

Министерство науки и высшего образования Российской Федерации

САНКТ-ПЕТЕРБУРГСКИЙ
ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

Институт кибербезопасности и защиты информации



Д. П. Зегжда

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ
КИБЕРУСТОЙЧИВОСТИ
И ПРАКТИКА
ПРОГНОСТИЧЕСКОЙ ЗАЩИТЫ
ОТ КИБЕРАТАК

Монография



ПОЛИТЕХ-ПРЕСС

Санкт-Петербургский
политехнический университет
Петра Великого

Санкт-Петербург
2022

Зегжда Д. П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак : монография / Д. П. Зегжда. – СПб. : ПОЛИТЕХ-ПРЕСС, 2022. – 490 с.

Монография посвящена обеспечению безопасности новых цифровых систем в условиях постоянных кибератак. Рассматривается эволюция цифровых систем и когерентная эволюция технологий безопасности, формализуются понятия кибербезопасности, киберсреды, киберустойчивости и приводятся угрозы новым цифровым системам. Изложены модели и методы в области моделирования цифровых систем для решения задач информационной безопасности и моделирования кибератак. В монографии представлены основные теоретические концепции сохранения функциональных характеристик цифровых систем в условиях деструктивных воздействий, такие как гомеостаз, функциональная устойчивость и опережающее отражение. Представлен общий биоинспирированный подход к киберустойчивости. Практическая часть книги включает примеры обеспечения киберустойчивости сетевых цифровых систем на базе приведенных концепций и прогностической защиты от кибератак. В заключении приводятся показатели киберустойчивости для различных классов систем и основные положения эволюционного подхода к кибербезопасности цифровых технологий.

Книга предназначена для широкого круга читателей, включая специалистов по информационной безопасности, исследователей, преподавателей и студентов, специализирующихся в данной области информационной безопасности.

Табл. 22. Ил. 139. Библиогр.: 259 назв.

Печатается по решению
Совета по издательской деятельности Ученого совета
Санкт-Петербургского политехнического университета Петра Великого.

Оглавление

Оглавление	4
Предисловие рецензента	9
Предисловие автора	13
Введение	20
Глава 1. Эволюция кибербезопасности	24
1.1 Безопасность цифровой трансформации	24
1.1.1 Новая цифровая среда	25
1.1.2 Понятия новой цифровой среды: кибербезопасность и киберпространство	31
1.2 Новая парадигма безопасности цифровой экономики и цифрового производства	40
1.2.1 Цифровая трансформация промышленных технологий	40
1.2.2 Киберфизические системы как пример новых цифровых систем в контексте кибербезопасности	44
1.2.3 Систематизация цифровых систем, связанных с физическими процессами	52
1.2.4 Угрозы современным цифровым системам	60
1.3 Конвергентная эволюция задач информационной безопасности в новом цифровом мире	69
1.4 Заключение	77
1.5 Библиографический список	78
Глава 2. Моделирование безопасности цифровых систем в условиях кибератак	85
2.1 Общий подход к моделированию кибербезопасности	85
2.2 Систематизация методов моделирования новых цифровых систем	90

2.3	Моделирование безопасности при помощи дискрипционных логик	97
2.4	Стохастическое моделирование безопасности цифровых систем	101
2.5	Моделирование безопасности Интернета Вещей	106
2.6	Моделирование сетевых цифровых систем и их безопасности с использованием графов	115
2.6.1	Формализация структуры объекта защиты на основе графовых моделей	115
2.6.2	Функционально-семантическая графовая модель функционирования систем с цифровым управлением	129
2.6.3	Моделирование кибератак на базе функционально-семантической графовой модели	140
2.7	Выводы	153
2.8	Библиографический список	154
Глава 3. Модели и методы обнаружения кибератак		159
3.1	Систематизация моделей и методов обнаружения кибератак	159
3.2	Методы обнаружения кибератак на основе модели образцов	163
3.2.1	Сигнатурные методы	163
3.2.2	Новые методы на базе машинного обучения	167
3.3	Методы обнаружения кибератак на основе модели граничных значений	182
3.3.1	Энтропийные методы	182
3.3.2	Статистические методы	185
3.3.3	Новые методы на основе самоподобия	190
3.4	Новые методы обнаружения кибератак на основе прогнозной модели	195
3.4.1	Оценка прогноза с использованием фильтра Калмана	196
3.4.2	Оценка прогноза с использованием нейронной сети	201

