УДК 327.56 DOI 10.18698/2306-8477-2016-09-379

Кибердипломатия: новые вызовы международного морского пиратства и методы информационного противоборства

© Д.А. Цезарь

Дипломатическая академия МИД России, Москва, 119021, Россия

Проанализирована новая эволюционная форма международных отношений — информационная, или кибердипломатия. Рассмотрены вызовы, стоящие перед международным сообществом в рамках международных отношений, а также феномен интернет-дипломатии как основы стратегии государственного аппарата при регулировании общественных отношений в сфере «общественной» дипломатии. Наряду с внедрением информационной дипломатии в основы государственного управления показано использование СМИ в своих целях международной пиратской и террористической средой, что усиливает стоящие перед державами угрозы, превращая их в глобальные проблемы современности. Отмечена необходимость усиления законодательного регулирования и обеспечения государственного контроля над информационной безопасностью стратегически важных данных.

Ключевые слова: *пиратская среда, международный терроризм, кибердипломатия, информационная дипломатия, международное морское пиратство, информационная безопасность, государственный контроль, информационный терроризм.*

Эволюция международного сотрудничества как предпосылка для информационно-сетевой войны. Государства на протяжении исторического пути развития и становления пытаются применить для достижения внешнеполитических целей, укрепления позиции и создания позитивного восприятия на международном уровне как можно более широкий набор средств.

Исследования политологов Жюля Камбона и Франсуа Кальера позволяют разделить этапы эволюции международного сотрудничества на «старую» и «новую» дипломатии. При этом «старая» дипломатия носит черты диспотичной, монархической и напрямую связана с понятием «тайная дипломатия», включающим в себя закрытые переговоры и договора, и опирается на обычаи. Применение СМИ и новых средств связи создало предпосылку к возникновению «новой» дипломатии.

«Старую» дипломатию также называют французской, или европейской. Одной из основных ее доктрин является принцип равновесия сил, состоящий в том, чтобы ни одна из стран не превосходила другую. Чтобы сохранить данный принцип, страны вступали в союзы для уравновешивания вырвавшейся вперед державы. Американский

ученый Р. Каплан отмечает, что Европа уже не является центральной ареной XXI в. ввиду наличия у современных систем международных отношений сформированных правил адаптации к изменениям политической среды. В «новой» дипломатии акцент международных отношений смещен на Восток. Об этом пишет О.П. Иванов в исследовании военно-политической стратегии ведущих держав в Азиатско-Тихоокеанском регионе (АТР), приводя доводы в пользу того, что Индийский океан и АТР превратились в центр притяжения внимания главных участников международных отношений и мировой политики [1].

«Новая» дипломатия в большей степени, чем «старая», отводила место аналитической информации, носившей научный характер. Особенно важное место занял анализ международных отношений, мировой политики и экономики. Значительно стала меняться роль общественности в политике, и в этой связи расширяется методология «информационной дипломатии». Ее также отличают оперативность и скорость принятия решений управленческого характера. При этом принято считать, что «новую» дипломатию особенно плодотворно внедряли СССР и США.

Ряд ученых отмечают смену курса дипломатии с абсолютистского на курс демократического контроля. Данная смена курса обоснована превалированием фактора чувства общности между народными массами, растущим у населения государства пониманием значения общественного мнения, увеличением путей сообщения и способов связи. В пример можно привести Великобританию, Германию при Гитлере, Италию при Муссолини.

Рост глобальных и региональных проблем совместно с усилением влияния на международные отношения СМИ привел к формированию определения «информационная», или «кибердипломатия». Считается, что информационная дипломатия распространяет свое влияние на все ветви власти: законодательную, исполнительную и судебную. СМИ используются государством для создания более широкой опоры для руководства и правящей элиты иностранных государств. Интенсивность использования информатизации в политике сформировала тенденцию к открытости политических дебатов, общественным обсуждениям законопроектной деятельности.

Сотрудничество стран между собой и с международными организациями призвано совершенствовать и укреплять глобальную международную безопасность, создавать эффективные механизмы противодействия новым угрозам, новым вызовам безопасности, таким как терроризм (в том числе международный), киберпреступность, морское пиратство. Это явилось предпосылкой для определения в качестве приоритета внешней политики Российской Федерации взаимо-действия с международными организациями и странами в сфере противодействия вышеуказанным угрозам в XXI в.

