В МГИМО МИД России вышла в свет монография д.и.н., профессора, главного научного сотрудника Центра международной информационной безопасности и научно-технологической политики, президента НИИГЛОБ. А.Смирнова.

УДК 004

ББК 32.81

С50

Рецензенты:

д-р ист. наук, проф. *А.В. Зинченко,*

д-р техн. наук, д-р юрид. наук, проф. *А.А. Стрельцов*

д-р полит. наук, проф. *Т.А. Шаклеина*

С50

Смирнов, Анатолий Иванович.

Современные информационные технологии в международных отношениях (монография) / А.И. С

ISBN 978-5-9228-1756-1

Цифровая эпоха диктует новые тенденции в международных отношениях. В монографии систем

В книге с учетом зарубежного опыта детально рассматривается роль инновационных цифровых

В условиях обострения глобальной конкуренции особое внимание уделено теоретическим и прак дипломатических миссий как объектов критической информационной инфраструктуры, методам

С учетом стремительных процессов усиления роли цифровых технологий в геополитической кон

УДК 004

ББК 32.81

ISBN 978-5-9228-1756-1
© МГИМО МИД России, 2017

© Смирнов А.И., 2017

ОГЛАВЛЕНИЕ

Предисловие. 8

К читателю.. 10

Введение. 13

1. МЕГАТРЕНДЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ.. 20

1.1. Вехи цивилизации:
от пещеры до «Homo Informaticus». 20

1.2. Измерение информационного общества Международным союзом электросвязи 25

1.1.2. Индекс развития ИКТ в странах мира 2015-2016 гг. 27

1.3. «Интернет вещей» и технология блокчэйн — драйверы Industry 4.0 36

1.3.1. Блокчейн — новая эпоха Интернета. 40

1.4. НБИК-технологии: искусственный интеллект
и стратегические риски для матрицы национальной и международной безопасности 51

1.4.1. Когнитивный компьютинг (CC)
и машинное обучение (ML) 55

1.4.2. Подходы России к развитию цифровых технологий
в документах стратегического планирования. 57

2. СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ В АРСЕНАЛЕ
ВНЕШНЕЙ ПОЛИТИКИ ГОСУДАРСТВА.. 61

2.1. Концептуальные позиции России
о роли ИКТ во внешней политике. 61

2.1.1. Современные ИКТ как инструмент
«мягкой силы» государства. 62

2.2. Базовые научно-теоретические составляющие фактора «мягкая сила» 64

2.3. Фактор «мягкой силы»:
международный рейтинг ведущих стран.. 69

2.4. Особенности «мягкой силы» Китая. 74

2.5. Социальные сети как инструмент
«мягкой силы 2.0». 77

2.5.1. Анализ перспективных направлений
развития соцсетей и мессенджеров. 80

3. ЦИФРОВЫЕ ТЕХНОЛОГИИ
В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ.. 84

3.1. Особенности использования
цифровых технологий
во внешнеполитическом процессе. 85

3.1.1. Проекты исследования Оксфордским университетом использования социальных сетей
в дипломатической практике. 89

3.1.2. Нарратив уровней использования
социальных сетей МИД Израиля. 93

3.2. Электронная дипломатия США.. 96

3.3. Цифровые технологии
в информационных войнах:
от эры «post-truth» к эпохе «post-fake». 114

3.3.1.«Технологии манипуляции» —
SEME и микротаргетирование. 118

3.3.2. Цифровые фейки в международных отношениях. 121

4. ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ АНАЛИЗА
В СИТУАЦИОННО-КРИЗИСНОЙ ДИПЛОМАТИИ.. 125

4.1. Краткий обзор традиционных методов анализа. 125

4.2. Международный конфликт:
определение, фазы развития. 133

4.3. Современные методы анализа.
Метод ситуационного анализа

академика Е.М. Примакова. 151

4.3.1. Методы прогнозирования
международных конфликтов. 155

4.3.2. Когнитивная система анализа. 158

4.4. Ситуационно-кризисные центры
во внешнеполитическом процессе. 163

4.5. Основные структуры кризисного реагирования МИД ФРГ, Италии, и Швеции 171

4.6. Система ситуационных центров
органов государственной власти России.. 178

4.6.1. Национальный центр управления обороной Российской Федерации 181

4.7. Основные параметры СКЦ МИД России.. 183

5. ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ, ГЕОИНФОРМАЦИОННЫЕ И
БИОМЕТРИЧЕСКИЕ СИСТЕМЫ В МЕЖДУНАРОДНОЙ ПРАКТИКЕ.. 188

