



ТЕОРИЯ СЕТЕВЫХ ВОЙН

#11

КИБЕР- БЕЗОПАСНОСТЬ: УПРАВЛЕНИЕ СЕТЕВЫМИ РИСКАМИ



ОГЛАВЛЕНИЕ

Введение	3
1. Графовая формализация описания сетевых структур и процессов в контексте обеспечения кибербезопасности	8
1.1. Основы топологического описания сетей	8
1.1.1. Приложение теории графов к описанию сетевых структур	8
1.1.2. Элементы и части графов сетей	10
1.1.3. Матричное описание сетей	12
1.2. Наполнители сетей	16
1.3. Методики и модели взвешивания сетей	17
1.3.1. Матрицы взвешенности сетей и их графы	17
1.3.2. Ресурс и потенциал взвешенной сети	23
1.4. Метрики взвешенных сетей	27
1.4.1. Метрики центральности	27
1.4.2. Метрики эквивалентности	31
Контрольные вопросы первой главы	34
2. Систематизация и исследование сведений об инструментальных средствах оценки и регулирования рисков реализации кибератак	36
2.1. Базовые понятия сферы обеспечения безопасности ..	36
2.2. Информационное обеспечение риск-анализа компьютерных атак	41
2.2.1. База знаний MITRE ATT&CK	41
2.2.2. База знаний CAPEC	42
2.2.3. База знаний CWE	43
2.2.4. Базы знаний об уязвимостях	43

2.2.5. База знаний CPE	44
2.2.6. База знаний CISA KEV	46
2.2.7. Взаимосвязи рассмотренных баз знаний	46
2.2.8. Агрегаторы знаний для генерации моделей	47
2.2.9. Базы знаний о мерах противодействия кибер- атакам	49
2.3. Анализ особенностей известных риск-калькуляторов	52
2.3.1. CVSS	53
2.3.2. SSVC	55
2.3.3. EPSS	57
2.3.4. VISS	59
2.3.5. OWASP	60
2.3.6. BVSS	63
2.3.7. HVSS	64
2.3.8. Red Hat Severity Ratings	66
2.3.9. Сравнительная оценка калькуляторов	69
2.4. Инструментарий оценки и регулирования киберрис- ков	70
2.4.1. Концепция управления рисками кибербезопас- ности США	70
2.4.2. Модель факторного анализа информационных рисков от компании FAIR-institute	80
2.4.3. Графовый риск-анализ эффективности кибер- контроля от компании Monaco Risk	83
2.4.4. Методика оценки и приоритизации кибер-рисков от компании Qualys	86
2.4.5. Система VPR для оценки уязвимости с помощью машинного обучения	92
2.5. Перспективы совершенствования инструментария оцен- ки и регулирования киберрисков	94
Контрольные вопросы второй главы	96
3. Риск-моделирование процессов реализации кибер- атак	98
3.1. Вероятностные модели на векторном уровне форма- лизации	98
3.1.1. Многообразие составляющих и разновидностей кибератак	98
3.1.2. Задачи риск-анализа успешности единичных и множественных кибератак	100

3.1.3. Вычисление параметров риск-моделей одиночных кибератак	103
3.1.4. Рисканализ множественных кибератак	108
3.1.5. Массированные кибератаки: оценка рисков	113
3.2. Риск-модели на сценарном уровне формализации ...	116
3.2.1. Сущность сценарного моделирования кибератак	116
3.2.2. Подходы к генерации сценариев кибератак	120
3.2.3. Методическое обеспечение риск-анализа сценариев реализации кибератак	122
Контрольные вопросы третьей главы	128
4. Модели процессов управления рисками реализации кибератак	130
4.1. Проактивное управление кибер-рисками	130
4.1.1. Методики управления защищенностью путем распределения риска	131
4.1.2. Управление защищенностью сети посредством устранения рисков	136
4.2. Компенсация рисков реализации атак, нарушающих качества информации	137
4.2.1. Методика оценки коэффициента смягчения риска	140
4.2.2. Смягчение риска с использованием нескольких компенсационных мер	141
Контрольные вопросы четвертой главы	143
Заключение	146
Литература	148
Приложения	156
Приложение А	156
Приложение Б	162
Приложение В	186