

УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ



УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Горячая линия-Телеком



Н.Г. МИЛОСЛАВСКАЯ
А.И. ТОЛСТОЙ

4-е издание

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 51897-2021/Руководство ИСО 73:2009 — термины и определения в области рисков	10
1.1.2. ГОСТ Р 51901.23-02012 — реестр рисков	12
1.1.3. NIST SP 800-30 — руководство по проведению оценок рисков	20
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	33
1.2. Документы, посвященные рискам информационной безопасности	55
1.2.1. РС ВР ИБВС-2.2-2009 — управление рисками нарушения ИБ для организаций банковской системы	56
1.2.2. NIST SP 800-39 — управление рисками ИБ с точки зрения организации, миссии и информационных систем ...	59
1.2.3. ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 — риск-ориентированный подход к управлению ИБ	64
1.2.4. BS 7799-3:2017 — руководство по управлению рисками ИБ	69
1.2.5. NIST SP 800-37 — инфраструктура управления рисками для информационных систем и организаций для обеспечения безопасности	72
1.2.6. ГОСТ Р 57580.3-2022 — управление рисками реализации информационных угроз	77
1.2.7. ISO/IEC 27005:2022 и ГОСТ Р ИСО/МЭК 27005-2010 — управление рисками ИБ	81
Вопросы для самоконтроля	87

2. Основные определения	88
2.1. Риск нарушения ИБ, или риск ИБ	88
2.2. Управление рисками ИБ	95
2.3. Составляющие процесса управления рисками ИБ	99
2.4. Системный подход к управлению рисками ИБ	107
2.5. Установление контекста управления рисками ИБ	112
2.5.1. Базовые критерии принятия решений по управлению рисками ИБ	115
2.5.2. Область действия и границы управления рисками ИБ	122
Вопросы для самоконтроля	123
3. Оценка рисков ИБ	124
3.1. Подходы к оценке рисков ИБ	126
3.1.1. Комбинированная, высокоуровневая и детальная оценка рисков ИБ	129
3.1.2. Базовая оценка рисков ИБ	136
3.1.3. Подход к оценке рисков ИБ РС ВР ИБВС-2.2-2009 ..	138
3.2. Этапы оценки рисков ИБ	147
3.3. Этап 1 — анализ рисков ИБ	151
3.3.1. Подэтап 1 анализа рисков ИБ — идентификация рис- ков ИБ	157
3.3.2. Шаг 1 подэтапа 1 — идентификация активов	164
3.3.3. Шаг 2 подэтапа 1 — идентификация угроз ИБ	170
3.3.4. Шаг 3 подэтапа 1 — идентификация мер ОИБ	174
3.3.5. Шаг 4 подэтапа 1 — идентификация уязвимостей	181
3.3.6. Шаг 5 подэтапа 1 — идентификация последствий	185
3.3.7. Подэтап 2 анализа рисков ИБ — количественная оцен- ка рисков ИБ	187
3.3.8. Шаг 1 подэтапа 2 — оценка последствий	188
3.3.9. Шаг 2 подэтапа 2 — оценка вероятностей/правдопо- добности	197
3.3.10. Шаг 3 подэтапа 2 — определение уровня (величины) рисков ИБ	205
3.4. Этап 2 — оценивание рисков ИБ	221
Вопросы для самоконтроля	224
4. Обработка рисков ИБ	226
4.1. Снижение риска ИБ	235

4.2. Сохранение риска ИБ	239
4.3. Предотвращение риска ИБ	240
4.4. Перенос риска ИБ	241
Вопросы для самоконтроля	243
5. Принятие, коммуникация, мониторинг и переоценка рисков ИБ	244
5.1. Принятие рисков ИБ	244
5.2. Информирование (коммуникация) и консультирование в области рисков ИБ	245
5.3. Мониторинг и переоценка рисков ИБ	249
5.3.1. Мониторинг и переоценка факторов риска ИБ	250
5.3.2. Пересмотр, коррекция и постоянное улучшение процесса управления рисками ИБ	254
Вопросы для самоконтроля	257
6. Обеспечение управления рисками ИБ	258
6.1. Кадровое обеспечение управления рисками ИБ	258
6.2. Документальное обеспечение управления рисками ИБ	259
6.3. Инструментальные средства управления рисками ИБ	269
Вопросы для самоконтроля	273
Принятые сокращения	275
Глоссарий	276
Литература	286