

СОДЕРЖАНИЕ

Предисловие.....	3
Предисловие к первому изданию.....	7

Раздел I

СИСТЕМА СОЦИАЛЬНЫХ И ПОЛИТИЧЕСКИХ ОТНОШЕНИЙ ИНФОРМАЦИОННОГО ОБЩЕСТВА КАК СРЕДА ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ТАЙНЫХ ОПЕРАЦИЙ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ

Глава 1. Информационно-психологические конфликты в современном информационном обществе	23
1.1. Информационно-психологическое пространство	24
1.2. Субъекты деятельности в информационно-психологическом пространстве	28
1.3. Условия, тенденции и закономерности возникновения и эволюционного развития острых конфликтных ситуаций в современном информационном обществе	30
1.4. Основные этапы возникновения и развития конфликтов в современном информационном обществе	34
1.5. Информационно-психологическая безопасность современного информационного общества	36
1.6. Информационно-психологический конфликт как средство достижения политических целей	45
Глава 2. Политические процессы в современном информационном обществе.....	46
2.1. Общая характеристика содержания и направленности политических процессов в современном информационном обществе ...	46
2.2. Система политических отношений общества в условиях глобальной информатизации	47
2.2.1. Изменения в массовом и индивидуальном сознании граждан, связанные с глобальной информатизацией	47
2.2.2. Субъекты информационно-психологических отношений	49
2.2.3. Информационный неокOLONиализм.....	53
2.3. Система политических отношений информационного общества в условиях глобализации	54
2.3.1. Влияние процессов глобализации на информационное общество и происходящие в нем процессы	55
2.3.2. Обеспечение информационной безопасности государства в условиях глобализации	57
2.4. Геополитические процессы в современном информационном обществе и информационная политика	67
2.4.1. Геополитические процессы и закономерности в современном многополярном мире.....	69

2.4.2. Информационное превосходство как форма реализации геополитической конкуренции в информационном пространстве	77
2.4.3. Взаимосвязь и взаимозависимость геополитических процессов и информационной политики в современном информационном обществе	82
2.4.4. Взаимосвязь и взаимозависимость геополитических процессов и информационной безопасности	86
2.5. Безопасность и система политических отношений информационного общества	88
2.5.1. Влияние политических конфликтов на безопасность общества	91
2.5.2. Безопасность политической системы общества	100
2.6. Информационная политика в системе политических отношений информационного общества	103
2.6.1. Новый подход к информационной политике	103
2.6.2. Правовое регулирование общественных отношений в информационной сфере	106
2.6.3. Интернет-суверенитет	119
2.6.4. Информационная безопасность Российской Федерации	121
2.6.5. Информационно-психологическая безопасность Российской Федерации	123
2.6.6. Государственная информационная политика	129

Раздел II

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ ВОЙНА В СИСТЕМЕ ПОЛИТИЧЕСКИХ ОТНОШЕНИЙ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Глава 3. Информационная война как инструмент внешней агрессии и средство достижения политических целей	134
3.1. Особенности среды, в которой проводятся операции информационной войны	135
3.1.1. Средства массовой информации и коммуникации	135
3.1.2. Открытые информационно-телекоммуникационные сети	136
3.2. Эволюция знаний и представлений об информационной войне	139
3.3. Определение информационной войны	148
3.4. Цель информационной войны	149
3.5. Информационная асимметрия	151
3.6. Информационное доминирование	153
3.7. Информационное оружие	153
3.8. Роль СМИ в информационных войнах и психологических операциях	156
3.9. Организационно-технологическая схема операции информационной войны	156
3.10. Роль периодов экспозиции («информационной тишины»)	158
3.11. Основная итерационная схема	160
3.12. Механизм положительной обратной связи	160

