

УДК 65.012.8  
ББК 65.290.4с51  
А65

Под общей редакцией А.П. Курило  
Руководитель проекта по маркетингу и рекламе М.Г. Ручкина

**Андреанов В.В.**

А65 Обеспечение информационной безопасности бизнеса / В. В. Андреанов, С. Л. Зефилов, В. Б. Голованов, Н. А. Голдуев. — 2-е изд., перераб. и доп. — М.: Альпина Паблишерз, 2011. — 373 с.

ISBN 978-5-9614-1364-9

Данную книгу можно назвать практической энциклопедией. В ней дан максимальный охват проблематики обеспечения информационной безопасности, начиная с современных подходов, обзора нормативного обеспечения в мире и в России и заканчивая рассмотрением конкретных направлений обеспечения информационной безопасности (обеспечение ИБ периметра, противодействие атакам, мониторинг ИБ, виртуальные частные сети и многие другие), конкретных аппаратно-программных решений в данной области. Книга будет полезна бизнес-руководителям компаний и тем, в чью компетенцию входит решение технических вопросов обеспечения информационной безопасности.

УДК 65.012.8  
ББК 65.290.4с51

*Все права защищены. Никакая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, включая размещение в сети Интернет и в корпоративных сетях, а также запись в память ЭВМ для частного или публичного использования, без письменного разрешения владельца авторских прав. По вопросу организации доступа к электронной библиотеке издательства обращайтесь по адресу [lib@alpinabook.ru](mailto:lib@alpinabook.ru).*

© ООО «Центр исследований  
платежных систем и расчетов», 2010  
© ООО «Альпина», 2010

ISBN 978-5-9614-1364-9

# Содержание

Предисловие А. А. Стрельцова.....	7
Предисловие С. П. Расторгуева .....	11
Введение.....	17
<b>1. Философия информационной безопасности бизнеса.....</b>	<b>25</b>
1.1. Бизнес и информация .....	25
1.1.1. Информационная сущность бизнеса .....	25
1.1.2. Информационные характеристики бизнеса .....	27
1.1.3. Уязвимости процессов накопления знаний (самообучения) .....	29
1.1.4. Определение информационной безопасности .....	33
1.2. Материальные и нематериальные (информационные) аспекты бизнеса.....	34
1.2.1. Общая структура информационной сферы. Связь с материальным миром .....	34
1.2.2. Правовая среда бизнеса и ее свойства .....	40
1.2.3. Учредительная и лицензионная база организации .....	41
1.2.4. Отражение материального мира.....	41
1.2.5. Внутренняя нормативная база организации .....	44
1.2.6. Информационная сфера — главный источник рисков бизнеса .....	46
1.3. Модель информационной безопасности бизнеса.....	49
1.3.1. Мотивация.....	49
1.3.2. Риски, рисковые события, ущербы и уязвимости. Полезные для построения моделей свойства .....	52
1.3.3. Обобщенная модель распределения ресурсов организации в условиях рисков .....	54

1.3.4.	Ущербы и негативные последствия.....	57
1.3.5.	Риск-ориентированный подход к обеспечению ИБ.....	60
1.3.6.	Модель с изменением цели.....	65
1.3.7.	Об идентификации событий ИБ.....	66
1.3.8.	Предварительный анализ.....	71
1.3.9.	Накопление знаний.....	72
1.3.10.	Интерпретация характеристик риска для управления ИБ.....	75
1.3.11.	Общая модель обеспечения ИБ бизнеса.....	78
1.3.12.	Проблемы практической реализации модели обеспечения ИБ организации.....	82

<b>2.</b>	<b>Существующие модели менеджмента (управления), применимые для обеспечения информационной безопасности бизнеса.....</b>	<b>87</b>
2.1.	Модели непрерывного совершенствования.....	87
2.1.1.	Модели непрерывного совершенствования и корпоративное управление.....	87
2.1.2.	Вопросы реализации моделей непрерывного совершенствования и процессного подхода в организации.....	95
2.1.3.	Модели непрерывного совершенствования и международные стандарты.....	102
2.2.	Стандартизированные модели менеджмента. Аспекты контроля и совершенствования. Интеграция.....	105
2.2.1.	Стандартизированные модели менеджмента в системе корпоративного управления.....	105
2.2.2.	Универсальные требования к стандартам на системы менеджмента.....	115
2.2.3.	Шаги реализации стандартной СМИБ организации.....	121
2.2.4.	Реализация моделей менеджмента в целевых задачах организации («частные менеджменты»).....	139
2.3.	Модели COSO, COBIT, ITIL.....	144
2.4.	Контроль и аудит (оценки, измерения) в моделях менеджмента (управления).....	159

### 3. Оценка информационной безопасности бизнеса.

#### Проблема измерения и оценивания

информационной безопасности бизнеса.....	169
3.1. Способы оценки информационной безопасности .....	169
3.2. Процесс оценки информационной безопасности .....	173
3.2.1. Основные элементы процесса оценки.....	173
3.2.2. Контекст оценки информационной безопасности организации.....	174
3.2.3. Мероприятия и выходные данные процесса оценки.....	178
3.2.4. Способы измерения атрибутов объекта оценки .....	190
3.3. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности .....	197
3.3.1. Модель оценки информационной безопасности на основе оценки процессов.....	197
3.3.2. Оценка информационной безопасности на основе модели зрелости процессов .....	204
3.4. Риск-ориентированная оценка информационной безопасности .....	210

### 4. Проблема персонала в задачах обеспечения информационной безопасности бизнеса .....

4.1. Общие сведения .....	215
4.1.1. Тенденции.....	215
4.1.2. Термины и определения .....	217
4.1.3. Общая характеристика угроз .....	220
4.1.4. Примеры инцидентов.....	223
4.2. Формализованное представление угроз ИБ от персонала.....	234
4.2.1. Цели моделирования угроз .....	234
4.2.2. Типология инцидентов .....	235
4.2.3. Факторная модель.....	240
4.2.4. Некоторые модели угроз.....	273
4.2.5. Внешние сообщники внутреннего злоумышленника .....	275
4.2.6. Типология мотивов .....	277
4.2.7. Сговор .....	278

4.2.8.	Деятельность внутреннего злоумышленника с точки зрения формальных полномочий.....	278
	Управление идентификационными данными и доступом (IBM Восточная Европа/Азия) .....	279
4.3.	Противодействие угрозам ИБ от персонала .....	291
4.3.1.	Общий подход к противодействию.....	291
4.3.2.	Обеспечение осведомленности персонала в области ИБ .....	293
4.3.3.	Получение информации от сотрудников организации.....	293
4.3.4.	Организационные аспекты .....	294
4.3.5.	Скрытность противодействия .....	294
4.3.6.	Управление системой ролей.....	295
4.3.7.	Программно-технические средства защиты от утечек информации.....	310
4.3.8.	Расследование инцидентов.....	310
4.3.9.	Раскрытие информации об инцидентах.....	312
1.	Приложение .....	315
	Архитектура стандартов защиты информации и обеспечения информационной безопасности .....	315
	Общие сведения .....	315
2.	Приложение .....	331
	Подходы к формированию нормативного обеспечения системы информационной безопасности организации .....	331
	Обзор современных средств управления доступом (ЗАО «Инфосистема Джет»).....	346
3.	Приложение (справочное) .....	351
	Примеры метрик для измерения атрибутов.....	351
4.	Приложение .....	361
	ЗАО «ЕС-лизинг» .....	361
5.	Приложение .....	367
	Монитор TopCM .....	367
	Список литературы .....	369
	Участники проекта	
	«Обеспечение информационной безопасности бизнеса».....	372