3.5	Заключение	208
3.6	Библиографический список	209
Глава 4. Теория обеспечения киберустойчивости цифровых систем		217
4.1	Систематизация и обзор теоретических концепций обеспечения киберустойчивости	219
4.2	Обеспечение киберустойчивости на основе гомеостаза	225
4.3	Обеспечение киберустойчивости на основе функционального подхода	236
4.4	Обеспечение киберустойчивости на основе концепции опережающего отражения	245
4.5	Общий биоинспирированный подход к обеспечению киберустойчивости цифровых систем	258
4.6	Заключение	263
4.7	Библиографический список	264
Глава 5. Примеры обеспечения киберустойчивости и прогностической защиты цифровых систем		268
5.1	Обеспечение устойчивости в условиях кибератак через архитектурный гомеостаз	269
5.2	Обеспечение киберустойчивости путем саморегуляции	274
5.2.1	Пример оценки времени саморегуляции	274
5.2.2	Пример саморегуляции в условиях кибератак для сети энергоснабжения Smart Grid	283
5.2.3	Пример саморегуляции в условиях кибератак для системы класса «Умный город»	294
5.2.4	Пример оценки защищенности и саморегуляции в условиях кибератак для VANET-сети	302

5.2.5	Пример саморегуляции в условиях кибератак сетевых цифровых систем на основе теоретико-игрового подхода	310
5.3	Обеспечение киберустойчивости путем управления по состоянию	320
5.3.1	Пример обеспечения устойчивости к кибератакам систем класса «Умный дом» на базе ПКС с использованием ситуационного управления	320
5.3.2	Пример обеспечения киберустойчивости многоагентной сети на основе конечного автомата поведения	328
5.4	Практика прогностической защиты при отражении кибератак	335
5.4.1	Пример предотвращения влияния кибератак для сети энергоснабжения Smart Grid на основе иммунного подхода	336
5.4.2	Пример прогнозирования кибератак для системы класса «Умный город» при реализации опережающего отражения	344
5.4.3	Пример поиска прецедентов кибератак в ассоциативной памяти для сетевых цифровых систем	349
5.5	Заключение	356
5.6	Библиографический список	357
Глава 6. Показатели киберустойчивости цифровых систем		361
6.1	Оценка киберустойчивости цифровых систем	361
6.1.1	Модель оценки киберустойчивости	362
6.1.2	Систематизация показателей киберустойчивости	365
6.2	Структурные показатели киберустойчивости	372
6.3	Функциональные показатели киберустойчивости	375
6.3.1	Киберустойчивость как функциональное самоподобие	376
6.3.2	Киберустойчивость как устойчивость гомеостаза	382
6.3.3	Киберустойчивость как запас функциональных маршрутов	384

6.3.4	Киберустойчивость как запас управляемости в многоагентных системах	393
6.4	Топологические показатели киберустойчивости	399
6.5	Заключение	412
6.6	Библиографический список	413
Глава 7. Эволюционный подход к кибербезопасности цифровых систем		421
7.1	Основы эволюционного подхода к кибербезопасности	423
7.2	Эволюционная кибербезопасность самоорганизующихся цифровых систем	429
7.3	Показатели безопасности в цифровом мире и оценка пространства состояний	435
7.4	Показатели опасности внешних воздействий и живучести цифровых систем	443
7.5	Заключение	452
7.6	Библиографический список	453
Заключение		456
Библиографический список		461