющие процесса управления рисками ИБ	85

2.4. Системный подход к управлению рисками ИБ	91
2.5. Установление контекста управления рисками ИБ	96
2.5.1. Базовые критерии принятия решений по управлению рисками ИБ	97
2.5.2. Область действия и границы управления рисками ИБ	99
Вопросы для самоконтроля	100
3. Оценка рисков информационной безопасности	101
3.1. Подходы к оценке рисков ИБ	102
3.1.1. Комбинированная, высокоуровневая и детальная оценка рисков ИБ	104
3.1.2. Базовая оценка рисков ИБ	110
3.1.3. Подход к оценке рисков ИБ РС ВР ИВВС-2.2–2009 ...	112
3.2. Этапы оценки рисков ИБ	121
3.3. Этап 1 — анализ рисков ИБ	124
3.3.1. Подэтап 1 анализа рисков ИБ — идентификация рисков ИБ	129
3.3.2. Шаг 1 подэтапа 1 — идентификация активов	132
3.3.3. Шаг 2 подэтапа 1 — идентификация угроз ИБ	137
3.3.4. Шаг 3 подэтапа 1 — идентификация мер ОИБ	140
3.3.5. Шаг 4 подэтапа 1 — идентификация уязвимостей	144
3.3.6. Шаг 5 подэтапа 1 — идентификация последствий	147
3.3.7. Подэтап 2 анализа рисков ИБ — количественная оценка рисков ИБ	149
3.3.8. Шаг 1 подэтапа 2 — оценка последствий	149
3.3.9. Шаг 2 подэтапа 2 — оценка вероятностей	155
3.3.10. Шаг 3 подэтапа 2 — определение уровня (величины) рисков ИБ	159
3.4. Этап 2 — оценивание рисков ИБ	169
Вопросы для самоконтроля	171
4. Обработка рисков ИБ	173
4.1. Снижение риска ИБ	177
4.2. Сохранение риска ИБ	180
4.3. Предотвращение риска ИБ	181
4.4. Перенос риска ИБ	182
Вопросы для самоконтроля	183
5. Принятие, коммуникация, мониторинг и переоценка рисков ИБ	185
5.1. Принятие рисков ИБ	185
5.2. Коммуникация и консультирование в области рисков ИБ	186
5.3. Мониторинг и переоценка рисков ИБ	188
5.3.1. Мониторинг и переоценка факторов риска ИБ	189

5.3.2. Мониторинг, анализ и улучшение процесса управления рисками ИБ	190
Вопросы для самоконтроля	192
6. Обеспечение управления рисками ИБ	193
6.1. Кадровое обеспечение управления рисками ИБ	193
6.2. Документальное обеспечение управления рисками ИБ ..	194
6.3. Инструментальные средства управления рисками ИБ ..	200
Вопросы для самоконтроля	205
Заключение	206
Глоссарий	208
Приложение. Инструментальные средства управления рисками ИБ	217
Принятые сокращения	219
Литература	220