

И. Г. Милославская

НАУЧНЫЕ ОСНОВЫ ПОСТРОЕНИЯ ЦЕНТРОВ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ В ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ



Оглавление

Введение	3
1. Анализ текущего состояния обеспечения информационной безопасности информационно-телекоммуникационных сетей	16
1.1. Анализ информационно-телекоммуникационной сети как основного объекта защиты в едином информационном пространстве организаций	16
1.1.1. Особенности современного использования информационно-телекоммуникационных сетей	16
1.1.2. Определение информационно-телекоммуникационной сети	18
1.1.3. Информационно-телекоммуникационная сеть как симбиоз телекоммуникационной и информационной сетей	20
1.1.4. Информационные ресурсы информационно-телекоммуникационной сети и среда их обработки	22
1.1.5. Логическая структура информационно-телекоммуникационной сети	25
1.1.6. Информационно-телекоммуникационная сеть как системообразующая структура единого информационного пространства организации	26
1.2. Современные проблемы защиты информации в информационно-телекоммуникационных сетях	28
1.2.1. Тенденция возрастания угроз информационной безопасности для информационно-телекоммуникационных сетей	28
1.2.2. Задачи обеспечения информационной безопасности для информационно-телекоммуникационных сетей	31
1.2.3. Эволюция технологий и средств обеспечения сетевой безопасности	37
1.2.4. Необходимость сложной аналитики данных для обеспечения сетевой безопасности	44
1.2.5. Понятие сетевой безопасности для информационно-телекоммуникационной сети	46
1.3. Нормативная и правовая база в области обеспечения информационной безопасности, применимая к объекту исследования и использованная для разработки глоссария предметной области исследования	48
1.3.1. Правовая база исследования	48

1.3.2. Нормативная база исследования	49
Выводы по главе 1	53
2. Таксономия уязвимостей, угроз, сетевых атак и инцидентов информационной безопасности для информационно-телекоммуникационных сетей	57
2.1. Таксономия понятий уязвимости, угроз, сетевых атак и инцидентов информационной безопасности	57
2.2. Системная классификация уязвимостей элементов информационно-телекоммуникационной сети	60
2.3. Системная классификация угроз информационной безопасности информационно-телекоммуникационной сети	73
2.4. Системная классификация сетевых атак на информационно-телекоммуникационную сеть	88
2.5. Системная классификация инцидентов информационной безопасности для информационно-телекоммуникационной сети	110
Выводы по главе 2	122
3. Исследование и разработка процессов обеспечения информационной и сетевой безопасности информационно-телекоммуникационных сетей	129
3.1. Понятие обеспечения информационной безопасности информационно-телекоммуникационной сети	129
3.1.1. Понятие процесса и процессного подхода к деятельности организации	130
3.1.2. Определение понятия обеспечения информационной безопасности информационно-телекоммуникационной сети	132
3.1.3. Модель обеспечения информационной безопасности информационно-телекоммуникационной сети	135
3.1.4. Определение понятия обеспечения сетевой безопасности информационно-телекоммуникационной сети	141
3.2. Управление информационной безопасностью информационно-телекоммуникационной сети как часть обеспечения ее информационной безопасности	142
3.2.1. Определение понятия управления информационной безопасностью информационно-телекоммуникационной сети	144
3.2.2. Уровни управления информационной безопасностью информационно-телекоммуникационной сети	144
3.2.3. Система управления информационной безопасностью информационно-телекоммуникационной сети	148
3.2.4. Циклическая модель рассмотрения процессов управления информационной безопасностью информационно-телекоммуникационной сети	149

