

УДК 004.056.5
ББК 32.973.202
ПЗ0

Петренко, Сергей Анатольевич.

ПЗ0 Политики безопасности компании при работе в Интернет [Электронный ресурс] / С. А. Петренко, В. А. Курбатов. — 3-е изд. (эл.). — Электрон. текстовые дан. (1 файл pdf : 397 с.). — М. : ДМК Пресс, 2018. — (Информационные технологии для инженеров). — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10".

ISBN 978-5-93700-057-6

Книга является первым полным русскоязычным практическим руководством по вопросам разработки политик информационной безопасности в отечественных компаниях и организациях и отличается от других источников, преимущественно изданных за рубежом, тем, что в ней последовательно изложены все основные идеи, методы и способы практического решения вопросов разработки, внедрения и поддержки политик безопасности в различных российских государственных и коммерческих структурах.

Книга может быть полезна руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), ответственным за утверждение политик безопасности и организацию режима информационной безопасности; внутренним и внешним аудиторам (CISA); менеджерам высшего эшелона управления компаний (ТОР- менеджерам), которым приходится разрабатывать и внедрять политики безопасности в компании; администраторам безопасности, системным и сетевым администраторам, администраторам БД, которые отвечают за соблюдение правил безопасности в отечественных корпоративных информационных системах. Книга также может использоваться в качестве учебного пособия студентами и аспирантами соответствующих технических специальностей.

УДК 004.056.5
ББК 32.973.202

Деривативное электронное издание на основе печатного издания: Политики безопасности компании при работе в Интернет / С. А. Петренко, В. А. Курбатов. — 2-е изд. — М. : ДМК Пресс, 2011. — (Информационные технологии для инженеров). — 400 с. — ISBN 978-5-94074-728-4.

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 978-5-93700-057-6

©ДМК Пресс, 2011

ОГЛАВЛЕНИЕ

| | |
|---|-----------|
| Предисловие | 7 |
| Глава 1 | |
| Актуальность политик безопасности компании | 13 |
| 1.1. Анализ отечественного рынка средств защиты информации | 13 |
| 1.1.1. Средства управления обновлениями | 15 |
| 1.1.2. Средства межсетевого экранирования | 15 |
| 1.1.3. Средства построения VPN | 16 |
| 1.1.4. Средства контроля доступа | 16 |
| 1.1.5. Средства обнаружения вторжений и аномалий | 18 |
| 1.1.6. Средства резервного копирования и архивирования | 18 |
| 1.1.7. Средства централизованного управления безопасностью | 18 |
| 1.1.8. Средства предотвращения вторжений на уровне серверов | 19 |
| 1.1.9. Средства мониторинга безопасности | 19 |
| 1.1.10. Средства контроля деятельности сотрудников в Интернете | 20 |
| 1.1.11. Средства анализа содержимого почтовых сообщений | 21 |
| 1.1.12. Средства анализа защищенности | 21 |
| 1.1.13. Средства защиты от спама | 23 |
| 1.1.14. Средства защиты от атак класса «отказ в обслуживании» | 23 |
| 1.1.15. Средства контроля целостности | 24 |
| 1.1.16. Средства инфраструктуры открытых ключей | 24 |
| 1.1.17. Средства усиленной аутентификации | 24 |
| 1.2. Характеристика зрелости технологий защиты информации | 25 |
| 1.3. Основные причины создания политик безопасности | 28 |
| 1.4. Как разработать политики безопасности? | 32 |
| 1.4.1. Кому и что доверять | 33 |
| 1.4.2. Трудности внедрения политик безопасности | 33 |
| 1.4.3. Кто заинтересован в политиках безопасности? | 34 |
| 1.4.4. Состав группы по разработке политик безопасности | 34 |
| 1.4.5. Процесс разработки политик безопасности | 35 |
| 1.4.6. Основные требования к политике безопасности | 35 |
| 1.4.7. Уровень средств безопасности | 35 |
| 1.4.8. Примеры политик безопасности | 35 |
| 1.4.9. Процедуры безопасности | 38 |
| 1.5. Возможные постановки задачи | 39 |
| 1.5.1. Metallургическая компания | 39 |
| 1.5.2. Коммерческий банк | 42 |
| 1.5.3. Субъект РФ | 48 |
| 1.6. Российская специфика разработки политик безопасности | 50 |

Глава 2

| | |
|--|-----|
| Лучшие практики создания политик безопасности | 57 |
| 2.1. Подход компании IBM | 57 |
| 2.1.1. Структура документов безопасности | 58 |
| 2.1.2. Пример стандарта безопасности для ОС семейства UNIX | 61 |
| 2.2. Подход компании Sun Microsystems | 67 |
| 2.2.1. Структура политики безопасности | 67 |
| 2.2.2. Пример политики безопасности | 73 |
| 2.3. Подход компании Cisco Systems | 78 |
| 2.3.1. Описание политики безопасности | 78 |
| 2.3.2. Пример политики сетевой безопасности | 84 |
| 2.4. Подход компании Microsoft | 91 |
| 2.5. Подход компании Symantec | 95 |
| 2.5.1. Описание политики безопасности | 96 |
| 2.6. Подход SANS | 99 |
| 2.6.1. Описание политики безопасности | 99 |
| 2.6.2. Пример политики аудита безопасности | 100 |

