

Предисловие автора ко второму изданию

написано Александр Астахов | 10 июня, 2023

Вторая редакция книги «Искусство управления информационными рисками» называется по другому и существенно превосходит первую редакцию по объему.

Теперь книга называется **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ как искусство управления рисками»**. Необходимость смены вывести связана с тем, что в магазинах эту книгу нельзя было найти в разделе ЗАЩИТА ИНФОРМАЦИИ, а помещали ее куда угодно: в бизнес-литературу, стратегический и риск-менеджмент, экономические аспекты информатики и др.

В книгу внесено много добавлений и исправлений, в том числе:

1. Отныне речь идет о возможности реализации угрозы (threat likelihood), а не о вероятности (threat probability). Воспоминания о школьной теории вероятности не должны более вводить читателя в заблуждение при использовании формул количественной оценки риска.
2. В книге дается определение новой структуры данных под названием «профиль риска» и приводятся примеры профилей риска для различных типов организаций и информационных систем. Использование шаблонных профилей риска значительно упрощает процессы управления рисками в каждой конкретной организации и позволяет осуществлять стандартизацию данной области по схеме принятой в международном стандарте ISO 15408 (Общие критерии оценки безопасности информационных технологий).
3. В книге дается краткий обзор стандартов международных управления рисками общего назначения (ISO 31000, 31010), чтобы показать, что управления рисками ИБ осуществляется в общем контексте управления бизнес-рисками и основано на тех же самых общих принципах риск менеджмента.

4. В соответствии с международным стандартом ISO 31010 описываются 39 методов оценки риска (Дельфи, Монте-Карло, мозговой штурм и пр.), из которых 31 метод стандартизирован, а 8 – реально применяются на практике.
5. Интеграция риск-менеджмента в процессы управления организацией (стратегический менеджмент, управление изменениями, проектами, инцидентами, обучением и т.д.). Для наглядности добавлены схемы, иллюстрирующие взаимосвязи между этими процессами управления.
6. Признаки улучшенного менеджмента риска.
7. Дается методика измерения эффективности системы риск-менеджмента в соответствии со стандартом ISO 27004.
8. Также в книгу было внесено множество других дополнений и корректировок.

Эти добавления сначала были сделаны в блоге автора по адресу <http://iso27000.ru/blogi/aleksandr-astahov>, затем переносились в электронную редакцию книги <http://анализ-риска.рф>, а затем в печатную редакцию, которая выходит как на русском, так и на английском языках.