В этой связи целесообразно отметить в числе новых вызовов международному сообществу методы информационно-сетевой войны. Термин впервые введен в научный оборот Бэзилом Генри Лиддел Гартом и был проводником для концепта «мягкая сила» в опубликованном им в 1941 г. в Лондоне труде «Стратегия непрямых действий». В отличие от Ганса Дельбрюка, выделявшего социальное обеспечение армии на примере римских легионов, принимавших участие в битвах при Марафоне, Гавгамелах, Заме, как преимущество силовой направленности государства [2], и Карла фон Клаузевица, видевшего в качестве основного вектора применения боевых действий измор и сокрушение [3], Лиддел Гарт полагал, что основной целью войны является не полное уничтожение вооруженных сил и экономического потенциала вражеского государства, а принуждение правящих кругов враждебной страны (или даже нескольких государств-противников) к принятию таких условий, которые бы полностью отвечали политическим, экономическим, военным интересам государства-агрессора [4].

Концепция информационно-сетевых войн значительно подтвердила свое влияние в настоящее время. Цифровая дипломатия, ранее представленная как закрытая сфера деятельности, в связи с развитием информационного общества приобрела законодательное закрепление в основных доктринальных документах государств. Так, инструментарий информационно-коммуникационных технологий содержится в Концепции внешней политики Российской Федерации от 12 февраля 2013 г. как опорный комплексный инструментарий для «мягкой силы», а также в Стратегии национальной безопасности США от 15 февраля 2015 г. как обеспечительный аппарат разведывательных служб [5]. И. Сурма рассматривает информационно-телекоммуникационные сети в качестве дипломатического инструментария ресурсов государств, включающего средства по созданию благоприятного имиджа государства за счет формирования общественного мнения (на примере компаративного анализа ведомственных сайтов Министерств иностранных дел Российской Федерации, Французской Республики и Италии) [6]. В этой связи также следует отметить показательный пример формирования СМИ негативного образа государства — события после оранжевых революций на Украине 2005 и 2015 гг. По причине политики «мягкой силы» США после наложения ряда санкций Россия фактически оказалась в экономической изоляции. По итогам докладов в Европейском парламенте наряду с возрастающей степенью осуждения действий Российской Федерации в отношении Украины у бывших членов Варшавского договора и прибалтийских государств также усматривается публичное признание эффективности ее действий по защите собственных интересов некоторыми из перечисленных стран.

Кроме того, достаточно распространенной политикой в настоящее время является проводимое государствами повышение открытости информации о правосудии, здравоохранении, органах исполнительной и законодательной власти.

Вместе с тем увеличение возможностей доступа к информационно-телекоммуникационным сетям, социалиальная электронификация общества ведут к формированию особой зоны риска. Незащищенные информационные каналы в рамках концепции обеспечения международной безопасности провоцируют возможность применения информационно-коммуникационных технологий в целях, несовместимых с задачами обеспечения международной стабильности и безопасности.

В пользу вышеизложенного свидетельствуют доводы французского политолога Поля Вирилио, в соответствии с которыми террор всегда ориентировался на СМИ, перенося территорию несущих угрозу событий на экран телевизора и дисплей компьютера.

Отчеты об оценке влияния информационно-сетевой войны, проведенной ВМС США, выделяют Россию, Китай, Индию и Кубу в качестве стран, проводящих политику подготовки к информационной войне. Активными в указанной политике государствами в данных отчетах представляются Франция, Япония и Германия. Также оценены экономические затраты государств на информационно-сетевые разработки: 120 млрд долларов в год [7].

Наиболее опасную роль в информационно-сетевой войне государств играют ее спутники, невидимые акторы. Информация и информационная инфраструктура в настоящее время являются наиболее опасным оружием, используемым на мировой арене акторами различного масштаба как на уровне международных и национальных структур противоборствующих государств, так и в масштабе террористических и пиратских сред, представляющих собой источники глобальных угроз современности.

Кибердипломатия (digital diplomacy) представлена в законодательстве США как применение социальных сетей в дипломатической практике. Вместе с тем это обобщенное определение в дальнейшем получает развернутую классификацию, в которую входят: создание молодежного протестного движения, объединение пользователей вокруг интерактивного радио и телевидения, мобилизация групп оппозиционеров, формирование диалога между представителями правительства и блогерами и др.

Согласно исследованиям И. Сурмы, цифровая дипломатия несет более широкую смысловую нагрузку и, являясь формой публичной дипломатии, представляет собой механизм влияния на зарубежную аудиторию посредством методов размещения радио- и телепередач в сети Интернет, распространения в открытом доступе литературы в

цифровом формате, мониторинга блог-дискуссий, электронных рассылок информации, создания сайтов политиками и политическими формированиями [8].

Современные исследователи проблематики информационно-психологического противоборства выделяют укрепление информационной безопасности в качестве средства реализации целей и обеспечения интересов государств [9]. Также следует отметить, что пропорционально увеличению запросов субъектов информационного противоборства (государств, международных организаций, вооруженных формирований и организаций пиратской, террористической, экстремистской, радикальной политической направленности, транснациональных корпораций) наблюдается эволюция методов информационного противоборства.