3.13. Принцип действия многокаскадной итерационной схемы с положительной обратной связью	162
3.14. «Пограничное» психоэмоциональное состояние	162
3.15. Структура и основные этапы операции информационной войны.....	163
3.16. Каскады.....	164
3.17. Подготовительный этап информационной операции.....	165
3.18. Выбор объекта (мишени) информационной атаки	166
3.19. Выбор референтных каналов доведения информационного воздействия	166
3.20. Какой должна быть информация во вбросе, чтобы ей поверили	169
3.21. Операции легализации вбрасываемой информации	173
3.22. Виды операций «контролируемой утечки»	177
3.22.1. Провокация кражи секретных сведений	178
3.22.2. Технологии класса WikiLeaks	180
3.22.3. Операции класса «перебежчик».....	182
3.22.4. Технологии вброса управляющей информации через механизм публичных дебатов (технологии класса «Псаки — Метью Ли»).....	183
3.23. Признаки операций легализации вбрасываемой информации	185
3.24. Фейковые новости как инструмент перехвата информационной повестки.....	186
3.25. Характерные черты информационной войны	192
3.26. Основные различия между информационной войной и войной традиционной	194
3.27. Концепция информационного сдерживания	195
3.28. Основные структурные элементы информационно-психологического воздействия, определяющие содержание информационно-психологической войны	196
3.28.1. Дезинформирование	198
3.28.2. Лоббирование	200
3.28.3. Манипулирование	201
3.28.4. Пропаганда	207
3.28.5. Управление кризисами.....	209
3.28.6. Шантаж	210
3.29. Основные этапы мероприятий и аксиомы информационно-психологической войны	211

Глава 4. Практика организации и проведения информационных операций.....

4.1. Теория и практика информационных войн против первых лиц государства	213
4.2. «Дело об отравлении Скрипалей» как пример операции информационной войны с пошаговым повышением ставок.....	217
4.2.1. Первый этап информационной операции: «игра с пошаговым повышением ставок»	220
4.2.2. Второй этап информационной операции: Петров, Боширов и метод «загонной охоты»	230

4.2.3. Возможный сценарий третьего этапа информационной операции британской разведки	239
4.2.4. Реакция России	242
4.3. По лезвию бритвы: в деле Скрипалей, возможно, появится еще одна «сакральная жертва»	245
4.4. Panama Papers («Панамское досье»): классический пример информационной атаки на первых лиц государства.....	265
4.5. Помпео прилетел в Боготу инспектировать свою агентуру	270
4.6. Даллас: и снова «неизвестные снайперы».....	273
4.7. Джеймс Коми и Хиллари Клинтон: шпионаж в пользу ИГИЛ	276
4.8. Переговоры Лаврова — Керри и военный мятеж в Турции: история одного совпадения.....	278
4.9. «Кремлевский доклад» С. Мнучина	280
4.10. Под колпаком у Мюллера, или Легко ли быть русским агентом в тылу врага	284
4.11. «Универсальный центр противодействия новым вызовам и угрозам»: ШОС создает наднациональные органы обеспечения безопасности	290
4.12. Ливия: игры разума	292
4.13. Провокация как инструмент современных информационных войн	296
4.13.1. Пример 1. Провокация, которая не удалась	297
4.13.2. Пример успешно организованной провокации	301
4.14. Ассанж: тюрьма или казнь	306
4.15. Personal Spy Story Марии Бутиной	308
4.16. Как «снести» Францию	312
4.17. Шпионские скандалы и прослушивание лидеров иностранных государств.....	315
4.18. Никарагуа: цветные революции возвращаются?	318
4.19. Что стоит за новой (2017 г.) Стратегией национальной безопасности США.....	323
4.20. США и Китай в объятиях торговой войны: кто кого	326
4.21. Трёп или «дырявое решето»?.....	332
4.22. Государственный переворот в Боливии: основные выводы и уроки.....	334
4.23. Как ЦРУ работает с протестами в Москве.....	337
4.24. «Твиттер» как пятая власть.....	340
Глава 5. Новейшая практика российских информационных операций [успешных]	344
5.1. «Скрипальские чтения» как пример специальной операции по перехвату информационной повестки.....	344
5.2. Вирусные технологии и «эпидемии» каскадного типа на примере операции по разоблачению агента влияния ЦРУ, бывшего вице-президента Венесуэлы Диосдадо Кабельо 17-21/08/2019	346
5.3. Продолжение «дела Диосдадо Кабельо»: поиск «крота»	354
5.4. «Венесуэльский прецедент», или Новые технологии организации государственных переворотов	359

