УДК 321.6/.8

# ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ СОВРЕМЕННОГО ГОСУДАРСТВА И ОСНОВНЫЕ ИНСТРУМЕНТЫ ЕГО ОБЕСПЕЧЕНИЯ

**Е. Г. Зорина**

Московский государственный университет имени М. В. Ломоносова
E-mail: z-surfer@mail.ru

Статья посвящена исследованию понятия «информационный суверенитет» и основных средств его обеспечения. В статье раскрываются причины, обострившие потребность государства в формировании информационного суверенитета, выявляются основные составляющие последнего. Анализируются и концептуализируются понятия политики «информационного щита» и политики «информационного меча», рассматриваются различия между ними, ресурсы, необходимые для их проведения.

**Ключевые слова:** информационный суверенитет, информационный щит, информационный меч, информационное противоборство, СМИ, постинформационное общество.

**Informational Sovereignty of Contemporary State and the Main Instruments of its Ensuring**

**E. G. Zorina**

The article is devoted to the study of the concept of "information sovereignty" and the basic means of its implementation. The article reveals the reasons that have aggravated the demand of the state for the construction of information sovereignty. Moreover, the paper reveals the main components of it. Further in the item, the concepts of the "information shield" policy and the "information sword" policy are analyzed and conceptualized. The differences between them are detected, the resources necessary for their realization are analyzed.

**Key words:** informational sovereignty, informational shield, informational sword, informational confrontation, mass media, postinformational society.

DOI: 10.18500/1818-9601-2017-17-3-345-348

Начиная с 1991 г. как в публицистике, так и в научной литературе всё чаще поднимается проблема информационных войн, в особенности их идеологических и психологических составляющих[1]. Актуализация методов таких войн, по нашему мнению, произошла в конце XX – начале XXI вв. по трём основным причинам.

Так, своеобразные информационные атаки применялись еще в Древнем мире[2], однако современную форму они приобрели в XX–XXI вв. под натиском страха перед последствиями применения ядерного оружия. Использование последнего даже одной стороной в прямой «горячей» войне может стать причиной уничтожения не только человеческой цивилизации, но и всего живого на планете. Так, страх перед «ядерным апокалипсисом» стал первой причиной трансформации «горячих» прямых военных столкновений между империями в состоянии скрытого противостояния, в том числе информационного.

Вторая причина высокой популярности методов информационных противоборств кроется в основных чертах пост-информационного общества, таких как всеобщая электронизация и компьютеризация, распространение сети Интернет по всему миру, маргинализация научного знания, выход на первый план индустрии развлечений, религии и паранауки, появление новых ценных информационных ресурсов. Они буквально произвели революцию в области доступа к информации, кардинально изменили отношение к ней и создали благоприятные условия для применения технологий информационного противоборства[3].

Третья причина заключается в том, что информационные войны менее ресурсозатратны. При относительно малых вложениях в информационную кампанию агрессор может получить достаточно высокий результат. Для сравнения, военные расходы РФ в 2016 г. составили 63,7 млрд долл.[4]. Зарплаты так называемых «ботов», работающих в составе около шестидесяти человек и осуществляющих пропагандистскую пророссийскую деятельность в Интернете, по некоторым данным, не превышают 44 тыс. руб.[5]. Таким образом, сумма, необходимая для содержания команды «ботов», составляет примерно 32 млн руб., что несопоставимо с вышеуказанной суммой военных расходов.

Эти три аспекта являются стимулами для широкого распространения и постоянного совершенствования технологий информационной агрессии, в результате чего у государства обостряется потребность в обеспечении своей информационной безопасности. В современных условиях обеспечить эту безопасность способно лишь то государство, которое обладает информационным суверенитетом или, по крайней мере, теми или иными его признаками.

Одним из первых исследователей понятия «информационный суверенитет» стал руководитель управления Федеральной службы по техническому и экспортному контролю М. М. Кучерявый. Он выводит достаточно широкое определение: «…информационный суверенитет – это верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве»[6]. Согласно данному определению, «информационный суверенитет» включает в себя любые компоненты, связанные с информационной сферой государства. На наш

взгляд, такое определение достаточно точно описывает природу этого понятия.

Другой исследователь проблемы «информационного суверенитета», российский предприниматель в сфере информационных технологий И. С. Ашманов, определил «информационный суверенитет» как устойчивость государства к информационной войне в любых её проявлениях. Другими словами, он приводит достаточно узкое определение «информационного суверенитета» и сводит его характеристики лишь к инструментам ведения информационного противоборства. Также, по его мнению, «информационный суверенитет» наравне с «электронным» (техническим) является составляющей «цифрового суверенитета»[7]. Фактически, И. С. Ашманов понимает под «цифровым суверенитетом» то же самое, что мы понимаем под «информационным суверенитетом».

