НЕЖЕЛЬСКИЙ Александр Александрович – аспирант Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН (117997, Россия, г. Москва, Профсоюзная ул., 23; nejel@mail.ru)

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННЫХ ВОЙН И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Аннотация. *Статья посвящена вопросам международной информационной безопасности в контексте информационных конфронтаций между государствами. Автор пытается оценить место информационной безопасности государства в информационно-коммуникационных технологиях (ИКТ) и в современном мире. Рассматриваются такие явления, как информационный разрыв и цифровой парадокс мощи. Особое внимание уделено вопросам критической информационной инфраструктуры (КИИ): различным подходам к формулировке термина и существующим дискуссиям по этому вопросу.*
Ключевые слова: *информация, безопасность, государство, инфраструктура, кибербезопасность, информационное общество, инфраструктура, власть, сеть*

Сегодня все чаще актуализируются проблемы государственной и международной информационной безопасности. В силу транснациональной природы сферы информационно-коммуникационных технологий (ИКТ) зачастую проблемы такого характера не могут быть разрешены на уровне отдельных государств и требуют международных ответов.

Сфера ИКТ характеризуется анонимностью множества рядовых участников и отсутствием монополии государства на применение «силы» в информационном оружии. Также стоит отметить высокую потенциальную угрозу применения информационного оружия. Несмотря на то что во многих передовых странах военные бюджеты после завершения «холодной войны» сократились, затраты правительств на информационную безопасность активно растут. Это свидетельствует о высокой значимости данной темы для государств разных уровней.

Информатизация в целом представляется одной из ключевых характеристик современности. За счет развития информационного сектора множество сфер уже стали значительно более масштабными и конкурентными. В то же время политическое лидерство конкретных государств предполагает и информационное лидерство: если в 1990-х и начале нулевых годов информатизация сама по себе виделась исследователям источником глубинных трансформаций в экономике государства, то сегодня она выступает в качестве базовой инфраструктуры, необходимой для развития различных отраслей бизнеса, общества и самого государства. На первое место по степени влияния выходит производная высокого развития ИКТ – пользовательские данные, персональные данные и так называемые большие данные (*big data*). Значимость данных сегодня намного превышает значимость программного обеспечения и технической инфраструктуры [Зиновьева 2016: 237].

Уровень развития государства и его положение на международной арене сегодня в значительной степени обусловлены уровнем его информатизации. Развитые и развивающиеся страны существенно отличаются по степени внедрения и эффективности эксплуатации ИКТ. Это явление получило название «цифровой разрыв». Проблема цифрового разрыва сегодня препятствует реализации экономического потенциала ИКТ на межстрановом и глобальном уров-

нях. Цифровой разрыв часто усугубляет иные виды неравенства между государствами – экономическое, социальное.

В последние годы в исследовательской литературе все чаще появляется понятие «балканизация Интернета» – регионализация режимов управления Интернетом. В свою очередь, это ведет к выделению суверенных сегментов глобальной сети. Границы этих сегментов могут как повторять государственные границы, так и противоречить им. Как правило, в основе логики разделения и сегментации Интернета лежат соображения по обеспечению государственной информационной безопасности. Государства все чаще приходят в Интернет и пытаются установить правила игры на «участке ответственности», который они считают своим.

Все это приводит к появлению новых подходов и определений. К примеру, появляется такое понятие, как информационный суверенитет. М.М. Кучерявый определяет информационный суверенитет как «верховенство и независимость государственной власти при формировании и реализации информационной политики» [Кучерявый 2013].

Значительную роль в этом вопросе играет конфликт вокруг самого определения информационной безопасности и его трактовок. Поэтому остановимся на нем подробнее.

Россия, согласно анализу официальных документов и выступлений официальных лиц, придерживается широкого подхода к определению информационной безопасности. Такое определение включает в себя как информационно-технические, так и политико-идеологические аспекты. Россия выступает за использование термина «информационная безопасность» в ходе международных переговоров. Схожего подхода придерживается Китай. Страны Запада, особенно США, в дипломатической риторике используют термин «кибербезопасность», что предполагает учет исключительно информационно-технических проблем, прежде всего обеспечение стабильной работы информационных сетей и систем, а также защиту данных. Россия пытается снизить риски, связанные с развитием информационного пространства. Россия исходит из представления о существовании «национальных сегментов» Интернета, в рамках которых действует юрисдикция конкретного государства. Официальные лица России добиваются введения принципа невмешательства в информационное пространство других стран. По проекту Конвенции об обеспечении международной информационной безопасности, выдвинутому Россией на рассмотрение ООН, «каждое государство вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством». В документе подчеркивается, что государства должны защищать свободу слова в Интернете и «не вправе ограничивать доступ граждан к информационному пространству», однако здесь дается важная оговорка: правительства могут вводить ограничения «в целях защиты национальной и общественной безопасности» [Зиновьева 2016: 237]. Таким образом, в основе позиции России лежит идея о регионализации и выделении «государственных сегментов» в Интернете.