5.1. Мониторинг глобального информационного пространства
информационно-аналитическими системами США и их союзников. 188

5.1.1. «Под колпаком» лидеры государств

и иностранные дипломаты.. 192

5.2. Основные параметры
некоторых отечественных ИАС.. 196

5.2.1. «Медиалогия». 196

5.2.2. ИАС «Семантический архив 4.5». 203

5.2.3. ИАС «Демон Лапласа» против террористов. 205

5.2.4. Prognoz platform.. 207

5.2.5. Иные системы прикладного анализа. 210

5.3. Геоинформационные системы
по глобальным техногенным, природогенным
и иным чрезвычайным ситуациям.. 220

5.4. Биометрические технологии
в консульской службе. 225

5.4.1. Электронные визы в Россию.. 231

6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
В ДИПЛОМАТИЧЕСКОЙ ПРАКТИКЕ — НАЦИОНАЛЬНОЕ

И МЕЖДУНАРОДНОЕ ИЗМЕРЕНИЕ.. 233

6.1. Ключевые положения
Доктрины информационной безопасности Российской Федерации (2016) 233

6.2. Особенности обеспечения информационной безопасности загранучреждений как объектов критической инфраструктуры.. 236

6.2.1. Федеральный закон «О безопасности
критической информационной инфраструктуры Российской Федерации» 237

6.2.2. Система обнаружения, предупреждения
и ликвидации последствий компьютерных атак
на информационные ресурсы России (СОПКА) 242

6.2.3. Система центров реагирования
на компьютерные инциденты в информационно-телекоммуникационных сетях (CERT) 24
6

6.3. Ботнеты, вирусы, шпионские программы
и методы борьбы с ними.. 249

6.3.1. МИД России и его загранучреждения
как объекты компьютерных атак. 249

6.3.2. Вирусы, шпионские программы
и методы борьбы с ними. 251

6.3.2.1. Каналы проникновения. 253

6.3.2.2. Угрозы шпионских программ
и способы их нейтрализации. 256

6.3.2.3. Федеральный закон от 29 июля 2017 года № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и защите информации» 259

7. СПЕЦИФИКА ДИПЛОМАТИЧЕСКОЙ
ДЕЯТЕЛЬНОСТИ В ДИСКУРСЕ
МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ГИБРИДНЫХ ВОЙН 2
63

7.1. Составляющие гибридных войн
и международной информационной
безопасности.. 263

7.1.1. Военно-политическая страта. 266

7.1.2. «Кибербомбы» Б. Обамы.. 273

7.2. Информационные технологии гибридных войн.. 275

7.2.1. Концепт «гибридной войны» России. 276

7.2.2. Гибридная война — подходы США. 279

7.2.3. Гибридные войны: базовые позиции НАТО.. 281

7.2.3.1. Саммит НАТО в Варшаве (2016)
о гибридных войнах. 282

7.2.3.2. Центр передового опыта НАТО в Таллине — идеолог кибервойн 284

7.2.3.3. Стратком НАТО в Риге —
центр «холодной войны 2.0». 286

7.2.3.4. Центр НАТО и ЕС в Хельсинки
по противодействию гибридным угрозам.. 290

7.2.4. Оперативная рабочая группа
по стратегическим коммуникациям ЕС — инструмент дезинформации и фальсификации 291

