

Содержание

Вводные слова	7
Введение	12
Глава 1. Концепция обеспечения киберустойчивости Индустрии 4.0	14
1.1. Ландшафт угроз кибербезопасности	14
1.1.1. Результаты исследования АPT-атак	14
1.1.2. Известные приемы злоумышленников	19
1.1.3. Угрозы кибербезопасности АСУ ТП	24
1.2. Проблема обнаружения «цифровых бомб»	35
1.2.1. Задача обнаружения программных закладок	35
1.2.2. Методы выявления дефектов программ	41
1.2.3. «Паспортизация» программ инвариантами подобия	48
1.2.4. Метод нейтрализации программных закладок	57
1.3. Проблема обеспечения киберустойчивости	66
1.3.1. Основные понятия и определения	66
1.3.2. Учет трендов цифровой трансформации	71
1.3.3. Математическая постановка задачи	77
Глава 2. Модели и методы управления киберрисками Индустрии 4.0	86
2.1. Практика управления киберрисками	86
2.1.1. Эволюция управления киберрисками	86
2.1.2. Возможные методические рекомендации	94
2.1.3. Методы получения субъективной вероятности	102
2.2. Развитие метрик киберустойчивости	113
2.2.1. Возможная метрика киберустойчивости	113
2.2.2. Задание предикатных функций	120
2.2.3. Верификация схем программ	125
2.3. Примеры управления киберрисками	134
2.3.1. Пример методики управления киберрисками	134
2.3.2. Пример BIA (Business Impact Analysis)	139
2.3.3. Инструментальные средства управления киберрисками	154
Глава 3. Методы обеспечения киберустойчивости Индустрии 4.0	160
3.1. Методы управления непрерывностью деятельности	160
3.1.1. Практика управления непрерывностью деятельности	160
3.1.2. Основные этапы жизненного цикла BCM	167
3.1.3. Рекомендации по разработке планов BCP/DRP	173

3.2. Способы управления проектами обеспечения киберустойчивости	183
3.2.1. Подготовка Плана проекта обеспечения киберустойчивости	183
3.2.2. Разработка прогнозных моделей	189
3.2.3. Формирование динамических профилей	193
3.3. Методика создания киберустойчивой инфраструктуры	204
3.3.1. Оценка системы управления киберустойчивостью	204
3.3.2. Проектирование киберустойчивой инфраструктуры	212
3.3.3. Метод обеспечения киберустойчивости	218
Заключение	232
Список литературы	238