При написании данной статьи был привлечен достаточно широкий круг источников, среди которых публикации официальных нормативных правовых документов и выступлений, издания различных органов исполнительной власти, научные публикации зарубежных и отечественных ученых, исследовавших тематику кибердипломатии и проявлений международного морского пиратства. Для полноты исследования и сравнения были использованы официальные документы законодательной ветви власти, основные положения которых проанализированы в рамках исследования применения пиратской и террористической средой методов информатизации для достижения преследуемых целей.

Важным источником информации, содержащим большое количество значимых фактов касательно исследования природы пиратской среды, являются книги М. Вершинина «Психологические особенности членов деструктивных и террористических (радикальных) групп» и Г. Тревертона «Пиратство, организованная преступность и терроризм». Исследования ученых взаимно дополняют друг друга и дают понятие о структуре пиратской среды. На основании данных исследований изучена возможность применения методов информационной дипломатии пиратами.

В качестве теоретико-методологической базы исследования выступили использованные в процессе исследования законы и принципы политической науки, историко-политический, формально-юридический методы, метод политического прогнозирования, дискурс-анализ и системный подход.

Информационная разведка — угроза безопасности морских пространств. Рассматривая вопрос применения информационного ресурса в качестве инструментария пиратской и террористической средой следует напомнить системообразующие элементы указанных сред.

Согласно М. Вершинину, пиратская среда — это насильственная радикально-культовая среда, состоящая из идеологического центра

специальных формирований и социальной базы. Г. Тревертон углубляется в изучение особенностей окружения идеологического центра и предполагает окольцование его криминальными общностями (формированиями) в результате определенных предпосылок для усиления указанных формирований: ослабленные законодательные рычаги, экономические (в том числе торговые) отношения между странами и политические (в том числе управленческие) проблемы в отдельных регионах.

Пиратская среда является сложным системообразующим элементом, который формирует пиратскую обстановку в регионе.

Сходное строение обозначено и у террористической среды.

Таким образом, идеологический центр, снабженный достаточным информационным ресурсом, имеет тенденцию к расширению и превращается в угрозу безопасности акваторий отдельных стран, угрозу международной и региональной безопасности.

Рассмотрим информационную разведку как социально-политическое явление. Немецкий ученый Никлас Луман предлагает рассматривать коммуникацию как синтез трех составляющих: информации, сообщения и понимания. Исходя из этого, можно предположить, что первичной основой взаимодействия политических субъектов в процессе коммуникации между пиратами и обществом является насилие.

Это коррелируется с системой концептов, формирующих политическое определение международного морского пиратства, которое представляет собой, с одной стороны, социально-политическое явление, при котором осуществляется насилие (или угроза насилия), направленное на захват чужой собственности в море пиратскими группами с целью получения финансового дохода, воздействия на конкурирующую компанию, а также выполнения задач политического, экономического и военного характера в условиях противоборства акторов международных отношений, а с другой — преступление международного характера, совершаемое в морском пространстве против физических, юридических лиц и государств, которое может привести к подрыву международной стабильности и снижению уровня международной безопасности.

Международное морское пиратство произрастает из пиратской среды. На основании исследований, приведенных указанными учеными-политологами, представляется целесообразным уточнить определение пиратской среды с учетом выявленных современных особенностей и условий ее существования. Пиратская среда — это насильственная радикально-культовая среда, в которую входят идеологический центр, пиратские формирования, военизированные (силовые) и социальные структуры, охваченные торговыми, финансо-

выми, информационными и политическими взаимосвязями. Пиратская среда является системообразующим элементом, который формирует пиратскую обстановку в регионе. Рассматривая этот элемент, можно выявить роль пиратских формирований, снабжающих идеологический центр результатами информационной разведки в пиратоопасных регионах в Аденском заливе (Сомали), Юго-Восточной Азии (Вьетнам, Сингапур, Тайланд) и Гвинейском заливе (Либерия, Нигерия).

Пиратство как социально-политическое явление является важнейшим источником средств к существованию целых групп населения (что имеет место, например, в Сомали), а также транснациональной деятельностью для извлечения преступных сверхдоходов, в том числе посредством шантажа конкретных корпораций и транспортирующих компаний. В сложные периоды международных отношений пиратство может выступать орудием дестабилизации политической обстановки в регионе, а также воздействия на конкретное государство для достижения политических целей. Таким образом, в случае использования пиратами информационной разведки можно спрогнозировать немалый размер ущерба, влекомый объектом криминальных деяний, и оценить риски (угрозы) его применения пиратской средой.