7.3. Дипломатические инициативы России
по обеспечению МИБ.. 293

Заключение. 298

Приложение 1. 302

Приложение 2. 325

Глоссарий. 328

Abstract 339

Об авторе

ПРЕДИСЛОВИЕ

Применение информационно-коммуникационных технологий (ИКТ) для реализации интересов человека, общества и государства в последнее время все более активно расширяет свое место в перечне факторов, определяющих направления развития человечества. Это обусловлено, с одной стороны, масштабностью последствий

расширения областей применения ИКТ и использования глобальной информационной инфраструктуры для развития экономики, социальной и политической сфер многих государств мира, позволивших некоторым специалистам говорить об изменении технологического уклада жизни общества, а с другой — стремительностью, с которой информационно-коммуни-кационные технологии превращаются в среду реализации разнообразных общественных отношений, создавая новые условия для решения проблем обеспечения безопасности людей, частного сектора и выполнения функций государственного управления. Информационно-коммуникационные технологии существенно изменили пространство выполнения государствами внешнеполитических задач, решения проблем поддержания международного мира и безопасности.

Осмысление этого нового явления жизни национальных обществ и международного сообщества, противодействие негативным тенденциям развития и использования информационно-коммуникационных технологий для разрешения противоречий в межгосударственных отношениях, для осуществления деятельности международных террористических и иных преступных организаций становится все более настоятельной потребностью человеческой цивилизации. Практическая безграничность влияния этих технологий на жизнь людей порождает и необозримость проблем предотвращения злонамеренного и враждебного использования информационных технологий в ущерб суверенитету государств, их территориальной целостности и политической независимости, международному миру и безопасности.

Сложность возникающих в этой области проблем наглядно демонстрирует и неудачное завершение деятельности очередного набора (2016) Группы правительственных экспертов ООН
по достижениям в области информатизации и коммуникации, которые не смогли преодолеть разногласий по поводу выбора приоритетных направлений международного сотрудничества в среде информационно-коммуникационных технологий.

Автор представляемой работы, Смирнов Анатолий Иванович, главный научный сотрудник Центра международной информационной безопасности и научно-технической политики МГИМО МИД России, доктор исторических наук, профессор, с научных позиций предпринял попытку анализа ситуации, складывающейся в области влияния научно-технической революции в области информационно-коммуникационных технологий на развитие международных отношений. Автор предлагает свою оценку процессов, происходящих в рассматриваемой сфере, существующих проблем информационной безопасности глобального и национального масштаба и возможных путей их решения.

Позиция автора создает широкое пространство для дискуссий и одновременно расширяет представление о комплексном, междисциплинарном характере исследуемых процессов, порождает новые возможности для проведения научных исследований и подготовки практических рекомендаций по укреплению режима международной информационной безопасности.

Уверен, что монография А.И. Смирнова будет интересна широкому кругу читателей, а также ученым и специалистам, занимающимся данной проблематикой.

*Директор Института проблем информационной безопасности
МГУ им. М.В. Ломоносова,
член научного совета при Совете Безопасности Российской Федерации,
член-корреспондент Академии криптографии Российской Федерации,
председатель Международного консорциума
по международной информационной безопасности*

В.П. Шерстюк

К ЧИТАТЕЛЮ

Планета охвачена беспрецедентной технологической рево-люцией. Её драйвером последние полвека стали информационно-коммуникационные технологии (ИКТ). Их феномен поражает количественными и качественными масштабами, но главное — тем влиянием, которое ИКТ оказывают на личность, общество и го-сударство, в том числе и на его внешнеполитическую сферу.

Проводимый США и их союзниками курс на сдерживание России, оказание на нее политического, экономического и информационного давления с помощью новейших ИКТ вызвал серьезный кризис в международных отношениях.

В этом контексте исключительно актуальна монография главного научного сотрудника Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России (ЦМИБ), д.и.н, профессора А.И. Смирнова «Современные информационные технологии в международных отношениях», выполненная согласно плану работы ЦМИБ.

Как представляется, системно проведенное исследование весьма информативно. Несомненный интерес представляет глава о мегатрендах цифровой эпохи, ибо наряду с данными Международного союза электросвязи по измерению информационного общества и индексу развития ИКТ в странах мира рассматриваются «Интернет вещей» и технология «блокчейн», как драйверы Industry 4.0.