3.2.5. Определение понятия управления сетевой безопасностью информационно-телеkomмуникационной сети	153
3.3. Проверка информационной безопасности информационно-телеkomмуникационной сети как средство постоянно-го контроля общего управления информационной безопасностью организаций	153
3.3.1. Определение понятия мониторинга информационной безопасности информационно-телеkomмуникационной сети	155
3.3.2. Взаимосвязь процессов мониторинга и аудита информационной безопасности информационно-телеkomмуникационной сети	160
3.3.3. Взаимосвязь процессов мониторинга и управления инцидентами информационной безопасности в информационно-телеkomмуникационной сети	162
3.4. Разработка процесса управления инцидентами информационной безопасности для информационно-телеkomмуникационной сети	163
3.4.1. Задачи процесса управления инцидентами информационной безопасности	163
3.4.2. Нормативная база управления инцидентами информационной безопасности	164
3.4.3. Деятельность в рамках процесса управления инцидентами информационной безопасности	166
3.4.4. Требования к разрабатываемому процессу управления инцидентами информационной безопасности	173
3.4.5. Формализация разработанного процесса управления инцидентами информационной безопасности	175
3.4.6. Разрабатываемый Центр интеллектуального управления сетевой безопасностью как фундамент системы управления инцидентами информационной безопасности для информационно-телеkomмуникационной сети	207
Выводы по главе 3	209
4. Критический анализ существующих Центров и выработка требований к Центрам интеллектуального управления сетевой безопасностью	213
4.1. Понятие <i>SIEM</i> -системы	214
4.2. Эволюция Центров управления безопасностью	221
4.3. Центры мониторинга безопасности	222
4.3.1. Цели и задачи Центров мониторинга безопасности	222
4.3.2. Функции <i>SIEM</i> -системы 1.0 в Центрах мониторинга безопасности	226
4.3.3. Классификация Центров мониторинга безопасности	228
4.3.4. Ограниченность Центров мониторинга безопасности	228
4.4. Концепция интеллектуальной безопасности	234

4.5. Центры интеллектуальной безопасности	242
4.5.1. Назначение Центров интеллектуальной безопасности	242
4.5.2. Расширение бизнес-логики функционирования Центров мониторинга безопасности для ее применения в Центрах интеллектуальной безопасности	243
4.5.3. SIEM-системы 2.0 в Центрах интеллектуальной безопасности	246
4.6. Модели зрелости Центров управления безопасностью	250
4.7. Формулирование требований к разрабатываемому Центру интеллектуального управления сетевой безопасностью	253
4.7.1. Общие требования к Центру интеллектуального управления сетевой безопасностью	254
4.7.2. Специальные требования к Центру интеллектуального управления сетевой безопасностью	255
4.7.3. Перечень детальных требований к Центру интеллектуального управления сетевой безопасностью	257
4.7.4. Требования по обеспечению информационной безопасности Центра интеллектуального управления сетевой безопасностью	259
Выводы по главе 4	261
5. Построение типового Центра интеллектуального управления сетевой безопасностью для информационно-телецоммуникационной сети организации	265
5.1. Методология построения типового Центра интеллектуального управления сетевой безопасностью	266
5.2. Принципы построения типового Центра интеллектуального управления сетевой безопасностью	273
5.3. Типовой Центр интеллектуального управления сетевой безопасностью как объединение Центра интеллектуальной безопасности и Сетевого операционного центра	276
5.3.1. Сетевой операционный центр	277
5.3.2. Функциональные возможности объединенного типового Центра интеллектуального управления сетевой безопасностью	280
5.3.3. Визуализация информации в типовом Центре интеллектуального управления сетевой безопасностью для принятия решений по управлению инцидентами информационной безопасности в информационно-телецоммуникационной сети	284
5.4. Архитектура типового Центра интеллектуального управления сетевой безопасностью	287
5.4.1. Функциональная архитектура типового Центра интеллектуального управления сетевой безопасностью	287

5.4.2. Архитектура обработки относящихся к информационной безопасности информационно-телекоммуникационных сетей данных в типовом Центре интеллектуального управления сетевой безопасностью.....	289
5.4.3. Зональная архитектура обеспечения информационной безопасности в типовом Центре интеллектуального управления сетевой безопасностью.....	304
5.5. Проект SIEM-системы 3.0 для типового Центра интеллектуального управления сетевой безопасностью	318
5.6. Функциональная устойчивость типового Центра интеллектуального управления сетевой безопасностью в едином информационном пространстве организации	332
5.7. Вопросы кадрового обеспечение типового Центра интеллектуального управления сетевой безопасностью	343
5.8. Демонстрация выполнения требований к типовому Центру интеллектуального управления сетевой безопасностью	353
Выводы по главе 5	361
Заключение	368
Список сокращений и условных обозначений	380
Словарь терминов	383
Литература	405