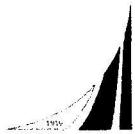
НАУЧНАЯ МЫСЛЬ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ

А.В. Царегородцев,
С.В. Романовский, С.Д. Волков

АНАЛИЗ РИСКОВ В ПРОЦЕССАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЖИЗНЕННОГО ЦИКЛА ФИНАНСОВЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

НАУЧНАЯ МЫСЛЬ
СЕРИЯ ОСНОВАНА В 2008 ГОДУ



ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

А.В. ЦАРЕГОРОДЦЕВ
С.В. РОМАНОВСКИЙ
С.Д. ВОЛКОВ

АНАЛИЗ РИСКОВ В ПРОЦЕССАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЖИЗНЕННОГО ЦИКЛА ФИНАНСОВЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

МОНОГРАФИЯ

znanium.com
электронно-библиотечная система

Москва
ИНФРА-М
2024

УДК 004.056+658.15(075.4)
ББК 16.8:65стд1-93-21
Ц18

Рецензенты:
А.С. Марков, доктор технических наук, профессор, почетный работник науки и высоких технологий Российской Федерации, профессор кафедры ИУ-8 «Информационная безопасность» Московского государственного технического университета имени Н.Э. Баумана, президент группы компаний «Эшелон»;
А.К. Жарова, доктор юридических наук, доцент, старший научный сотрудник Института государства и права Российской академии наук, директор Центра исследований киберпространства факультета права, доцент Департамента стратегического и международного менеджмента Высшей школы бизнеса Национального исследовательского университета «Высшая школа экономики»

Царегородцев А.В.

Ц18 Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем : монография / А.В. Царегородцев, С.В. Романовский, С.Д. Волков. — Москва : ИНФРА-М, 2024. — 198 с. – (Научная мысль). — DOI 10.12737/2049718.

ISBN 978-5-16-018719-8 (print)
ISBN 978-5-16-111637-1 (online)

Одним из ключевых элементов стратегии развития современной организации является решение задачи трансформации системы управления рисками информационной безопасности. Сегодня все чаще современные организации отходят от модели, основанной на зрелости, в пользу подхода, основанного на оценке рисков. В монографии рассматривается данный подход и даются рекомендации по его применению в организациях кредитно-финансовой сферы.

Может представлять интерес как для сотрудников подразделений, деятельность которых связана с анализом и управлением рисками, организаций кредитно-финансовой сферы, так и для преподавателей, студентов и аспирантов, обучающихся по направлениям подготовки и специальностям, относящимся к укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

УДК 004.056+658.15(075.4)
ББК 16.8:65стд1-93-21

ISBN 978-5-16-018719-8 (print)
ISBN 978-5-16-111637-1 (online)

Оглавление

Введение **3**

Глава 1. Обзор практик управления рисками ИБ **8**

1.1. NIST Risk Management Framework 11
1.2. NIST SP 800-39 11
1.3. NIST SP 800-37 12
1.4. NIST SP 800-30 13
1.5. NIST SP 800-137 14
1.6. Стандарт ISO/IEC 27005 15
1.7. Стандарт IEC 31010 15

Глава 2. Ключевые аспекты корпоративного управления рисками ИБ **17**

2.1. Роль оценки рисков в системе корпоративного управления 17
2.2. Корпоративное управление рисками 30
2.3. Внутренний контроль 31
2.4. Внедрение процессов управления рисками 31
2.5. Система управления рисками 31
2.6. Политика управления рисками 33
2.7. Состав процесса управления рисками 34
2.8. Источники риска 35

Глава 3. Процесс управления рисками **36**

3.1. Анализ организации 39
3.2. Процессная модель 41
3.3. Цели процесса анализа организации 41
3.4. Описание процесса управления рисками 42
3.4.1. Входы процесса 42
3.4.2. Выходы процесса 46
3.5. Ограничения процесса управления рисками 46
3.6. Финансовые показатели процесса управления рисками 47
3.7. Диагностика процесса управления рисками 49
3.7.1. Трудности внедрения системы управления рисками 49
3.7.2. Модель зрелости процессов управления рисками 50
3.7.3. SWOT-анализ 51
3.7.4. PEST-анализ 54