Информационную разведку морских пространств можно отнести к разновидности информационного терроризма. В соответствии с определением, приведенным Центром политического анализа и информационной безопасности, это особая форма насилия, представляющая собой сознательное и целенаправленное информационное воздействие или угрозу применения такого воздействия для принуждения правительства к реализации политических, экономических, религиозных и иных целей террористической организацией или отдельными террористами, сопровождаемое эмоциональным воздействием на общество для возбуждения в нем страха, панических настроений, потери доверия к власти и создания политической нестабильности [10].

Угрозой информационным ресурсам может быть деятельность космических, воздушных, морских и наземных технических средств разведки иностранных государств. Некоторые виды данной разведки включают в себя следующие мероприятия:

- сбор и анализ данных из открытых источников;
- несанкционированные отключения объектов от источников питания, а также из-за доступа к информации и вычислительным ресурсам. В частности, в 2015 г. сотрудники Федеральной службы безопасности Российской Федерации отразили свыше 1 млн 200 тыс. хакерских атак, причем более 280 тыс. из них были направлены на сайт Президента Российской Федерации;

• распространение информации террористического или экстремистского содержания для реализации пиратскими и террористическими структурами преступных замыслов в сети Интернет, а также посредством телевидения, радио, периодических изданий;

• бизнес-разведка, т. е. похищение информации стратегического назначения посредством внедрения агентов в структуру объекта информационной угрозы, например транснациональной корпорации, промышленного предприятия, синдиката. Другое определение бизнес-разведки (конкурентной разведки) — особый вид информационно-аналитической работы, позволяющий собирать обширнейшую информацию о юридических и физических лицах без применения специфических методов оперативно-разыскной деятельности, являющихся исключительной прерогативой государственных правоохранительных органов и спецслужб.

Значительный вклад в исследования в области обеспечения безопасности цифровой информации в разрезе конкурентной разведки принадлежит Б. Шнайеру, основателю криптографической компании Counterpane Internet Security, Inc. Им определены основные директивы защиты информации от бизнес-разведки, а также от политической и экономической разведки, сформулирован ряд доводов в пользу совершенствования использования террористической и пиратской средами методов информационной разведки и кибердипломатии. По его мнению, средства министерств внутренней безопасности ведущих государств должны быть вложены в развитие разведывательных управлений и служб реагирования на чрезвычайные ситуации. Защищаться от масштабной угрозы терроризма, как правило, лучше, чем сосредотачиваться на конкретных потенциальных террористических заговорах. Шнайер отмечает, что, несмотря на сложность анализа разведывательных данных, этот способ является лучшим для борьбы с глобальным терроризмом. Человеческий интеллект имеет преимущества по сравнению с автоматизированным и компьютеризированным анализом, при этом увеличение количества собранных разведывательных данных не поможет улучшить процесс анализа. Различным агентствам, созданным во время холодной войны, не свойственен обмен информацией. Однако практика обмена информацией очень важна при борьбе с децентрализованными и плохо финансируемыми противниками, такими как Аль-Каида [11];

• прослушивание радиоканалов из-за границы;

• наблюдение при помощи разведывательных спутников.

На фоне приведенной классификации, отнюдь не исчерпывающей, поскольку с каждым годом увеличиваются и совершенствуются методы хищения информации, следует отметить увеличение количества уголовных дел, связанных с преступлениями в сфере информа-

ционных технологий. В 2007 г. количество таких уголовных дел составляло 4,5 тыс., в 2008 г. оно превысило 5,5 тыс., в 2009 г. — около 8 тыс. [12].

Практика борьбы с международным морским пиратством и терроризмом показывает, что эффективность международных усилий по противодействию данным глобальным угрозам снижена ввиду отсутствия согласованного механизма по объединению усилий заинтересованных государств. Данная проблема могла возникнуть из-за того, что в определениях и мерах наказания, применяемых рядом стран, нет единообразия.

Представляется целесообразным гармонизировать используемые в национальном и международном праве понятия терроризма, морского и информационного пиратства, придать им единообразную смысловую нагрузку, а также создать профильные региональные организации по борьбе с данными явлениями посредством заключения заинтересованными сторонами партнерских соглашений по организации и осуществлению противодействия пиратству.

В этой связи стоит привести положительный опыт создания и дальнейшей имплементации в Малайзии, Индонезии и Брунее нормативно-правового комплекса мер, унифицирующего национальные правоохранительные системы в сфере противодействия морскому пиратству, — Модель национального законодательства по борьбе с пиратством и насильственными преступлениями на море, созданную Международным морским комитетом в 2001 г. Модель содержит набор юридических процедур по захвату, задержанию и уголовному преследованию пиратов в территориальных водах сопредельных государств [13].

