

# ОГЛАВЛЕНИЕ

Введение .....	3
<b>1. Методическое обеспечение организационно-правовой защиты корпоративных сетей .....</b>	<b>9</b>
1.1. Риск-аналитика для совершенствования организационно правового обеспечения сетевой безопасности ...	9
1.1.1. Формализация риск-анализа атакуемых корпоративных сетей .....	10
1.1.2. Методическое обеспечение для построения риск-ландшафта атакуемой корпоративной сети .....	12
1.2. Частная политика обеспечения сетевой безопасности	15
1.2.1. Общие положения .....	16
1.2.2. Цели и задачи Частной политики обеспечения сетевой безопасности .....	18
1.2.3. Нормативно-правовое обеспечение .....	19
1.2.4. Информация, необходимая для построения плана мероприятий по обеспечению безопасности Организации .....	19
1.2.5. Требования и меры по защите информации в Организации с учетом специфики сетевой атаки заданного типа .....	21
1.2.6. Документы, регламентирующие выполнение процедур по обеспечению безопасности Организации.....	22
1.2.7. Документы, устанавливающие требования к сотрудникам Организации .....	23
1.2.8. Определение общих ролей и обязанностей, связанных с обеспечением информационной безопасности в Организации .....	23
1.2.9. Контроль за реализацией Частной политики ...	25

1.2.10. Условия пересмотра (выпуска новой редакции) Частной политики .....	25
1.3. Частные регламенты обеспечения сетевой безопасности .....	26
1.3.1. Регламент обнаружения и регистрации инцидентов нарушения сетевой безопасности организации ....	28
1.3.2. Регламент реагирования на инциденты нарушения сетевой безопасности организации .....	36
1.3.3. Регламент ликвидации последствий инцидентов нарушения сетевой безопасности организации .....	39
1.4. Частные инструкции обеспечения сетевой безопасности .....	42
1.4.1. Инструкция администратора .....	43
1.4.2. Инструкция внутреннего и внешнего пользователя .....	51
<b>2 Сетевая контрразведка: организационно-правовое обеспечение</b> .....	<b>58</b>
2.1. Формирование риск-ландшафта сетевой разведки ...	58
2.1.1. Формирование и описание полного множества сценариев атак сетевой разведки .....	58
2.1.2. Формирование и описание полного множества уязвимостей, используемых сетевой разведкой .....	69
2.1.3. Формирование риск-ландшафта сетевой разведки .....	72
2.2. Частная политика сетевой контрразведки .....	77
2.2.1. Нормативная база и объекты защиты сетевой контрразведки .....	78
2.2.2. Модель сетевого разведчика .....	78
2.2.3. Требования к технологическому и организационному обеспечению защиты от сетевой разведки .....	83
2.3. Частные регламенты сетевой контрразведки .....	92
2.3.1. Частный регламент обнаружения и регистрации контрразведкой инцидентов нарушения сетевой безопасности Организации .....	93
2.3.2. Частный регламент реагирования контрразведки на инциденты нарушения безопасности Организации .....	98
2.3.3. Частный регламент ликвидации последствий инцидентов нарушения сетевой безопасности Организации при атаках типа «сетевая разведка» .....	105

2.4. Частные инструкции сетевой контрразведывательной деятельности Организации .....	106
2.4.1. Частная инструкция администратора по защите информации в Организации .....	106
2.4.2. Частная инструкция пользователя .....	116
<b>3. Корпоративный киберполигон: инструментарий освоения и отработки техник сетевого противоборства .....</b>	<b>118</b>
3.1. Архитектура киберполигона .....	118
3.1.1. Киберполигон как объект управления рисками .....	118
3.1.2. Подход к разработке архитектуры киберполигона .....	123
3.1.3. Сравнение с аналогами .....	128
3.2. Организационно-правовое обеспечение программы «Киберполигон» .....	132
3.2.1. Предпосылки появления программы (на вузовском примере) .....	132
3.2.2. Мероприятия программы .....	133
3.2.3. Горизонты внедрения программы .....	145
3.3. Особенности проектной деятельности при реализации программы «Киберполигон» .....	146
3.3.1. Целеполагание проектной деятельности .....	146
3.3.2. Матричный подход к формализации целеполагания и результативности проектной деятельности .....	148
3.3.3. Студенческая проектная деятельность в рамках программы «Киберполигон» .....	156
3.4. Полигонные киберучения на примере моделирования компьютерных эпидемий .....	167
3.4.1. Особенности модуля эпидемического моделирования .....	167
3.4.2. Программный модуль моделирования сетевых эпидемий Epidemics on Networks (EoN) .....	169
3.4.3. АИС дискретного моделирования сетевых эпидемий на основе ПТК NetEpidemic .....	171
3.4.4. Программа моделирования эпидемических процессов «Бахчисарайский фонтан» .....	173
3.4.5. Основные противоречия и перспективы дальнейшего совершенствования инструментария .....	181
<b>Заключение .....</b>	<b>186</b>

<b>Литература</b> .....	188
<b>Приложения</b> .....	206
Приложение А .....	206
Приложение Б .....	206
Приложение В .....	209
Приложение Г .....	210
Приложение Д .....	211
Приложение Е .....	221