Глава 4. Особенности процесса идентификации рисков **58**

4.1. Таксономия рисков 63
4.2. База данных рисков 65
4.3. Аудит риска 65
4.4. Реестр рисков 66

Глава 5. Ключевые компоненты процесса управления рисками информационной безопасности 68

5.1. Причинно-следственный анализ 68
5.2. Анализ Парето 71
5.3. Определение методик и критериев оценки рисков информационной безопасности 72
5.3.1. Определение методик и критериев расчета вероятности реализации угроз ИБ 72
5.3.2. Определение критериев приемлемости рисков ИБ 73
5.3.3. Определение критериев принятия решения о способе обработки рисков ИБ 74
5.4. Идентификация и оценка активов 75
5.5. Оценка рисков ИБ 78
5.5.1. Идентификация угроз ИБ 78
5.5.2. Идентификация владельцев риска ИБ 79
5.5.3. Выбор мер управления риском ИБ 80
5.5.4. Определение вероятности реализации угроз ИБ 80
5.5.5. Определение уровня ущерба от реализации угрозы ИБ 80
5.5.6. Определение уровня риска ИБ 81
5.5.7. Формирование отчета по результатам оценки рисков ИБ 81
5.6. Обработка рисков ИБ 82
5.6.1. Выбор способа обработки рисков ИБ 82
5.6.2. Выбор мероприятий по обработке рисков ИБ 83
5.6.3. Приоритизация мероприятий по обработке рисков ИБ 84
5.6.4. Формирование плана обработки рисков ИБ 85
5.7. Коммуникации в отношении рисков ИБ 85

Глава 6. Мониторинг рисков информационной безопасности 87

6.1. Ключевые индикаторы рисков ИБ 87
6.2. Разработка и пересмотр ключевых индикаторов риска ИБ 90
6.2.1. Формирование целей мониторинга индикаторов риска ИБ 91
6.2.2. Определение области мониторинга индикаторов риска ИБ 93
6.2.3. Определение интервала мониторинга индикаторов риска ИБ 94
6.2.4. Определение метода измерений индикаторов риска ИБ 95
6.2.5. Разработка функций измерений индикаторов риска ИБ 97
6.2.6. Формирование пороговых значений индикаторов риска ИБ 98
6.3. Мониторинг индикаторов риска ИБ 100
6.3.1. Произведение измерений и вычислений 100
6.3.2. Оценка получившихся результатов 101
6.3.3. Запись результатов и отчетность 102

Глава 7. Обеспечение информационной безопасности в процессах реализации жизненного цикла АИС 103

7.1. Обеспечение ИБ в процессе разработки ТЗ 104
7.2. Обеспечение ИБ в процессе проектирования АИС 105
7.3. Обеспечение ИБ в процессе разработки и тестирования АИС 105

7.4. Обеспечение ИБ в процессе ввода в эксплуатацию АИС 106
7.5. Обеспечение ИБ в процессе эксплуатации АИС 107
7.6. Обеспечение ИБ в процессе сопровождения и модернизации АИС 109
7.7. Обеспечение ИБ в процессе снятия с эксплуатации АИС 109

Глава 8. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем 110

8.1. Концепция анализа рисков обеспечения информационной безопасности АИС 111
8.2. Качественные и количественные подходы к анализу рисков обеспечения информационной безопасности АИС 114
8.3. Анализ ключевых методов оценки рисков обеспечения информационной безопасности АИС 123

Заключение 132

Приложения 134

Приложение 1. Основные термины и определения 134
Приложение 2. Пример матрицы распределения ущерба 145
Приложение 3. Пример анкеты риска 149
Приложение 4. Пример структуры реестра рисков 154
Приложение 5. Пример модели зрелости процессов СУР 158
Приложение 6. Пример рекомендаций к проведению контроля исходного кода компонент АИС 162
Приложение 7. Пример содержания работ по тестированию на проникновение компонент АИС 167
Приложение 8. Пример содержания работ по выявлению ошибок конфигурации АИС 175
Приложение 9. Пример формата паспорта ключевого индикатора риска ИБ 177

Список использованной литературы 189