

Оглавление

Предисловие	3
Предисловие рецензента (<i>Р. М. Юсупов</i>)	7
Глава 1. Основные понятия кибербезопасности индустриальных систем (<i>Д. П. Зегжда, В. М. Крундышев</i>)	10
1.1. Цифровая трансформация производства	10
1.2. Киберфизические системы	14
1.3. Новые угрозы безопасности	20
1.4. Статистика кибератак	24
1.5. Безопасная организация цифрового производства	28
1.6. Безопасная среда функционирования информационных систем	30
1.7. Сбор и анализ информации в компьютерных сетях	31
1.8. Оценка текущего состояния киберфизической системы	33
1.9. Оценка способности системы сопротивляться деструктивным воздействиям	34
1.10. Общая архитектура управления безопасностью	35
Литература	38
Глава 2. Эволюция технологий информационной безопасности киберфизических систем с точки зрения теории управления (<i>Д. П. Зегжда</i>)	40
2.1. Развитие теоретической базы технологий информационной безопасности	40
2.2. Эволюция технологий защиты — выявленные закономерности	45
2.3. Классификация технологий защиты в терминах теории управления	46
2.4. Цифровая трансформация управления	50
2.5. Обеспечение кибербезопасности цифрового производства на основе методологии гомеостатического управления	54
2.5.1. Киберустойчивость как развитие парадигмы динамической технологии обеспечения безопасности	55
2.5.2. Примеры обеспечения киберустойчивости с использованием гомеостатического управления	58
2.5.3. Пример оценки устойчивости систем цифрового производства	61
2.6. Перспективы подходов теории управления в кибербезопасности	62
Литература	63
Глава 3. Отечественная защищенная платформа информационных систем цифровой индустрии (<i>Д. П. Зегжда, М. О. Калинин, А. С. Марков, И. Ю. Жуков</i>)	65

3.1. Проблема технологической независимости информационно-телекоммуникационной отрасли Российской Федерации	65
3.2. Методология построения защищенных гибридных систем	67
3.3. Технология гибридных систем как основа защищенной платформы цифровой индустрии	71
3.3.1. Создание доверенной виртуализованной среды	71
3.3.2. Гибридизация операционных сред и информационных систем .	73
3.3.3. Использование технологии гибридных систем	80
3.4. Безопасность автоматизированных банковских систем	89
3.4.1. Комплекс контроля и анализа защищенности ресурсов автоматизированных банковских систем	89
3.4.2. Облачные технологии и средства внутреннего контроля защищенности ресурсов АВС	92
3.4.3. Облачные технологии и средства внешнего контроля защищенности ресурсов АВС	93
3.4.4. Мобильные технологии и средства внешнего контроля защищенности ресурсов банковских информационных инфраструктур	94
3.4.5. Контроль защищенности локальных сетей объектов информатизации АВС	95
3.4.6. Выявление уязвимостей в программном обеспечении АВС	96
3.5. Построение систем управления безопасностью в сетях беспилотных транспортных средств	97
Литература	104
Глава 4. Обеспечение киберустойчивости информационных систем цифровой индустрии (Д. П. Зегжда, Е. Ю. Павленко)	106
4.1. Анализ особенностей обеспечения информационной безопасности КФС	106
4.2. Систематизация КФС	111
4.3. Графовая модель КФС	115
4.4. Подход к обеспечению киберустойчивости КФС на основе принципа гомеостаза	117
4.4.1. Возможные подходы к оценке устойчивости КФС к деструктивным воздействиям	123
4.4.2. Оценка киберустойчивости КФС на основе избыточности	126
4.4.3. Оценка киберустойчивости КФС с использованием спектральной теории графов	128
4.4.4. Сценарии переконфигурирования КФС на основе принципа гомеостаза	135
Литература	136
Глава 5. Киберустойчивость сетей с гибкой топологией (Д. В. Иванов, Д. А. Москвин)	140
5.1. Разработка метода автоматизированной саморегуляции структуры сети на основе теории фрактальных графов и его исследование с использованием имитационной модели VANET-сети	140