Особый интерес представляет анализ возможностей и угроз НБИК-технологий и искусственного интеллекта для матрицы национальной и международной безопасности.

Детально проработаны теоретические и практические аспекты использования новейших ИКТ как «мягкой силы 2.0.» ведущих стран мира, в том числе с учетом исследований использования социальных сетей в дипломатической практике Оксфордского университета, а также различных технологий манипуляции и цифровых фейков в информационных войнах.

Принимая во внимание рост конфликтного потенциала в мире, особо актуален обзор ситуационно-кризисных центров внешнеполитических ведомств ряда зарубежных стран и России, а также применяемых в них информационно-аналитических, геоинформационных и иных систем, в т.ч. когнитивного анализа и прогнозирования международных конфликтов.

В условиях беспрецедентного обострения международных отношений

заинтересованному читателю будет несомненно полезен анализ информационной безопасности в дипломатической практике с учетом ключевых положений Доктрины информационной безопасности Российской Федерации (2016), Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (2017), Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России (СОПКА) и Системы центров реагирования на компьютерные инциденты (CERT).

Принимая во внимание, что МИД России и его загранучреждения все чаще становятся объектами компьютерных атак, весьма важны такие практические вопросы, как методы борьбы с ботнетами, вирусами, шпионскими программами, цифровыми фейками и т.д.

Завершает работу анализ специфики дипломатической деятельности в дискурсе МИБ и гибридных войн, в котором рассмотрены информационные составляющие угроз со стороны США и НАТО, включая антироссийскую деятельность центров киберзащиты в Таллине и по стратегическим коммуникациям в Риге, Центра НАТО и ЕС в Хельсинки по противодействию гибридным угрозам, а также оперативной группы по стратегическим коммуникациям ЕС.

Но одной из наиболее острых и опасных в стратегическом плане является проблема возможного применения ИКТ и, в частности, Интернета в целях, не совместимых с задачами обеспечения международной и национальной стабильности и безопасности. Становится очевидным, что «поигрывание технологическими мускулами» толкает человечество в сторону конфронтации.

В этом контексте безусловно полезными для читателей будет представленный в заключении анализ направленного против России закона «О противодействии противникам Америки посредством санкций», который позволяет США вводить новые санкции за «деятельность, подрывающую кибербезопасность <…> в интересах правительства Российской Федерации».

В противовес такому милитаристскому подходу Россия продвигает на международной арене целый ряд миротворческих инициатив в сфере МИБ. Среди них проект «Правил ответственного поведения в области обеспечения МИБ» и Концепция конвенции об обеспечении международной информационной безопасности, призванные установить «правила честной игры» в информационной сфере.

Специальный представитель

Президента Российской Федерации

по вопросам международного сотрудничества

в области информационной безопасности,

посол по особым поручениям,

Директор Центра международной

информационной безопасности

и научно-технологической политики

МГИМО МИД России

доктор исторических наук, профессор

А.В.КРУТСКИХ

Abstract

The digital age dictates new trends in international relations.
The monograph by A. I. Smirnov "Modern information technologies in international relations" systematically examines megatrends of the development of ICT as the locomotive of the socialization of mankind, as well as their role in the modern information support of the foreign policy process, including "soft power 2.0". In the conditions of development of Industry 4 and NBIC-technologies, new opportunities and challenges for the matrix of national and international security are being explored.

In the book, taking into account foreign experience, the role of innovative digital technologies is considered in detail, incl. Cognitive information-analytical and geo-information systems in such topical areas as situational-crisis and electronic diplomacy.

In the context of aggravation of global competition, special attention is paid to the theoretical and practical aspects of ensuring the security of diplomatic missions, as critical information infrastructure facilities, methods of combating viruses and spyware, as well as in the discourse of threats to international information security and hybrid wars.

Given the rapid processes of strengthening the role of digital technologies in geopolitical competition, the book can be useful for a wide range of readers interested in such topical areas of international relations.

. 340