Модель содержит эффективные для определенных пиратоопасных регионов комплексы юридических мер. Вместе с тем для применения модели мировым сообществом требуется ее дальнейшая унификация.

Ответ информационно-сетевой угрозе. Методы информационного противоборства. Цифровая дипломатия превратилась в грозную силу. Стремление радикальных организаций к обретению информационного контроля порождает новые формы международных конфликтов.

Информационное пространство объективно становится предметом пристального внимания как со стороны криминального сообщества (террористов, пиратской среды), так и со стороны сил, противостоящих ему.

Ввиду того что защита национального информационного пространства является приоритетным направлением в осуществлении концепции национальной безопасности современного государства, в противовес усилиям пиратской и террористической среды между-

народное сообщество вынуждено разрабатывать инновационные методы противодействия. Так, для усиления контроля и надзора в области противодействия пиратству на море и в авиации регулярно проводятся заседания коллегии Федеральной службы по надзору в сфере транспорта. Например, 25 марта 2014 г. состоялось расширенное заседание данной коллегии, посвященное обеспечению мер в области безопасности на транспорте. В числе достижений последнего времени отмечены Комплексная информационная система управления контрольно-надзорной деятельностью, направленная на обеспечение контроля и надзора, в том числе дистанционного, в области транспортной безопасности за нарушениями на всех объектах инфраструктуры, а также ведение непрерывного мониторинга состояния безопасности транспортного комплекса [14].

В свете изложенного следует отдельно отметить эффективность системы непрерывного мониторинга, созданной Международной гражданской авиационной организацией ИКАО [15] в области обеспечения авиационной безопасности. Положительные аспекты данного мониторинга приведены в докладах участников Международного семинара ИКАО по проведению контроля в сфере обеспечения авиационной безопасности с использованием механизма постоянного мониторинга, состоявшегося 2–4 июня 2014 г. в Москве. Некоторые положения представляются целесообразными в отечественной практике мер безопасности как в авиации, так и на море, для обеспечения противодействия пиратству. Надо отметить, что в настоящее время статистика воздушных пиратских актов также представляет собой политические захваты. В качестве примера можно привести перехват российского гражданского лайнера «Сирийские авиалинии»с экипажем по маршруту из Москвы в Дамаск, осуществленный 11 октября 2012 г. турецкими истребителями в воздушном пространстве Анкары, по выводам зарубежных СМИ, в связи с политическим видением США, а также с целью не допустить военные поставки в Дамаск [16].

Говоря об эффективности положений механизма постоянного мониторинга, для обеспечения противодействия пиратству на море представляется необходимым проведение анализа критических элементов системы надзора за обеспечением национальной безопасности государств, введение практики универсальных проверок в сфере обеспечения безопасности, протокольное отражение нарушений безопасности в соответствии с международными соглашениями, регулирующими пиратство, и национальными стандартами, а также проведение государствами оценочных мероприятий по контролируемым регионам особой опасности, направленных на устранение негативных последствий выявленных угроз.

Механизм непрерывного мониторинга предполагает четкое разделение контролируемых зон (в случае противодействия морскому пиратству — акваторий), а также применение моделей рисков в области безопасности. Результаты деятельности национальных служб в области обеспечения безопасности на море в соответствии с принципами непрерывного мониторинга должны подвергаться оперативному анализу и сводиться в диаграммы, отражающие состояние объектов мониторинга (персонал, безопасность в портах, контроль доступа к информации, состояние оборудования оборонного назначения, обеспечение безопасности пассажиров, груза и багажа, транспортная документация, международные, региональные и локальные нормативно-правовые акты в области транспортной безопасности).

Целесообразно также включить в мероприятия мониторинга осуществляемый в настоящее время Европейским агентством морской безопасности мониторинг общего функционирования европейского портового контрольного режима. В рамках осуществления данного вида мониторинга Европейским агентством разработаны стандарты безопасности.

К мерам информационно-сетевого противодействия можно также отнести создание специальных штабов по противодействию глобальным угрозам в рамках мер нормативно-правового регулирования. В частности, согласно Указу Президента Российской Федерации от 26 декабря 2015 г. № 664 «О мерах по совершенствованию государственного управления в области противодействия терроризму», для организации планирования применения сил и средств федеральных органов исполнительной власти и их территориальных органов по борьбе с терроризмом, управления контртеррористическими операциями в территориальном море, исключительной экономической зоне, на континентальном шельфе Российской Федерации, в других морских пространствах, в пределах которых Российская Федерация осуществляет суверенитет, суверенные права и юрисдикцию, а также на судах, плавающих под Государственным флагом Российской Федерации, в городах Мурманске, Каспийске, Южно-Сахалинске, Петропавловске-Камчатском, а также в Севастополе формируются оперативные штабы, управляемые Федеральным оперативным штабом.

