

УДК 004.056.5
ББК 32.973.202
ПЗ0

Петренко, Сергей Анатольевич.

ПЗ0 Управление информационными рисками. Экономически оправданная безопасность [Электронный ресурс] / С. А. Петренко, С. В. Симонов. — 2-е изд. (эл.). — Электрон. текстовые дан. (1 файл pdf : 396 с.). — М. : ДМК Пресс, 2018. — (Информационные технологии для инженеров). — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10".

ISBN 978-5-93700-058-3

В книге подробно рассмотрены возможные постановки задач анализа информационных рисков и управления ими при организации режима информационной безопасности в отечественных компаниях. Рассмотрена международная концепция обеспечения информационной безопасности, а также различные подходы и рекомендации по решению задач анализа рисков и управления ими. Дан обзор основных стандартов в области защиты информации и управления рисками: ISO 17799, ISO 15408, BSI, NIST, MITRE.

В настоящем издании обсуждаются инструментальные средства для анализа рисков (COBRA, CRAMM, MethodWare, RiskWatch, Авангард). Даны рекомендации по использованию указанных средств на практике для анализа рисков информационных систем. Показана взаимосвязь задач анализа защищенности и обнаружения вторжений с задачей управления рисками. Предложены технологии оценки эффективности обеспечения информационной безопасности в отечественных компаниях.

Книга будет полезна руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), внутренним и внешним аудиторам (CISA), менеджерам высшего эшелона компаний, занимающимся оценкой информационных рисков компании и их управлением, а также студентам и аспирантам соответствующих технических специальностей.

УДК 004.056.5
ББК 32.973.202

Деривативное электронное издание на основе печатного издания: Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. — М. : ДМК Пресс, 2004. — 384 с. — ISBN 5-94074-246-7.

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 978-5-93700-058-3

© ДМК Пресс, 2004

СОДЕРЖАНИЕ

Предисловие	10
--------------------------	----

Глава 1

Анализ рисков в области защиты информации	15
1.1. Информационная безопасность бизнеса	15
1.2. Развитие службы информационной безопасности	19
1.3. Международная практика защиты информации	22
1.3.1. Модель <i>Symantec LifeCycle Security</i>	27
1.4. Постановка задачи анализа рисков	30
1.4.1. Модель <i>Gartner Group</i>	30
1.4.2. Модель <i>Carnegie Mellon University</i>	30
1.4.3. Различные взгляды на защиту информации	36
1.5. Национальные особенности защиты информации	38
1.5.1. Особенности отечественных нормативных документов	38
1.5.2. Учет остаточных рисков	40

Глава 2

Управление рисками и международные стандарты	43
2.1. Международный стандарт ISO 17799	44
2.1.1. Обзор стандарта <i>BS 7799</i>	44
2.1.2. Развитие стандарта <i>ISO 17799</i>	54
2.2. Германский стандарт BSI	57
2.2.1. Сравнение стандартов <i>ISO 17799</i> и <i>BSI</i>	60
2.3. Стандарт США NIST 800-30	60
2.3.1. Алгоритм описания информационной системы	62
2.3.2. Идентификация угроз и уязвимостей	63
2.3.3. Организация защиты информации	65
2.4. Ведомственные и корпоративные стандарты управления ИБ	68
2.4.1. <i>XBSS</i> -спецификации сервисов безопасности <i>X/Open</i>	68
2.4.2. Стандарт NASA «Безопасность информационных технологий»	73
2.4.3. Концепция управления рисками <i>MITRE</i>	73

Глава 3

Технологии анализа рисков	75
3.1. Вопросы анализа рисков и управления ими	75
3.1.1. Идентификация рисков	75
3.1.2. Оценивание рисков	76
3.1.3. Измерение рисков	78
3.1.4. Выбор допустимого уровня риска	87
3.1.5. Выбор контрмер и оценка их эффективности	88
3.2. Разработка корпоративной методики анализа рисков	91
3.2.1. Постановка задачи	91
3.2.2. Методы оценивания информационных рисков	93
3.2.3. Табличные методы оценки рисков	94
3.2.4. Методика анализа рисков Microsoft	98