Глава 6. Уголовно-правовая и криминалистическая характеристика операций информационно-психологической войны	361
6.1. Информация и информационные отношения как новый криминалистический объект.....	362
6.2. Криминалистическая характеристика компьютерных преступлений как информационно-технических составляющих операций информационно-психологической войны	368
6.2.1. Понятие «информация» в криминалистической характеристике компьютерных преступлений.....	368
6.2.2. Противоправные действия в отношении компьютерной информации.....	370
6.3. Уголовно-правовая характеристика компьютерных преступлений как информационно-технических составляющих операций информационно-психологической войны	371
6.3.1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	371
6.3.2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).....	374
6.3.3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК)	378
6.3.4. Виды преступных последствий.....	379
6.3.5. Способы совершения преступлений.....	382
6.3.6. Свойства личности субъекта преступления.....	390
6.4. Предупреждение компьютерных преступлений.....	393
6.5. Методика и практика расследования преступлений в сфере компьютерной информации	394
6.5.1. Типичные следственные ситуации первоначального этапа и следственные действия.....	394
6.5.2. Практические особенности отдельных следственных действий	397
6.6. Уголовно-правовая характеристика операций информационно-психологической войны	405
6.6.1. Уголовно-правовая характеристика основных структурных элементов операций информационно-психологической войны	405
6.6.2. Уголовно-правовая характеристика некоторых наиболее распространенных операций информационно-психологической войны	408
6.7. Операции информационно-психологической войны в контексте международного права.....	408
Глава 7. Операция «Вторжение»: вмешательство США в выборы в Российской Федерации в ходе президентских кампаний 1996–2018 гг.	416
7.1. Внешнее вмешательство в выборы как угроза безопасности Российской Федерации	416
7.2. Виды внешнего вмешательства в процесс избирательной кампании.....	418
7.3. Концептуальные и стратегические основания вмешательства США во внутривнутриполитическое пространство России	419

7.3.1. Стратегии национальной безопасности США 1995–1996 гг.: вовлеченность и расширение	420
7.3.2. Стратегии национальной безопасности США 1997–2000 гг. для нового века	420
7.3.3. Стратегия национальной безопасности США 2001 г. для глобальной эпохи	421
7.3.4. Стратегии национальной безопасности США 2002 и 2006 гг. в период президентства Дж. Буша-мл.	422
7.3.5. Стратегии национальной безопасности США 2010 и 2015 гг. в период президентства Б. Обамы	422
7.3.6. Стратегия национальной безопасности США 2017 г.	423
7.4. Агенты внешнего вмешательства США в выборы в Российской Федерации, их цели и методы	424
7.4.1. Государственные органы и структуры	424
7.5. Политические партии США, финансово-промышленные группы и аффилированные с ними НКО и СМИ	428
7.5.1. Демократическая партия США	428
7.5.2. Республиканская партия США	429
7.6. Методы и технологии вмешательства США в информационное пространство РФ в ходе президентских кампаний 1996–2018 гг. на примере конкретных кейсов	431
7.6.1. Выборы Президента РФ 1996 г.	431
7.6.2. Выборы Президента России 2000 г.	434
7.6.3. Выборы Президента России 2004 г.	436
7.6.4. Выборы Президента России 2008 г.	437
7.6.5. Выборы Президента России 2012 г.	438
7.6.6. Выборы Президента России 2018 г.	441
7.7. Практические рекомендации по противостоянию методам и технологиям вмешательства США в выборы Президента РФ в 2024 г.	442
Глава 8. Деструктивные механизмы воздействия психологических операций на сознание людей	444
8.1. Психологические операции, направленные на эрозию сознания подростающего поколения России	444
8.2. Психологические операции, направленные на фальсификацию истории Второй мировой войны	448
8.3. Психологические операции, направленные на эрозию чувства патриотизма у подрастающего поколения	462
8.4. Профилактика негативного информационно-психологического воздействия на социализацию личности подрастающего поколения ...	466
Раздел III	
ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА В УСЛОВИЯХ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ	
Глава 9. Основные принципы деятельности органов исполнительной власти государств, интегрированных в информационное общество, в условиях информационно-психологической войны	475

