

УДК 002.6
ББК 65.050.2
А91

Астахов, Александр Михайлович.

А91 Искусство управления информационными рисками [Электронный ресурс] / А. М. Астахов. — 2-е изд. (эл.). — Электрон. текстовые дан. (1 файл pdf : 314 с.). — М. : ДМК Пресс, 2018. — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10".

ISBN 978-5-93700-032-3

В книге подробно излагается системный подход к управлению информационными рисками, основанный на эффективной авторской методологии, многократно проверенной на практике в российских компаниях и полностью совместимой с международными стандартами. Из этой книги вы узнаете:

- как разобраться с информационными активами, угрозами, уязвимостями, механизмами контроля, требованиями безопасности и рисками, а также определить, каким образом все это влияет на бизнес;
- как реализовать на практике риск-ориентированный подход к обеспечению информационной безопасности, построив сбалансированную систему управления рисками;
- как анализировать и оценивать информационные риски бизнеса, успешно справляясь с возникающими при этом трудностями; как оценивать и управлять возвратом инвестиций в информационную безопасность;
- как отличить реальные угрозы от мнимых, а также что такое глобальные информационный кризис и почему он уже не за горами.

Книга ориентирована прежде всего на специалистов по информационной безопасности, ИТ специалистов и риск-менеджеров. Она будет также полезна руководителям компаний, менеджерам всех уровней, имеющим отношение к подготовке и принятию решений по рискам, аудиторам, а также широкому кругу читателей, интересующихся вопросами управления рисками, информационными технологиями и связанными с ними угрозами. Глубина и обстоятельность изложения материала позволяет использовать книгу в качестве учебного пособия для высших учебных заведений и послевузовского образования.

УДК 002.6
ББК 65.050.2

Деривативное электронное издание на основе печатного издания: Искусство управления информационными рисками / А. М. Астахов. — М. : ДМК Пресс, 2010. — 312 с. — ISBN 978-5-94074-574-7.

В соответствии со ст. 1299 и 1301 ГК РФ при устранении ограничений, установленных техническими средствами защиты авторских прав, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации.

ISBN 978-5-93700-032-3

© ООО «ГлобалТраст Солюшинс», 2010
© ДМК Пресс, 2010

СОДЕРЖАНИЕ

ОБ АВТОРЕ	9
ПРЕДИСЛОВИЕ	11
ПРЕДИСЛОВИЕ АВТОРА.....	12
ВВЕДЕНИЕ	14
Новые правила игры в новом информационном веке	14
О чем эта книга?	15
Существуют ли альтернативы управлению рисками?	17
Почему управление рисками является самым важным вопросом информационной безопасности?	18
Для кого написана эта книга?	18
Общая структура изложения материала	19
 Глава 1. ПРЕДПОСЫЛКИ ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ	 22
Риски, породившие мировой финансовый кризис	23
Информационные риски киберпространства	25
Кибертерроризм	26
Риски промышленных систем	30
Риски утечки информации	38
Точка зрения правоохранительных органов на киберугрозы	41
Риски электронных расчетов	43
Обилие стандартов, требований, средств и технологий защиты не уменьшает риски	46

Государственное регулирование только создает дополнительные риски	49
Оценка рисков как основа корпоративного управления	52
Как оценивают риски наши соотечественники?	54
Вопросы к размышлению	56

Глава 2. ОСНОВНЫЕ ЭЛЕМЕНТЫ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

58

Стандарты в области управления рисками информационной безопасности	58
Понятие риска	62
Оценка риска	64
Количественное определение величины риска	65
Качественное определение величины риска	67
Информационная составляющая бизнес-рисков	69
Активы организации как ключевые факторы риска	71
Подходы к управлению рисками	73
Уровни зрелости бизнеса в отношении рисков	76
Анализ факторов риска	77
Вопросы к размышлению	78

Глава 3. СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

80

О преимуществах системного подхода к управлению рисками	80
Структура документации по управлению рисками	85
Политика и контекст управления рисками	87
Структура системы управления рисками	91
Процессная модель управления рисками	91
Непрерывная деятельность по управлению рисками	96
Сопровождение и мониторинг механизмов безопасности	96
Анализ со стороны руководства	97
Пересмотр и переоценка риска	98
Взаимосвязь процессов аудита и управления рисками	98
Управление документами и записями	99
Корректирующие и превентивные меры	100
Коммуникация рисков	101

Аутсорсинг процессов управления рисками	102
Распределение ответственности за управление рисками	103
Требования к риск-менеджеру	106
Требования к эксперту по оценке рисков	106
Вопросы к размышлению	107