5.1.1. Представление VANET-сети в виде предфрактального графа ..	141
5.1.2. Описание метода саморегуляции VANET-сети с фрактальной топологией	151
5.1.3. Исследование предложенного метода автоматизированной саморегуляции с использованием имитационной модели VANET-сети	156
5.2. Разработка методики проверки защищенности VANET-сетей от информационных угроз сетевого уровня.....	158
5.2.1. Описание механизмов обеспечения безопасности VANET-сетей от угроз на сетевом уровне	158
5.2.2. Оценка минимальной и максимальной длины маршрута в VANET-сети с предфрактальной топологией.....	164
5.2.3. Методика проверки защищенности VANET-сетей от информационных угроз сетевого уровня на основе принципа самоподобия	166
Литература	168
Глава 6. Обнаружение инцидентов безопасности в магистральных сетях передачи данных (Д. С. Лаврова).....	169
6.1. Безопасность магистральных сетей Интернета	170
6.1.1. Магистральные сети Интернета	170
6.1.2. Особенности магистральных сетей Интернета с точки зрения обеспечения безопасности	176
6.2. Симуляционная модель системы обнаружения инцидентов безопасности в магистральных сетях Интернета	179
6.2.1. Общее описание симуляционной модели	179
6.2.2. Процесс распределенного сбора данных	182
6.2.3. Процесс автоматической классификации сетевого трафика	184
6.2.4. Процессы обнаружения и предотвращения сетевых атак	186
6.3. Технологии сбора и предварительной обработки сверхвысоких объемов трафика магистральных сетей.....	190
6.3.1. Метод распределенного сбора сверхвысоких объемов сетевого трафика	190
6.3.2. Метод автоматической классификации сетевого трафика «на лету»	197
6.4. Технология выявления инцидентов безопасности на основе контроля самоподобия	206
6.4.1. Подходы к оценке самоподобия	206
6.4.2. Метод выявления инцидентов безопасности в магистральных сетях на основе фрактального анализа	209
Литература	215
Глава 7. Технологии SIEM для промышленного Интернета вещей (Д. С. Лаврова)	218
7.1. Проблемы обеспечения безопасности в промышленном Интернете вещей	218
7.1.1. Концепция Интернета вещей и ее применение в крупномасштабных системах	218
7.1.2. Угрозы безопасности в Интернете вещей	221

7.1.3. Задача построения SIEM-системы для промышленного Интернета вещей	228
7.2. Подход к построению SIEM-систем для промышленного Интернета вещей	232
7.2.1. Математическая модель взаимодействия устройств	232
7.2.2. Онтологическая модель предметной области Интернета вещей ..	236
7.3. Технологии выявления инцидентов безопасности	244
7.3.1. Выявление инцидентов безопасности с использованием правил и статистических параметров	244
7.3.2. Выявление инцидентов безопасности на основе контроля неявных взаимосвязей устройств	253
7.3.3. Выявление инцидентов безопасности в промышленном Интернете вещей на основе оценки самоподобия	263
7.3.4. Анализ инцидентов безопасности и формирование событий	266
7.4. SIEM-система для выявления и анализа инцидентов безопасности в крупномасштабной сети промышленного Интернета вещей	270
7.4.1. Архитектура SIEM-системы	270
7.4.2. Экспериментальные исследования	274
Литература	280
Глава 8. Создание доверенной среды обмена данными для цифровой индустрии (А. С. Коноплев).....	285
8.1. Понятие доверенной среды обмена данными	285
8.2. Обзор подходов к построению доверенной среды обмена данными	286
8.2.1. Централизованная инфраструктура открытых ключей	287
8.2.2. Децентрализованный подход к проверке подлинности	291
8.2.3. Обеспечение достоверности информации с использованием распределенных реестров данных	293
8.3. Построение децентрализованной инфраструктуры открытых ключей с использованием распределенных реестров данных ..	298
8.3.1. Модель децентрализованной инфраструктуры открытых ключей на основе технологии блокчейн	298
8.3.2. Обзор существующих инфраструктур открытых ключей на основе технологии блокчейн	302
8.4. Применение блокчейн-подобных реестров для создания доверенной среды обмена данными в современных крупномасштабных распределенных системах	303
8.4.1. Обеспечение достоверности информации в высоконагруженных системах с ограниченными ресурсами	303
8.4.2. Поддержание связности узлов в самоорганизующихся сетях ...	308
8.4.3. Обеспечение устойчивости функционирования киберфизических систем с применением блокчейн-подобного ориентированного ациклического графа	312
Литература	315