Таким образом, понятие «информационный суверенитет» характеризуется как минимум двумя аспектами: техническим и идеологическим. Технический аспект включает в себя наличие национального программного обеспечения, собственных социальных сетей, поисковиков, национальную электронную платёжную систему и т. д. Идеологический аспект включает в себя такие компоненты, как наличие официальной идеологии или национальной идеи, высокого уровня популярной массовой культуры, развитой системы пропаганды, а также усовершенствованного законодательства в области информации и т. д.

Изучив сущность понятия «информационный суверенитет», перейдём к рассмотрению основных методов его обеспечения. Для этого государство в своей информационной политике должно грамотно сочетать методы «информационного щита» и «информационного меча». Понятия эти на данный момент также плохо изучены и почти не концептуализированы.

И. С. Ашманов понимает под «информационным щитом» совокупность технических, коммуникативных, идейных и культурных средств, используемых для перехвата и нейтрализации невыгодной государству информации, противодействия попыткам хищения стратегически важной информации и личной информации каждого гражданина, охраны национальных платёжных систем и т. д. Соответственно, под «информационным мечом» – совокупность методов и конкретных действий, направленных на подрыв информационного суверенитета противника[8]. Таким образом, под «информационным щитом» понимаются пассивные элементы системы и реактивные защитные меры, а под «информационным мечом» – атакующие, активные, превентивные или трансформационные инструменты.

Можно сказать, что фундаментом государственного информационного суверенитета является крепкий «информационный щит» государства. Также без него затруднительна или даже невозможна реализация политики «информационного меча». Как мы уже выяснили, к основным инструментам реализации политики «информационного щита» относятся пассивные элементы системы, либо реактивные меры. Рассмотрим основные из них.

Первый элемент – это высокий уровень компьютеризации государства и его обеспеченности коммуникационными системами. В случае если государство обладает низким уровнем информационной обеспеченности и информационно-коммуникационного оборота, то информация обладает в нём далеко не первой значимостью, а информационному суверенитету не на чем основываться.

Второй элемент – собственные программное обеспечение, национальные антивирусы и системы защиты данных. Так, информационный суверенитет крайне слаб, если государство не в состоянии защитить свои данные и данные своих граждан от киберпреступников. Если же оно зависит в техническом плане от внешних игроков, то и его информационный суверенитет находится в зависимости от внешнего производителя, что ставит его под угрозу.

Третий элемент – сильный положительный внутренний и внешний имидж государства[9]. Это один из важнейших компонентов информационного суверенитета государства: от него зависит как уважение к государству со стороны иностранных акторов, так и собственных граждан. Имиджевый ресурс легко конвертируется в материальные виды ресурсов, положительный имидж способен приносить государству экономические, политические и прочие преимущества[10]. Так, государство с сильным положительным имиджем привлекательно для квалифицированных мигрантов, внутренних и внешних инвесторов, туристов и т. д.

Четвёртым элементом выступает чёткая национальная идея или идеология. Так, существование группы людей невозможно без объединяющий их идеи. Причем чем больше группа, тем идея становится абстрактнее, но тем она необходимее. Особенно когда речь идёт о такой большой группе, как нация. Для её существования необходима сильная национальная идеология по нескольким причинам. Так, по мнению, В. Н. Шилова, идеология или национальная идея выполняет важнейшие функции постановки целей существования государства (целеполагания), интеграции общества и мобилизации населения[11]. Более того, в случае её отсутствия идейное поле заполнят иностранные, иногда разрушительные для нации идеи: информационный суверенитет пошатывается и разрушается.

Пятый элемент – наличие собственной интернет-инфраструктуры: поисковиков, социальных сетей. Наличие развитой интернет-инфраструктуры даёт возможность государству в той или иной степени контролировать сетевое пространство, национальные интернет-компании получают возможность конкурировать с иностранными ком-

паниями. Также интернет-инфраструктура может стать частью положительного имиджа государства, как внутреннего, так и внешнего.

Шестая составляющая «информационного щита» – это совершенная правовая база в информационном поле, являющаяся основой для обеспечения информационного суверенитета[12]. В информационном поле, недостаточно регулируемом законодательством, велика возможность зарождения информационной энтропии, информационных преступлений как против государства, так и против личности (кража данных, выкладывание в Сеть компрометирующей и провокационной информации, сетевой сталкинг и т. д.). При этом у государства будет отсутствовать возможность пресекать такие преступления и наказывать информационных преступников.

