Оглавление

Введение ... 9

1. Парадигма управления информационной безопасностью КИИ ... 21

1.1. Практика управления информационной безопасностью 21

1.1.1. Контекст управления безопасностью ... 22

1.1.2. Критерии и достаточность защищенности ... 28

1.1.3. Декларативное управление безопасностью ... 33

1.1.4. Развитие декларативных схем управления безопасностью ... 36

1.1.5. Системная стратегия управления безопасностью ... 40

1.2. Декларативное управление безопасностью КИИ ... 44

1.2.1. Нормирование информационной безопасности КИИ ... 44

1.2.2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) 49

1.2.3. Международная практика решения задач информационной безопасности для объектов КИИ ... 52

1.3. Парадигма асимптотического управления информационной безопасностью КИИ ... 57

1.3.1. Цели безопасности КИИ ... 57

1.3.2. Информационная и функциональная безопасность КИИ ... 61

1.3.3. Особенности управления безопасностью КИИ ... 62

1.3.4. Принципы и задачи управления безопасностью КИИ 67

1.3.5. Асимптотическое управление безопасностью КИИ ... 74

Литература ... 77

2. Управление событиями безопасности КИИ ... 80

2.1. Модель абстрактного сетевого сервиса безопасности ... 80

2.1.1. Функции защиты в базовой эталонной модели OSI ... 81

2.1.2. Механизмы реализации активных функций защиты ... 83

2.1.3. Функции мониторов безопасности ... 86

2.1.4. Прогностическая и адаптивная функции асимптотического управления безопасностью ... 93

2.2. Управление событиями безопасности КИИ ... 96

2.2.1. Событийно-ориентированная политика безопасности ... 96

2.2.2. Информационная база определения событий безопасности 100
2.2.3. Внутренняя структура событий безопасности 107
2.2.4. Агрегирование событий безопасности 111
2.2.5. Сигнатуры событий сетевой безопасности 116
2.2.6. Событие безопасности в сетевой субъектно-объектной модели 123
2.2.7. Механизм мониторинга сетевых событий безопасности 129
2.3. Оценка эффективности управления на базе событий безопасности 136
2.3.1. Качество индикации инцидента 136
2.3.2. Критерии оценки качества индикации инцидента 140
2.3.3. Факторы опасности и интенсивности множества событий безопасности 145
2.3.4. Инцидент как событие безопасности 147
2.3.5. Оценка защищенности индицируемых событий безопасности 150
2.3.6. Сравнение множеств сигнатур 152
2.3.7. Оценка корреляции множеств событий безопасности с инцидентом 155
2.4. Моделирование безопасности КИИ 159
2.4.1. Статическое моделирование безопасности КИИ 159
2.4.2. Концепция зональной защиты 165
Литература 171
3. Методы искусственного интеллекта в управлении безопасностью КИИ 177
3.1. Процедуры искусственного интеллекта в схеме активного мониторинга событий безопасности 177
3.2. Технологии искусственного интеллекта 181
3.2.1. Модели искусственного интеллекта 183
3.2.2. Критерии выбора технологии машинного обучения .. 189
3.3. Обучающие и тестовые множества сыбытий 192
3.3.1. Классификация обучающих и тестовых выборок 192
3.3.2. Оценка эффективности обучающих и тестовых выборок 195
3.4. Реализация управления безопасностью КИИ 198
3.4.1. Взаимодействие с ГосСОПКА 198
3.4.2. Архитектура центра управления информационной безопасностью с использованием технологий ИИ для объектов КИИ 204
3.4.3. Основные задачи и структура модуля управления ЦУ ИБ КИИ 208

Литература ... 210
Приложение А. Зарубежный опыт организации защиты критических информационных инфраструктур ... 213
А.1. Защита критической инфраструктуры в США ... 213
А.2. Защита критической инфраструктуры в странах Западной Европы, НАТО и Евросоюза ... 220
А.3. Политика Китая по обеспечению кибербезопасности ... 223
А.4. Заключение ... 226
Литература ... 227
Приложение В. Обзор открытых датасетов по информационной безопасности ... 229
В.1. Датасеты сетевого трафика ... 229
В.2. Датасеты Интернет-трафика ... 233
В.3. Датасеты VPN ... 233
В.4. Датасеты Android-приложений ... 233
В.5. Датасеты IoT-трафика ... 234
В.6. Датасеты устройств, соединенных через Интернет ... 234
В.7. Датасеты электрических сетей ... 234
В.8. Анализ датасетов ... 235
Литература ... 237