Глава 9. Методология аутентификации в сетях цифровой индустрии (Е. В. Александрова, Н. Н. Шенец)	319
9.1. Особенности аутентификации в распределенных системах	319
9.1.1. Типы аутентификации в распределенных системах	320
9.1.2. Подходы к групповой аутентификации	323
9.2. Групповая подпись	323
9.2.1. Классификация схем групповой подписи	328
9.2.2. Групповая подпись на билинейных отображениях	329
9.2.3. Групповая подпись на решетках	345
9.2.4. Подпись на решетках с процедурой отзыва	354
9.2.5. Применение групповой подписи для аутентификации субъектов в распределенных системах	357
9.3. Криптографические протоколы в условиях ограниченных вычислительных ресурсов	462
9.3.1. Использование личностных протоколов шифрования с подписью	363
9.3.2. Концепция аутсорс-вычислений	367
9.3.3. Неоспоримая подпись для выявления вредоносного сервера	369
9.3.4. Аутсорс-алгоритмы вычисления билинейного отображения	371
9.3.5. Аутсорс-реализация трехстороннего протокола установления ключа	374
9.3.6. Аутсорс-алгоритм умножения точки эллиптической кривой на число	375
9.4. Коллективная упорядоченная подпись	377
9.4.1. Упорядоченная подпись для иерархической групповой аутентификации	378
9.4.2. Организация иерархической аутентификации на изогениях эллиптических кривых	379
9.5. Направленная подпись с делегированием полномочий	385
9.5.1. Цифровые подписи со свойством направленности	386
9.5.2. Направленная подпись на изогениях эллиптических кривых ...	387
9.6. Протоколы гомоморфной криптографии	389
9.6.1. Общие понятия гомоморфной криптографии	389
9.6.2. Частично гомоморфные криптосистемы	392
9.6.3. Почти гомоморфные криптосистемы	396
9.6.4. Полностью гомоморфные криптосистемы	400
Литература	406
Глава 10. Экспериментальное тестирование защищенности киберфизических систем (А. Д. Дахнович, Д. А. Москвин) 414	
10.1. Особенности экспериментального тестирования защищенности киберфизических систем	414
10.1.1. Общий порядок экспериментального тестирования защищенности киберфизических систем	415
10.1.2. Уровни защиты объектов киберфизических систем	417

10.1.3. Жизненный цикл процесса обеспечения кибербезопасности объектов киберфизических систем	418
10.2. Поиск угроз и уязвимостей киберфизических систем	420
10.2.1. Таксономия методов поиска уязвимостей	421
10.2.2. Статические и динамические методы поиска уязвимостей	424
10.2.3. Удаленный поиск уязвимостей в защите объектов киберфизических систем	428
10.2.4. Фаззинг объектов киберфизических систем	431
10.2.5. Поиск уязвимостей в бинарном коде с использованием нейронных сетей	436
10.2.6. Threat Hunting в киберфизических системах	440
10.3. Моделирование векторов атак на киберфизические системы ..	442
10.3.1. Моделирование кибератак для анализа защищенности внешних информационных ресурсов	443
10.3.2. Моделирование кибератак для анализа защищенности внутренних информационных ресурсов	447
10.3.3. Имитационное моделирование атак с использованием цифровых двойников	448
10.3.4. Применение методов машинного обучения для автоматизации экспериментального тестирования защищенности	452
10.4. Нейтрализация угроз безопасности и устранение уязвимостей защиты объектов киберфизических систем	460
10.4.1. Планирование обеспечения киберзащиты и киберустойчивости	460
10.4.2. Классификация мер по нейтрализации выявленных угроз защиты объектов киберфизических систем	461
10.4.3. Рекомендации по устранению уязвимостей киберзащиты	467
Литература	468
Глава 11. Применение технологии Больших данных в обеспечении кибербезопасности (М. А. Полтавцева)	470
11.1. Большие данные и обеспечение кибербезопасности систем цифровой экономики	470
11.2. Технологии обработки Больших данных в задачах кибербезопасности	473
11.2.1. Задача обработки данных в системах безопасности	473
11.2.2. Нормализация и управление данными из разнородных источников	476
11.2.3. Сокращение размерности данных и методы агрегации	485
11.2.4. Иерархическая агрегация данных	493
11.2.5. Конвейер обработки данных	504
11.2.6. Интеллектуальное планирование задач	527
11.3. Технологии обеспечения безопасности данных в крупномасштабных системах	537
11.3.1. Особенности защиты данных в системах мониторинга безопасности	537
11.3.2. Шифрование и обеспечение конфиденциальности данных	541
Литература	547