В приложении к данному Указу, Положении о Национальном антитеррористическом комитете, в качестве функций комитета обозначены мониторинг состояния общегосударственной системы противодействия терроризму, информационное сопровождение деятельности по противодействию терроризму, а также своевременное информирование населения через СМИ о преступлениях террористической направленности или об угрозах их совершения, а также о мерах по минимизации и (или) ликвидации последствий таких преступлений.

Из данного примера можно сделать вывод, что законодательным актом сформирован перечень мер по оказанию информационного противодействия терроризму.

Стратегическое планирование противодействия глобальным угрозам в сфере защиты информационной безопасности. Стратегическое планирование является особенно важным аспектом формирования действий государства по отношению к выявленным угрозам.

Основополагающим нормативно-правовым актом, определяющим основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности, являются Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г., утвержденные Президентом Российской Федерации 24 июля 2013 г. № Пр-1753.

Настоящие Основы предназначены для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения; для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области; для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности; для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

Документом введен термин *международная информационная безопасность* — это состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Следующим важным нормативным правовым актом, устанавливающим совокупность методов защиты информационных ресурсов органов государственной власти Российской Федерации, а также определяющим основы информационной безопасности в области противодействия угрозам хищения сведений федерального назначения, столь часто применимых в 2014–2016 гг. морскими пиратами для получения информации о грузопотоках стратегического назначения, является Концепция государственной системы обнаружения,

предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденная Президентом Российской Федерации 12 декабря 2014 г. № К 1274.

Данной Концепцией утверждена Система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России, созданная на основе Указа Президента Российской Федерации № 31с от 15 января 2013 г. В составе Концепции определены силы (уполномоченные силовые подразделения) и средства (технологические решения) обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Органом государственной власти, правомочным осуществлять создание и функционирование Системы, является ФСБ России.

В Концепции перечислены следующие функции по обеспечению информационной безопасности интернет-ресурсов, возложенных на Систему:

- выявление признаков проведения компьютерных атак;
- разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- формирование детализированной информации об информационных ресурсах РФ, находящихся в зоне ответственности Системы (т. е. ресурсов органов власти);
- прогнозы в области обеспечения информационной безопасности Российской Федерации;
- организация и взаимодействие с правоохранительными органами и другими госорганами, владельцами информационных ресурсов Российской Федерации, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения компьютерных атак и установления их источников;
- организация и проведение научных исследований в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Защита информационных ресурсов органов государственной власти представляется особенно актуальной в свете усилившейся в 2015–2016 гг. активности морских пиратов, прибегающих к информационным ресурсам для получения сведений о местонахождении торговых и военных баз кораблей, перевозящих ценные и стратегически важные грузы.

Объем экономической потери государств от пиратства говорит об уязвимости экономик стран мира, а также, принимая во внимание вышеизложенную статистику информационных преступлений, о необходимости обеспечения дополнительной защиты сведений федерального значения. Указанная проблематика особенно актуальна

сейчас, во время перехода экономик многих стран в рецессию, в том числе в связи с усилением угрозы террористической группировки ИГИЛ.

Для борьбы с информационными преступлениями военного, пиратского и террористического характера в 2015 г. Министерством обороны России в Крыму создано отдельное подразделение войск информационных операций. В его задачи входит нарушение работы информационных сетей вероятного противника и в результате — нарушение функционирования его системы управления войсками, а также обеспечение кибербезопасности своих информационных сетей.

В мае 2014 г. в России сформированы войска информационных операций, предназначенные для защиты российских военных систем управления и связи. В их состав вошли части и подразделения в военных округах и на флотах, укомплектованные высококвалифицированными специалистами в области математики, программирования, криптографии, связи, радиоэлектронной борьбы [17]. Создание подобных подразделений представляется эффективным методом противодействия киберпиратству и предотвращения информационной разведки, направленной против баз данных государственного значения.

«Информационная» дипломатия призвана увеличить возможности международного сообщества по предотвращению угрозы международной информационной безопасности мирового сообщества, сформированной усилением информационного контроля со стороны пиратских и террористических формирований. В этой связи ведущим державам, безусловно, требуется скоординировать и усилить меры государственного контроля за внутренней и внешней информационной средой, определить стратегические меры противодействия информационному терроризму, гармонизировать законодательное регулирование защиты стратегически важных информационных ресурсов.

ЛИТЕРАТУРА

[1] Иванов О.П. Военно-политическая стратегия США в АТР. В кн.: *Современный мир и геополитика*. Москва, Канон+, 2015, с. 309–326.