9.1. Качественные изменения вида и содержания управления в информационном обществе	475
9.2. Использование информационных технологий в процессе государственного управления	478
9.2.1. Облик системы органов государственной власти в информационном обществе	479
9.2.2. «Электронное правительство» как форма интеграции традиционных структур государственной власти в информационное общество.....	488
9.2.3. Изменение роли и статуса СМИ в условиях использования информационных технологий в процессе государственного управления	489
9.2.4. СМИ и МК как объект пересечения интересов инициатора и жертвы информационно-психологической агрессии: условия вовлечения СМИ в психологическое противоборство.....	491
9.3. Методика оценки враждебных и агрессивных действий участников информационно-психологического противоборства.....	493
9.4. Классификация источников информационно-психологической агрессии.....	501
9.5. Система органов государственной власти и управления как основной регулирующий фактор в разрешении конфликтов и управлении кризисными ситуациями в информационно-психологической сфере современного информационного общества....	503
9.5.1. Система органов государственной власти и управления как объект информационно-психологической агрессии	505
9.5.2. Система органов государственной власти и управления как средство отражения информационно-психологической агрессии.....	506
9.5.3. Обеспечение органами государственной власти собственной информационно-психологической безопасности в условиях информационно-психологической войны.....	512
Глава 10. Информационное противоборство в условиях информационно-психологической войны	518
Статья 1. Общие положения.....	518
Статья 2. Приоритеты геополитической конкуренции в современном информационном обществе	519
Статья 3. Информационное противоборство	527
Статья 4. Внешнее управление информационно-психологическими процессами.....	528
Статья 5. Информационно-психологическая экспансия	529
Статья 6. Информационно-психологическая агрессия	530
Статья 7. Информационно-психологическая война.....	530
Статья 8. Информационно-психологические операции	534
Статья 9. Система органов государственной власти как основной регулирующий фактор в разрешении конфликтов и управлении кризисными ситуациями в информационно-психологической сфере.....	539

Статья 10. Особая роль в информационно-психологической войне субъектов, вовлекаемых в информационное противоборство	541
Статья 10.1. Средства массовой информации и массовой коммуникации	541
Статья 10.2. Транснациональные корпорации	544
Статья 10.3. Программы создания оперативного доступа к распределенным интеллектуальным и материальным ресурсам и новые социальные формации	547
Глава 11. Цветные революции и гибридные войны	551
11.1. Гибридная война и цветная революция: к вопросу о соотношении понятий	551
11.2. Точки сопряжения гибридных войн и цветных революций	553
11.3. Цветные революции как «отмычка для демократии» и инструмент демонтажа политических режимов	555
11.4. Цветные революции и «мягкая сила»	561
11.5. Цветные революции сквозь призму гибридных войн	562
11.6. «Убить котенка», или Технологии конфликтной мобилизации в социальных сетях	566
11.7. Новые технологии цветных революций: от Украины до Венесуэлы	571
11.8. Противодействие цветным революциям	578
Глава 12. Государственная информационная политика в условиях информационно-психологической войны	581
Статья 1. Цели, задачи, принципы и направления государственной информационной политики в условиях угрозы реализации иностранными государствами концепции информационно-психологической войны	581
Статья 2. Государственная система информационного противоборства	586
Статья 3. Противодействие информационно-психологической агрессии (войне) на ранних стадиях	588
Статья 4. Быстрое реагирование на внезапно выявленные акции (мероприятия) информационно-психологической агрессии (войны)	593
Статья 5. Информационно-психологическая борьба в условиях информационно-психологической войны	594
Статья 6. Российский центр информационных операций	595
Глава 13. Основные направления формирования пространства коллективной кибербезопасности стран БРИКС: российский подход	598
13.1. Актуальные проблемы обеспечения информационной безопасности в меняющемся мире	598
13.2. Актуальные вызовы и угрозы информационной безопасности РФ	601
13.3. Актуальное состояние системы обеспечения информационной безопасности Бразилии	602
13.4. Актуальное состояние системы обеспечения информационной безопасности Индии	603

13.5. Актуальное состояние системы обеспечения информационной безопасности Китая	603
13.6. Актуальное состояние системы обеспечения информационной безопасности ЮАР	604
13.7. Перспективные направления деятельности для РФ в рамках создания пространства коллективной безопасности БРИКС.....	605
13.8. Задачи формирования пространства информационной безопасности БРИКС	605
13.9. Организационная структура пространства коллективной информационной безопасности БРИКС	606
13.10. Организационная структура Центра обеспечения кибербезопасности БРИКС	606
13.11. Организационная структура Центра информационной политики и коммуникаций БРИКС	607
13.12. Области сотрудничества стран БРИКС в рамках формирования единого пространства информационной безопасности	607
13.13. Проблемные зоны формирования пространства информационной безопасности БРИКС	607
13.14. «Дорожная карта» создания пространства информационной безопасности БРИКС	608
Заключение	609
Литература	614