



ТЕХНОСФЕРА



ИНСТИТУТ
СТРАТЕГИЙ
РАЗВИТИЯ

БИБЛИОТЕКА

ИНСТИТУТА СТРАТЕГИЙ РАЗВИТИЯ

А.И. Белоус

ТЕХНОЛОГИИ, МЕТОДЫ И ИНСТРУМЕНТЫ
ВОЙН XXI ВЕКА

ТЕХНОСФЕРА

Москва

2023

Содержание

Предисловие.....	9
Глава 1.	
ГЕНЕЗИС И КЛАССИФИКАЦИЯ ВОЙН	13
1.1. Введение	13
1.2. Эволюция сущности войны	19
1.3. Типология войн	22
1.4. Детализированная классификация типов и подтипов войн.....	32
1.5. Блогинг и разведблогинг как современные методы информационного противоборства	45
Литература.....	50
Глава 2.	
ГИБРИДНЫЕ ВОЙНЫ	52
2.1. Генезис, концепции и инструменты гибридных войн.....	52
2.2. Феномен постправды	64
2.3. Украинский плацдарм — детализированный план гибридной войны против России в действии	78
2.4. Технологии создания дипфейков и методы противодействия	97
2.5. Эффективные методы и средства противодействия фейковой информации.....	112
Литература.....	132
Глава 3.	
ИНФОРМАЦИОННЫЕ ВОЙНЫ: ГЕНЕЗИС, КОНЦЕПЦИИ И ИНСТРУМЕНТЫ	134
3.1. Термины и определения информационных войн	134
3.2. Основные черты информационных войн.....	135
3.3. Виды информационных атак	136
3.4. Типы информационных войн	136
3.5. Генезис информационных войн.....	138
3.6. Американская доктрина информационных войн	140
3.7. Структурное обеспечение информационных войн.....	142
3.8. Как «простому человеку» не стать жертвой информационной войны? ..	148
3.9. Информационная сфера как компонент концепции сетцентричной войны	149
3.10. Проекты агентства DARPA в области информационного противостояния.....	152
3.11. Стратегии и методы ведения информационно-гибридной войны.....	157

3.12. Кибертерроризм как форма информационной войны	159
Литература	163

Глава 4.

ПРОКСИ-ВОЙНЫ: ГЕНЕЗИС, КОНЦЕПЦИЯ, СПОСОБЫ ВЕДЕНИЯ.....

4.1. История возникновения и особенности прокси-войн	164
4.2. Прокси-война как военная составляющая гибридной войны	169
4.3. Способы ведения прокси-войн.....	172
4.4. Особенности межгосударственных конфликтов в серой зоне	174
4.5. Оценка риска военного конфликта между КНР и США.....	186
4.6. Политика НАТО в области цифровизации методов ведения войны будущего	194
Литература	201

Глава 5.

КОГНИТИВНЫЕ ВОЙНЫ И НЕЙРОННОЕ ОРУЖИЕ.....

5.1. Цели, объекты и технологии когнитивных войн	204
5.2. Нейрооружие как средство массового подчинения	211
5.3. Военная нейробиология.....	215
5.4. Военная нейрофармакология	219
5.5. Искусственная стимуляция умственной деятельности.....	220
5.6. Интерфейсы типа «мозг — компьютер»	221
5.7. Биохимическое нейронное оружие	223
5.8. Направленное энергетическое оружие (DEW).....	223
5.9. Нейронное оружие на основе информации / программного обеспечения	225
5.10. Угрозы нейронного оружия.....	226
5.11. Опасности «неправильного» использования нейронных технологий.....	228
5.12. Особенности и преимущества США, России и Китая в гонке нейронных вооружений	229
5.13. Новые «нейронные угрозы» международной безопасности	234
5.14. Нейронная безопасность и нейронная этика	236
5.15. Стратегия обеспечения нейронной безопасности	238
5.16. От психологических операций до нейровойны: основные опасности ...	241
Литература	243

Глава 6.

КИБЕРОРУЖИЕ: КОНЦЕПЦИИ, МЕТОДЫ

И СРЕДСТВА ПРИМЕНЕНИЯ

6.1. Краткая история развития кибероружия.....	248
6.2. Терминология и классификация кибероружия	265
6.3. Методы решения задач идентификации исполнителей и заказчиков кибератак.....	296
6.4. Кибершпионаж, киберразведка и киберконтрразведка	306
Литература	319

Глава 7.**НОВЫЕ ОБЪЕКТЫ КИБЕРАТАК: МЕТОДЫ РЕАЛИЗАЦИИ
И СПОСОБЫ ЗАЩИТЫ**

7.1. Целевые атаки и средства защиты от них	321
7.2. Атаки на цепочки поставок	327
7.3. Кибератаки на медицинские учреждения	342
7.4. Кибератаки на отели: методы реализации и способы защиты	358
7.5. Анализ мирового ландшафта киберугроз за 2021 г.	372
Литература	391

Глава 8.**РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ ГЛОБАЛЬНОГО
ПЕРЕХВАТА ИНФОРМАЦИИ**

8.1. Радиоэлектронная система глобального перехвата информации «Эшелон»	392
8.2. Разведывательный альянс «Пять глаз»	402
8.3. Европейские системы электронного шпионажа	410
Литература	412

Глава 9.**СТРУКТУРА И ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ
НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРЗАЩИТЫ США**

9.1. Эволюция стратегии обеспечения кибербезопасности США	414
9.2. Стратегия кибербезопасности США в редакции 2018 г.	422
9.3. Основные модели киберугроз США	427
9.4. Краткий аннотированный перечень реализованных проектов обеспечения кибербезопасности США	434
Литература	442

Глава 10.**ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ
ЭНЕРГЕТИЧЕСКИХ СИСТЕМ**

10.1. Введение в проблему	445
10.2. Крупнейшие кибератаки на энергетические системы за период с 2010 по 2020 гг.	450
10.3. Особенности цифровизации энергетических систем	451
10.4. Типовой алгоритм кибератаки	464
10.5. Методика оценки рисков безопасности в энергетических системах	470
10.6. Обеспечение кибербезопасности в области возобновляемых источников энергии	491
10.7. Обеспечение кибербезопасности цифровых электрических подстанций	497
10.8. Основы государственной политики в области кибербезопасности в электроэнергетической отрасли	499
Литература	501

Глава 11.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ГИБРИДНЫЕ ВОЙНЫ	508
11.1. Место и роль искусственного интеллекта в современных кибервойнах.....	508
11.2. Основные направления применения искусственного интеллекта в системах вооружения и военной технике	509
11.3. Использование искусственного интеллекта для планирования и имитационного моделирования боевых действий	514
11.4. Особенности применения ИИ в автономных мобильных устройствах вооружений и военной техники	515
11.5. Кибербезопасность комплексов с беспилотными летательными аппаратами	519
Литература	527