Последней, седьмой составляющей «информационного щита» является такой технический фактор, как наличие собственной платёжной системы, существование которой гарантирует независимость государства, делает нечувствительным к политическому давлению извне. Так, прекращение работы платёжных систем Visa Mastercard в Крыму после его присоединения к России привело к образованию множества финансовых трудностей на полуострове[13]. В случае наличия у России собственной платёжной системы, работающей по всему миру, их количество можно было сократить или даже вообще избежать.

Подробно изучив структуру «информационного щита» как комплекса мер по обеспечению информационного суверенитета, перейдём к исследованию феномена политики «информационного меча». Так, государственная политика «информационного меча» может осуществляться в тех же информационных сферах, что и политика «информационного щита», но при помощи атакующих, активных, превентивных или трансформационных мер. Рассмотрим наиболее важные из них.

Первый момент – это развитая система пропаганды, в том числе и развитая система СМИ, которая должна включать в себя каналы внешней коммуникации – государственные каналы, осуществляющие вещание за рубежом (CNN, Russia Today). Их цель состоит в донесении необходимой государству информации до внутренней и иностранной аудитории: ознакомление с официальной позицией страны по тому или иному вопросу, собственной интерпретации событий и т. д. Необходимо отметить, что именно СМИ задают повестку дня как в традиционных моделях коммуникации, так и в новых интернет-коммуникациях. СМИ сообщают о событиях, происходящих в мире, частично дают им оценку, в то время как другая часть событий замалчивается. Так, например, официальные новостные ресурсы отказались от трансляции новостей об антикоррупционных митингах в Москве, проведённых 26 марта 2017 г. Информация о них также не попала в топ «Яндекса», в то время как новостные ленты социальных сетей были переполнены информацией об этом[14]. Таким образом, можно утверждать, что всё наше представление о мире политического построено СМИ. Именно поэтому без собственной вещательной интерпретационной машины невозможно проводить внутреннюю и внешнюю пропагандистскую политику. Более того, именно СМИ своим быстрым прогрессом в последние два столетия вывели информационную составляющую политического и правового суверенитета на первый план, в то время как информационные технологии технически обеспечили ее сегодняшнее устойчивое состояние[15].

Вторым атакующим методом являются производство и популяризация национальных культурных продуктов. Речь идет о фильмах, музыке, национальных брендах, при помощи которых возможно проведение сразу нескольких государственных информационных политик: по формированию общего положительного впечатления о стране в сознании иностранцев; по популяризации национальных ценностей и идей среди внутренней и иностранной аудиторий и даже по подрыву легитимности государственной власти в тех или иных странах, например, при помощи распространения роликов, документальных и псевдодокументальных фильмов о высших должностных лицах государства.

Третье – это распространение необходимых государству идей в интернет-пространстве (социальных сетях, видеохостингах, «Википедии»). Например, выкладывание видеороликов, содержащих просветительскую или пропагандистскую информацию, выгодную государству, нейтрализация ангажированной негативной информации в «Википедии», перевод статей о национальных ценностях на иностранные языки. «Википедия» обладает мощнейшим потенциалом для воздействия на массовое сознание[16], поэтому с её помощью возможны трансляция национальных ценностей и идей, интерпретации событий, элементы имиджа государства в массовое сознание.

Четвертый метод – продвижение сильного положительного имиджа государства, в том числе через интернет-пространство и массовую культуру. Занимаясь продвижением имиджа своей страны, возможно сконструировать общее положительное впечатление о ней на мировой арене, привлечь экономических партнёров и геополитических союзников, квалифицированные кадры, инвестиции. Одновременно в рамках проведения политики «информационного меча» возможно негативизировать имиджи государств-противников, подрывать их международный авторитет и привлекательность в глазах тех же инвесторов и торговых партнёров.

Пятый – институционализация информационной сферы, т. е. создание в государстве соответствующих институтов с чётко обозначенными иерархией обязанностями: министерств, ведомств, кибервойск и т. д. Они являются своеобразными рычагами проведения государственной информационной политики, устраняют институциональ-

ный хаос, неясности в разграничении полномочий в информационной сфере и т. д. Опять-таки отсутствие в государстве «информационных» министерств, ведомств и служб характеризует низкую информационную культуру государства. В таких условиях само существование информационного суверенитета находится под сомнением.

Шестой компонент: совершенная правовая база в информационном поле, которая может выполнять не только защитные функции, как было указано выше, но и быть ресурсом активных действий государства, позволяет своевременно и адекватно реагировать на внутренние попытки нарушения информационного суверенитета. Речь идет о применении правовых санкций против хакеров, зачинщиков «цветных» революций, сетевых сталкеров, ограничении распространения невыгодного государству контента и т. д.