Глава 4

Инструментальные средства анализа рисков	101
4.1. Инструментарий базового уровня	101
4.1.1. Справочные и методические материалы	102
4.1.2. COBRA	103
4.1.3. RA Software Tool	104
4.2. Средства полного анализа рисков	105
4.2.1. Метод CRAMM	105
4.2.2. Пример использования метода CRAMM	108
4.2.3. Средства компании MethodWare	117
4.2.4. Экспертная система «АванГард»	120
4.2.5. RiskWatch	129

Глава 5

Аудит безопасности и анализ рисков	135
5.1. Актуальность аудита безопасности	135
5.2. Основные понятия и определения	138
5.3. Аудит безопасности в соответствии с BS 7799, часть 2	141
5.3.1. Сертификация и аудит: организационные аспекты	141
5.3.2. Методика проведения аудита	142
5.3.3. Варианты аудита безопасности	143
5.3.4. Организация проведения аудита	146
5.4. Аудит информационной системы:	
рекомендации COBIT 3rd Edition	147
5.4.1. Этапы проведения аудита	151
5.4.2. Пример аудита системы расчета зарплаты	155

Глава 6

Анализ защищенности информационной системы	161
6.1. Исходные данные	162
6.1.1. Анализ конфигурации средств защиты внешнего периметра ЛВС	163
6.1.2. Методы тестирования системы защиты	164
6.2. Средства анализа защищенности	164
6.2.1. Спецификации <i>Security Benchmarks</i>	166
6.2.2. Спецификация <i>Windows 2000 Security Benchmark</i>	167
6.3. Возможности сетевых сканеров	169
6.3.1. Сканер <i>Symantec NetRecon</i>	171
6.3.2. Сканер <i>NESSUS</i>	174
6.4. Средства контроля защищенности системного уровня	177
6.4.1. Система <i>Symantec Enterprise Security Manager</i>	178
6.5. Перспективы развития	187

Глава 7

Обнаружение атак и управление рисками	189
7.1. Сетевые атаки	190
7.2. Обнаружение атак как метод управления рисками	192
7.2.1. Оценка серьезности сетевой атаки	193
7.3. Ограничения межсетевых экранов	194
7.4. Анализ подозрительного трафика	195
7.4.1. Сигнатуры как основной механизм выявления атак	195
7.4.2. Анализ сетевого трафика и анализ контента	196
7.4.3. Пример анализа подозрительного трафика	197
7.5. IDS как средство управления рисками	202
7.5.1. Типовая архитектура системы выявления атак	202
7.5.2. Стандарты, определяющие правила взаимодействия между компонентами системы выявления атак	203
7.5.3. Форматы обмена данными	204
7.5.4. CVE – тезаурус уязвимостей	204
7.5.5. CIDF	205
7.5.6. Рабочая группа IDWG	206
7.6. Возможности коммерческих IDS	208
7.6.1. Средства защиты информации компании <i>Symantec</i>	208
7.6.2. <i>Symantec Intruder Alert</i>	208
7.6.3. Пример использования <i>Symantec IDS</i>	214
7.7. Тенденции развития	216

Приложение 1

Исследование состояния информационной

безопасности в мире	217
Введение	217
Нарушения системы ИБ	219
Вовлечение высшего руководства	221
<i>Степень вовлечения высшего руководства</i>	<i>222</i>
Формальные критерии оценки функционирования системы ИБ	224
<i>Изменение эффективности работы системы ИБ</i>	<i>225</i>
Контроль и регистрация инцидентов в области ИБ	226
<i>Меры воздействия на нарушителей ИБ</i>	<i>227</i>
Программа внедрения ИБ	228
<i>Численность персонала службы ИБ</i>	<i>228</i>
<i>Квалификация персонала службы ИБ</i>	<i>229</i>
<i>Независимость службы информационной безопасности от ИТ</i>	<i>230</i>
Политика в области ИБ	230
<i>Области, охваченные политикой ИБ</i>	<i>233</i>
Управление ИБ	234
<i>Делегирование функций ИБ внешним организациям</i>	<i>234</i>
<i>Тестируют ли компании надежность системы ИБ?</i>	<i>236</i>
Управление персоналом	237
<i>Осведомленность в вопросах безопасности</i>	
<i>за пределами организации</i>	<i>238</i>
<i>Кампании по повышению осведомленности в вопросах ИБ</i>	<i>239</i>
Защита технологической инфраструктуры	
и обеспечение непрерывности ведения бизнеса	239
<i>Внедрение инфраструктуры открытых ключей (PKI)</i>	<i>239</i>
<i>Беспроводные сети</i>	<i>240</i>
<i>Защита портативных устройств</i>	<i>241</i>
<i>Идентификация пользователей</i>	<i>242</i>
<i>Удаленный доступ к корпоративным системам</i>	<i>242</i>
<i>Парольная защита</i>	<i>243</i>
<i>Система обнаружения вторжений (IDS)</i>	<i>244</i>
<i>Отчетность о нарушениях</i>	<i>245</i>