Глава 4. ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Идентификация активов	108
Описание бизнес-процессов	110
Идентификация требований безопасности	119
Реестр требований безопасности	120
Контрактные обязательства	131
Требования бизнеса	132
Определение ценности активов	133
Критерии оценки ущерба	135
Таблица ценности активов	137
Особенности интервьюирования бизнес-пользователей	138
Определение приоритетов аварийного восстановления	141
Анализ угроз и уязвимостей	147
Профиль и жизненный цикл угрозы	147
Задание № 1. Описание угроз безопасности	150
Способы классификации угроз	150
Уязвимости информационной безопасности	153
Идентификация организационных уязвимостей	154
Идентификация технических уязвимостей	158
Оценка угроз и уязвимостей	164
Определение величины риска	168
Калибровка шкалы оценки риска	170
Пример оценки риска	171
Отчет об оценке рисков	173
Задание № 2. Калибровка шкалы оценки риска	175

Глава 5. ОБРАБОТКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Процесс обработки рисков	176
Обработка рисков информационной безопасности	177

Способы обработки риска	179
Принятие риска	180
Уменьшение риска	182
Передача риска	185
Избежание риска	186
Оценка возврата инвестиций в информационную безопасность	187
Принятие решения по обработке риска	190
План обработки рисков	192
Декларация о применимости механизмов контроля	194

Глава 6. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ДЛЯ УПРАВЛЕНИЯ РИСКАМИ

197

Нужен ли для управления рисками специальный программный инструментарий?	197
Выбор инструментария для оценки рисков	200
Общие недостатки и ограничения коммерческих программных продуктов	201
Обзор методов и инструментальных средств управления рисками ...	202
OCTAVE	202
CRAMM	205
RiskWatch	208
COBRA	216
RA2 the art of risk	227
vsRisk	220
Callio Secura 17799	222
Proteus Enterprise	230

ВМЕСТО ЗАКЛЮЧЕНИЯ – ПРАКТИЧЕСКИЕ СОВЕТЫ ПО ВНЕДРЕНИЮ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

232

Документация	232
Начальные условия для внедрения СУИР	233
Организационная структура управления рисками	234
Обучение членов экспертной группы	235
Реализация пилотного проекта по оценке рисков	235
Проведение полной оценки рисков по всем активам	236
Жизненный цикл управления рисками	237

БИБЛИОГРАФИЯ	238
ПОЛЕЗНЫЕ ССЫЛКИ	240
Приложение № 0. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ	241
Приложение № 1. ВЗАИМОСВЯЗЬ МЕЖДУ СТАНДАРТАМИ ISO/IEC 27001:2005, BS 7799-3:2006 И ISO/IEC 27005:2008	244
Приложение № 2. АНТОЛОГИЯ КИБЕРАТАК	247
Приложение № 3. НАИХУДШИЕ СЦЕНАРИИ КИБЕРАТАК	249
Приложение № 4. БАЗОВЫЙ ОПРОСНИК ДЛЯ ОПРЕДЕЛЕНИЯ СТЕПЕНИ КРИТИЧНОСТИ СИСТЕМ ПО МЕТОДУ SRAMM	252
Приложение № 5. ПЕРЕЧЕНЬ ТИПОВЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	254
Приложение № 6. ПЕРЕЧЕНЬ ТИПОВЫХ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	260
Приложение № 7. ОПРОСНЫЙ ЛИСТ ДЛЯ ОЦЕНКИ УГРОЗ ПО МЕТОДУ SRAMM	263
Приложение № 8. ОПРОСНЫЙ ЛИСТ ДЛЯ ОЦЕНКИ УЯЗВИМОСТЕЙ ПО МЕТОДУ SRAMM	279
Приложение № 9. ЗАКОНОДАТЕЛЬНЫЕ И НОРМАТИВНЫЕ АКТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ	293
Приложение № 10. ПРОГРАММНЫЕ ПРОДУКТЫ ДЛЯ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	298
Приложение № 11. КОМПЛЕКТ ТИПОВЫХ ДОКУМЕНТОВ ДЛЯ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	299

Приложение № 12. РУССКИЕ РЕДАКЦИИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	302
Приложение № 13. ИНФОРМАЦИЯ О КОМПАНИИ GLOBALTRUST	304
Приложение № 14. УСЛУГИ GLOBALTRUST В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	307
Приложение № 15. МАСТЕР-КЛАСС ПО УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	308
ISO27000.RU – ИСКУССТВО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	310