В качестве седьмого метода «информационного меча» можно назвать осуществление прямого давления на зависимых от информационных продуктов игроков. Например, при помощи отключения государства или региона от электронной платёжной системы, ограничения работы той или иной социальной сети на его территории, прекращения поставок информационной техники и т. д. Необходимо отметить, что этот инструмент можно лишь косвенно отнести к политике «информационного меча».

Итак, в современных условиях у государства возникла острая потребность в формировании и обеспечении собственного информационного суверенитета, под которым понимается полная самостоятельность государства при проведении внутренней или внешней государственной информационной политики. Информационный суверенитет основывается как на технических моментах (программное обеспечение, интернет-инфраструктура), так и на идеологических (система пропаганды, национальная идея, массовое искусство). Для его обеспечения государству необходимо грамотно сочетать в своей информационной политике инструменты «информационного щита» и «информационного меча».

## Примечания

1 См.: *Крынина О. Ю.* Дефиниции понятия «информационная война» : анализ российского и зарубежного опыта // Новые технологии. 2009. № 3. С. 68–70.

2 См.: *Остроухов В. В.* Информационная безопасность. URL: https://uchebnikionline.coam/politologia/informatsiyna_bezpeka_-_ostrouhov_vv/istoriya_informatsiyno-psihologichnogo_protiborstva.htm (дата обращения: 16.04.2017).

3 См.: *Зорина Е. Г.* Концептуализация понятия «постинформационного общества» и влияние его характеристик на политическую сферу // Информационные войны. 2017. № 2 (39). С. 34–37.

4 См.: Рейтинг стран по военным расходам за 2016 год. Инфографика // Аргументы и факты. URL: http://www.aif.ru/dontknows/infographics/reyting_stran_po_voennym_rashodam_za_2016_god_infografika (дата обращения: 16.06.2017).

5 См.: Из жизни кремлеботов. Разоблачения и списки // Grimnir74. Lifejournal. URL: http://grimnir74.livejournal.com/4462399.html (дата обращения: 16.04.2017).

6 *Кучерявый М. М.* Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. Вып. 9 (69). С. 12.

7 См.: *Ашманов И. С.* Информационный суверенитет. URL: http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf (дата обращения: 16.04.2017).

8 Там же.

9 См.: *Пупкова А.* Международный имидж страны : теоретические аспекты. URL: http://lawinrussia.ru/content/mezhdunarodnyy-imidzh-strany-teoreticheskie-aspekty (дата обращения: 22.04.2017).

10 См.: *Гаврa Д. П., Савицкая А. С., Шишкин Д. П.* Внешний имидж государства в медиапространстве // Вестн. СПбГУ. 2011. Вып. 3. С. 187.

11 См.: *Шилов В. Н.* Идеология для современной России : необходимость и предпосылки // Научные ведомости. 2015. Вып. 34. С. 183–189.

12 См.: *Слесарчук О. М.* Современное состояние информационной сферы России // Изв. РГПУ им. А. И. Герцена. 2009. Вып. 93. С. 145.

13 См.: Игра в карты. Как Крым живет без международных платежных систем // Аргументы и факты. URL: http://www.krym.aif.ru/money/details/1431249 (дата обращения: 16.04.2017).

14 См.: Кремль ответил на вопрос об отказе телеканалов освещать акции протеста // РБК. URL: http://www.rbc.ru/rbcfreenews/58d8ef529a7947cb693fed03 (дата обращения: 16.04.2017).

15 См.: *Россошанский А. В.* Информационная составляющая политического суверенитета // Изв. Сарат. ун-та. Нов. сер. Сер. Социология. Политология. 2011. Т. 11, вып. 4. С. 91.

16 См.: *Зорина Е. Г.* Искажение значений и смыслов политико-исторических событий в разноязычных версиях статей «Википедии» // Власть. 2017. Т. 25, № 3. С. 211–214.

**Образец для цитирования:**

*Зорина Е. Г.* Информационный суверенитет современного государства и основные инструменты его обеспечения // Изв. Сарат. ун-та. Нов. сер. Сер. Социология. Политология. 2017. Т. 17, вып. 3. С. 345–348. DOI: 10.18500/1818-9601-2017-17-3-345-348.

**Cite this article as:**

Zorina E. G. Informational Sovereignty of Contemporary State and the Main Instruments of its Ensuring. *Izv. Saratov Univ. (N. S.), Ser. Sociology. Politology,* 2017, vol. 17, iss. 3, pp. 345–348 (in Russian). DOI: 10.18500/1818-9601-2017-17-3-345-348.