[2] Дельбрюк Г. *История военного искусства в рамках политической истории*: в 4 т. Санкт-Петербург, Наука, 2001.

[3] Клаузевиц К. *О войне*. Москва, Эксмо, 2007, 420 с.

[4] Лиддел Гарт Б.Х. Стратегия непрямых действий. *Перспективы*. URL: http://www.perspektivy.info/book/problematika_magkoj_sily_vo_vneshnej_politike_rossii_2014-03-03.htm (дата обращения 29.02.2016).

[5] *The National Military Strategy of the United States of America 2015*. URL: http://pentagonus.ru/load/3/strategii_i_koncepcii/the_national_military_strategy_of_the_united_states_of_america_2015/31-1-0-1287 (дата обращения 10.03.2016).

[6] Сурма И. Цифровая дипломатия США в дискурсе глобальной политики. В кн.: *Современный мир и геополитика*. Москва, Канон+, 2015, с. 332–337.

[7] *Cyberwarfare*. URL: http://fas.org/irp/crs/RL30735.pdf (дата обращения 29.02.2016).

[8] Сурма И. Цифровая дипломатия США в дискурсе глобальной политики. В кн.: *Современный мир и геополитика*. Москва, Канон+, 2015, с. 328.

[9] Анненков В.И. Информационно-психологическое противоборство: современные аспекты. В кн.: *Современный мир и геополитика*. Москва, Канон+, 2015, с. 11.

[10] Аникин В.И. *Теория и практика управления во внешнеполитической деятельности*. Москва, Научная книга, 1999, 384 с.

[11] Шнайдер Б. *Исправление провалов разведки — SFGate*, 15 января 2010 г. URL: http://www.sfgate.com/opinion/article/Fixing-intelligence-failures-3202795.php (дата обращения 18.03.2016).

[12] *Стенограмма парламентских слушаний на тему «Информационный терроризм как угроза национальной безопасности Российской Федерации» от 28 октября 2010 года*.
URL: defence.council.gov.ru/media/files/41d4536b62a3ef67e769.doc (дата обращения 18.03.2016).

[13] Китаев С. О борьбе с морским пиратством в Юго-Восточной Азии. *Зарубежное военное обозрение*, 2014, № 1, с. 73–79.

[14] Касьянов А.И. Об итогах контрольно-надзорной деятельности Федеральной службы по надзору в сфере транспорта и ее территориальных управлений в 2013 году и задачах на 2014 год. *Транспортная безопасность и технологии*, 2013, № 1, с. 8–11.

[15] Медведев А. Акт воздушного пиратства: Россия предложила Турции объясниться. *Вести*. URL: http://www.vesti.ru/doc.html?id=930443&cid=9 (дата обращения 5.12.2012).

[16] Киберпреступность и киберконфликты: Россия. *TAdviser*.
URL: http://www.tadviser.ru/index.php/

Статья поступила в редакцию 26.08.2016

Ссылку на эту статью просим оформлять следующим образом:

Цезарь Д.А. Кибердипломатия: новые вызовы международного морского пиратства и методы информационного противоборства. *Гуманитарный вестник*, 2016, вып. 9. http://dx.doi.org/10.18698/2306-8477-2016-09-379

Цезарь Дарья Алексеевна — соискатель ученой степени канд. полит. наук Дипломатической академии МИД России, заместитель начальника отдела подготовки и экспертизы правовых актов Управления правового обеспечения и имущественных отношений Федерального агентства воздушного транспорта Министерства транспорта Российской Федерации. e-mail: elfdariamiheeva-007@rambler.ru

Cyber diplomacy: new challenges of international maritime piracy and methods of information warfare

© D.A. Tsesar

Diplomatic Academy of Russian Foreign Ministry, Moscow, 119021, Russia

The article analyzes the new evolutionary form of international public relations – information or cyber diplomacy. The challenges the international community is faced are examined in the framework of international relations and the phenomenon of the cyber-diplomacy is considered as the basis for strategy of the government machine in the regulation of social relations in the field of the "public" diplomacy. Along with the introduction of cyber diplomacy into foundations of state administration using mass media for by international terrorist and pirate associations for their own purposes is shown. These factors escalate the threats facing the international community, transforming them into global problems of modern age. It is noted that it is necessary to strengthen legislation and to ensure the state control over strategic data information security.

Keywords: *piracy environment, international terrorism, cyber diplomacy, informational diplomacy, international maritime piracy, information security, state control, informational terrorism.*

REFERENCES

[1] Ivanov O.P. Voenno-politicheskaya strategiya SShA v ATR [The military and political strategy of the USA in the Asia-Pacific region]. In: *Sovremennyy mir i geopolitika* [The present-day world and geopolitics]. Moscow, Kanon+ Publ., 2015, pp. 309–326.