Глава 3

Рекомендации международных стандартов

| | |
|--|-----|
| по созданию политик безопасности | 103 |
| 3.1. Стандарты ISO/IEC 17799:2005 (BS 7799-1:2002) | 103 |
| 3.2. Международный стандарт ISO 15408 | 135 |
| 3.3. Германский стандарт BSI | 141 |
| 3.4. Стандарт CobiT | 143 |
| 3.5. Общие рекомендации по созданию политик безопасности | 148 |
| 3.6. Проблемы разработки политик безопасности | 152 |
| 3.7. Обзор возможностей современных систем управления политиками безопасности | 155 |
| 3.7.1. Bindview Policy Operations Center | 157 |
| 3.7.2. Zequel Technologies DynamicPolicy | 158 |
| 3.7.3. NetIQ VigilEnt Policy Center | 159 |
| 3.8. Отечественная специфика разработки политик безопасности | 165 |

Глава 4

| | |
|---|-----|
| Реализация политик безопасности | 169 |
| 4.1. Задание общих правил безопасности | 169 |
| 4.2. Архитектура корпоративной системы защиты информации | 171 |
| 4.2.1. Зона подключения к Интернету | 173 |
| 4.2.2. Зона доступа к Web-приложениям компании | 175 |
| 4.2.3. Зона выхода в Интернет | 176 |
| 4.2.4. Зона управления ресурсами сети компании | 179 |
| 4.2.5. Зона защищаемых данных компании | 185 |
| 4.2.6. Зона внутренней сети компании | 186 |

| | |
|--|-----|
| 4.3. Настройки основных компонент системы защиты компании | 188 |
| 4.3.1. Настройки пограничных маршрутизаторов | 188 |
| 4.3.2. Сервисы маршрутизатора | 190 |
| 4.3.3. Настройки внешних межсетевых экранов | 197 |
| 4.3.4. Настройки VPN | 212 |
| 4.3.5. Настройки внутренних межсетевых экранов | 213 |
| 4.3.6. Настройка корпоративной системы защиты от вирусов | 228 |
| 4.4. Дальнейшие шаги по совершенствованию правил безопасности | 231 |
| Приложение 1 | |
| Оценка состояния информационной безопасности в США | 233 |
| Приложение 2 | |
| Международный опрос 2003 года по информационной безопасности. | |
| Обзор результатов по странам СНГ | 249 |
| Приложение 3 | |
| Руководство по информационной безопасности предприятия | |
| (Site Security Handbook, RFC 1244) | 265 |
| Выработка официальной политики предприятия в области информационной безопасности | 265 |
| Выработка процедур для предупреждения нарушений безопасности | 277 |
| Типы процедур безопасности | 291 |
| Реакция на нарушение безопасности | 295 |
| Выработка мер, предпринимаемых после нарушения | 305 |
| Приложение 4 | |
| Политики безопасности, рекомендуемые SANS | 309 |
| 1. Политика допустимого шифрования | 309 |
| 2. Политика допустимого использования | 310 |
| 3. Руководство по антивирусной защите | 314 |
| 4. Политика хранения электронной почты | 315 |
| 5. Политика использования электронной почты компании | 317 |
| 6. Политика использования паролей | 318 |
| 7. Политика оценки рисков | 321 |
| 8. Политика безопасности маршрутизатора | 322 |
| 9. Политика обеспечения безопасности серверов | 323 |
| 10. Политика виртуальных частных сетей | 326 |
| 11. Политика беспроводного доступа в сеть компании | 327 |
| 12. Политика автоматического перенаправления электронной почты компании | 328 |

| | |
|--|-----|
| 13. Политика классификации информации | 329 |
| 14. Политика в отношении паролей для доступа к базам данных | 334 |
| 15. Политика безопасности лаборатории демитилизированной зоны | 336 |
| 16. Политика безопасности внутренней лаборатории | 339 |
| 17. Политика экстранета | 343 |
| 18. Политика этики | 344 |
| 19. Политика лаборатории антивирусной защиты | 346 |

Приложение 5

Оценка экономической эффективности затрат

| | |
|---|-----|
| на защиту информации | 348 |
| 1. Оценка затрат на защиту информации | 348 |
| 2. Обоснование инвестиций в информационную безопасность | 373 |

Приложение 6

Примеры методических материалов по

| | |
|---|-----|
| информационной безопасности | 383 |
| Инструкция администратору безопасности сети | 383 |
| Инструкция администратору Web-сервера сети | 385 |
| Инструкция пользователю Интернет/интранет-технологий сети | 386 |

Приложение 7

| | |
|---|-----|
| Перечень законодательных актов по защите информации | 390 |
| Нормативно-правовые акты | 390 |
| Федеральные законы | 390 |
| Указы Президента РФ | 391 |
| Постановления Правительства РФ | 391 |
| ГОСТ и Руководящие документы Гостехкомиссии (ФСТЭК) | 392 |