Приложение 2

Международное исследование

по вопросам информационной безопасности	247
Цифры и факты	247
Путеводитель по исследованию	247
Резюме исследования	248
<i>Насколько вы уверены в своем предприятии</i>	<i>249</i>
Управление безопасностью	250
<i>Результаты исследования</i>	<i>250</i>
<i>Что это может означать для вашего предприятия</i>	<i>251</i>
<i>Что может предпринять руководство</i>	<i>252</i>
<i>Что можно сделать</i>	<i>253</i>
Как используется система информационной безопасности	254
<i>Результаты исследования</i>	<i>255</i>
<i>К каким последствиям для вашей компании это может привести</i>	<i>256</i>
<i>Что можно сделать</i>	<i>258</i>
Доступность информационных технологий	259
<i>Выводы</i>	<i>259</i>
<i>Что это может означать для вашей компании</i>	<i>260</i>
<i>Что вы можете сделать</i>	<i>260</i>
Что в будущем	262
<i>Выводы</i>	<i>262</i>
<i>Что это может означать для вашей компании</i>	<i>262</i>
<i>Что вы можете сделать</i>	<i>263</i>
Что делать дальше	264
Методология проведения исследования	265
<i>«Эрнст энд Янг» – решение реальных проблем</i>	<i>265</i>

Приложение 3

Основные понятия и определения управления рисками	267
Терминология и определения в публикациях на русском языке	267
Терминология и определения на английском языке	
(определения взяты из глоссария [334] и даются в переводе)	268

Приложение 4

Каталоги угроз и контрмер IT Baseline	273
Каталоги угроз и контрмер, используемые в Германском стандарте IT Baseline Protection Manual	273
<i>Каталог угроз</i>	<i>273</i>
<i>Каталог контрмер</i>	<i>281</i>

Приложение 5

Классификация ресурсов, угроз и контрмер CRAMM	299
Классификация ресурсов, угроз и контрмер в методе CRAMM для профиля Commercial.	
Классификация физических ресурсов	299
Классы угроз	302
Классы контрмер	303

Приложение 6

Оценка рисков экспертными методами	305
Оценка субъективной вероятности	305
<i>Классификация методов получения субъективной вероятности</i>	<i>306</i>
<i>Методы получения субъективной вероятности</i>	<i>307</i>
Методы оценок непрерывных распределений	308
<i>Метод изменяющегося интервала</i>	<i>308</i>
<i>Метод фиксированного интервала</i>	<i>309</i>
<i>Графический метод</i>	<i>310</i>
<i>Некоторые рекомендации</i>	<i>310</i>
Агрегирование субъективных вероятностей	311
<i>Методы теории полезности</i>	<i>312</i>
<i>Необходимые сведения из теории полезности</i>	<i>313</i>
<i>Применение методов теории полезности</i>	<i>313</i>
<i>Классификация функций полезности по склонности к риску</i>	<i>314</i>
Многомерные функции полезности	314
<i>Методы построения многомерных функций полезности</i>	<i>315</i>
<i>Метод анализа иерархий</i>	<i>322</i>

Приложение 7

Оценка затрат (ТСО) на информационную безопасность	323
История вопроса	323
Западный опыт – на вооружение	325
<i>Оценка текущего уровня ТСО</i>	<i>327</i>
<i>Аудит ИБ компании</i>	<i>327</i>

Формирование целевой модели ТСО	328
Пример оценки затрат на ИБ	328
Специфика расчета ТСО в российских условиях	334
Примерный перечень затрат на безопасность	336
Затраты на ИБ и уровень достигаемой защищенности	340
Доля затрат на ИБ в обороте компании	342
Определение объема затрат	344
База измерений	348
Анализ затрат на ИБ	351
Отчет по затратам на безопасность	351
Анализ затрат	353
Принятие решений	355
Внедрение системы учета затрат на ИБ	356
Резюме	356
Заключение	357
Литература	360
Предметный указатель	382