[2] Delbruk G. *Istoriya voennogo iskusstva v ramkakh politicheskoy istorii. V 4 tomakh* [The history of the art of war within the framework of political history. In 4 volumes]. St. Petersburg, Nauka Publ., 2001.

[3] *«Vom Kriege, hinterlassenes Werk des Generals Carl von Clausewitz»* Vollständige Ausgabe im Urtext, drei Teilen in einem Band, Herausgeber: Werner Hahlweg (1. Auflage 1832–1834). Carl von Clausewitz *On War*. London, 1873 [In Russ.: Klauzevits K. O vojne. Moscow, Gosvoenizdat Publ., 1934, reprint Moscow Eksmo Publ., 2007].

[4] Liddel Hart B.H. Strategy: the indirect approach. Third revised edition and further enlarged. London, Faber and Faber Publ., 1954 [In Russ.: Liddel Gart B.H. Strategiya nepryamykh deystviy. Moscow, St. Petersburg, Inostrannaya Literatura Publ., 1957]. *Perspektivy — Prospects*. Available at: http://www.perspektivy.info/book/problematika_magkoj_sily_vo_vneshnej_politike_rossii_2014-03-03.htm (accessed February 29, 2016).

[5] *The National Military Strategy of the United States of America, 30.06.2015. The United States Military's Contribution to National Security June 2015*. Available at: http://pentagonus.ru/load/3/strategii_i_koncepcii/the_national_military_strategy_of_the_united_states_of_america_2015/31-1-0-1287 (accessed March 10, 2016).

[6] Surma I.V.Tsifrovaya diplomatiya SShA v diskurseglobalnoy politiki [Digital US diplomacy in global policy discourse]. In: *Sovremennyy mir i geopolitika* [The present-day world and geopolitics]. Moscow, Kanon+ Publ., 2015, pp. 332–337.

[7] *Cybrwarfare, CRS Report for Congress*, *RL 30735*, Nov. 15, 2000. Available at: http://fas.org/irp/crs/RL30735.pdf (accessed February 29, 2016).
[8] Surma I.V. Tsifrovaya diplomatiya SShA v diskurseglobalnoy politiki [Digital US diplomacy in global policy discourse]. In: *Sovremennyy mir i geopolitika* [The present-day world and geopolitics]. Moscow, Kanon+ Publ., 2015, p. 328.
[9] Annenkov V.I. Informatsionno-psikhologicheskoe protivoborstvo: sovremennye aspekty [The information- psychological confrontation: modern aspects]. In: *Sovremennyy mir i geopolitika* [The present-day world and geopolitics]. Moscow, Kanon+ Publ., 2015, p. 11.
[10] Anikin V.I. *Teoriya i praktika upravleniya vo vneshnepoliticheskoy deyatelnosti* [The theory and practice of management in foreign policy]. Moscow, Nauchnaya kniga Publ., 1999, 384 p.
[11] Schneier B. Fixing intelligence failures. *SF Gate of January, 15, 2010.* Available at: http://www.sfgate.com/opinion/article/Fixing-intelligence-failures-3202795.php (accessed March 18, 2016).
[12] *Stenogramma parlamentskikh slushaniy na temu "Informatsionnyy terrorizm kak ugroza natsionalnoy bezopasnosti Rossiyskoy Federatsii" ot 28 oktyabrya 2010 goda* [Transcript of the parliamentary hearings on the topic "Information terrorism as a threat to national security of the Russian Federation" dated October 28, 2010]. Available at: defence.council.gov.ru/media/files/41d4536b62a3ef67e769.doc (accessed March 18, 2016).
[13] Kitaev S. *Zarubezhnoe voennoe obozrenie — Foreign Military Review*, 2014, no. 1, pp. 73–79.
[14] Kasyanov A.I. *Transportnaya bezopasnost i tehnologii — Transport Security and Technologies*, 2013, no. 1 (32), pp. 8–11.
[15] Medvedev A. *Vesti — News.* 11.06.2012. Available at: http://www.vesti.ru/doc.html?id=930443&cid=9 (accessed December 5, 2012).
[16] *TAdviser 10.02.2016.* Available at: http://www.tadviser.ru/index.php/

Tsesar D.A., applicant for the degree of candidate of political sciences, Diplomatic Academy of the Russian Foreign Ministry, the Deputy head of the Department of Preparation and Expert Appraisal of Legal Acts, The Office of Legal Support and Property Relations of the Federal Agency for Air Transport, Ministry of Transport of the Russian Federation. e-mail: elfdariamiheeva-007@rambler.ru