Во многих государствах наблюдается создание специальных ведомственных подразделений, которые официально декларируют не только защиту государственных и коммерческих компьютерных сетей и систем, но и возможность проведения атак на информационные объекты недружественных государств. О намерениях ярче всего говорит тот факт, что чаще всего такие подразделения создаются в рамках военных и гражданских разведок, а также вооруженных сил.

Российская Федерация последовательно выступает за использование терминов «информационное пространство» и «информационная безопасность», отстаивает широкий подход к определению объекта этой безопасности.

Согласно позиции России, объектом безопасности являются не только сетевое оборудование и ПО, но и социально-гуманитарные явления и объекты развития общества. В свою очередь, США продолжают придерживаться использования термина «кибербезопасность», что подразумевает под собой обеспечение безопасности только компьютерных сетей [Зиновьева 2016: 237]. Таким образом, официальные лица США предпочитают частную модель регулирования и стараются избегать вопросов регулирования контента.

Китай также является одним из важных игроков в данной области. В официальных документах Китая не приводятся однозначные определения угроз кибербезопасности. Анализ риторики и политической позиции Китая позволяет сделать вывод, что Китай придает особое значение потенциальной опасности распространения через средства ИКТ нехарактерных или опасных общественных ценностей, выступает за сохранение «цифрового суверенитета».

На сегодняшний день на глобальном уровне все еще не появилось общепризнанное определение информационного оружия и информационной войны. В первую очередь это вызвано терминологическими расхождениями, которые, в свою очередь, вызваны разницей интересов государств и разницей в подходах к информационной безопасности. Термин «информационная война» в большинстве отечественных работ имеет расширенное толкование (информационная война как форма межгосударственного противоборства) и используется в ином смысле, нежели в американских военно-политических и научных кругах. Западные исследователи склонны использовать термин «кибервойна», которая ограничивается воздействием на компьютерные системы.

С целью унификации здесь и далее мы будем использовать термин «информационная конфронтация» как наиболее широкий по смыслу и нейтральный по характеру. Под информационной конфронтацией мы будем понимать любые формы негативного взаимодействия между субъектами в информационном поле – от дипломатических нот и негативно окрашенных новостных сообщений до применения кибероружия и активных систем радиоэлектронной борьбы (РЭБ) в ходе гибридного конфликта.

Все три крупных субъекта информационной безопасности – Китай, Россия и США – рассматривают информационную безопасность как составляющую своей национальной безопасности.

Глобальная сеть становится важным инструментом проекции власти государств на международной арене: «мягкой силы» – при помощи культурного и лингвистического влияния, «жесткой силы» – благодаря кибератакам, кибершпионажу и сбору разведывательных данных. Наиболее влиятельные акторы осуществляют управление через формирование повестки дня, создание «правил» и параметров сети.

Начиная с 2015 г. в России ведется целенаправленная политика по созданию государственного сегмента Интернета в целях обеспечения информационной безопасности. В контексте цифрового парадокса мощь государств и его информационная инфраструктура находятся во все нарастающей опасности применения информационного оружия. Цифровизация ключевых областей жизни привела к тому, что они тоже находятся под угрозой. Опасность удаленного взлома может поставить под угрозу как электропитание отдельного региона (*BlackEnergy:* отключение электроэнергии на Украине в 2015 г.), так и федеральную программу по обогащению урана (*Stuxnet:* ядерная программа Ирана, 2010 г.).

На сегодняшний день критические информационные и традиционные инфраструктуры сосуществуют. При этом в условиях формирования цифровой экономики все более широкое распространение приобретают информационные

инфраструктуры, поскольку они более экономически эффективны, удобны и эргономичны. Таким образом, с каждым днем все больше критических инфраструктур становятся информационными. Попытки выработать общепринятое определение термина «критическая информационная инфраструктура» (КИИ) на глобальном уровне пока что не увенчались успехом.

Исследователи института проблем информационной безопасности МГУ разработали следующий ряд определений:

– инфраструктура – это набор отдельных взаимосвязанных элементов системы, поддерживающих ее функциональность и работу по назначению;

– критическая инфраструктура – это комплекс отдельных взаимосвязанных элементов, поддерживающих функциональность национально значимых для страны сфер жизнедеятельности;

– критически важная информационная инфраструктура – это совокупность программно-аппаратных, сетевых и информационных компонентов, поддерживающих функциональность национально значимых для России сфер жизнедеятельности.

Согласно федеральному закону № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации» от 2017 г. под КИИ понимается совокупность автоматизированных систем управления производственными и технологическими процессами (АСУ ТП) критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка.

Характер международного взаимодействия по обеспечению информационной безопасности отражает более масштабные процессы, присущие всей международной системе, в частности тенденцию к регионализации, растущую роль негосударственных акторов, появление новых форматов международного взаимодействия. На сегодняшний день можно с уверенностью говорить о растущей секьюритизации (в определении Б. Бузана) глобального информационного пространства как в России, так и в других странах, а также о противоречивых тенденциях к регионализации информационного пространства при его глобальной природе [Buzan, Wæver, De Wilde 1998: 36].

Асимметричность потенциальных ответных мер увеличивает энтропию возможной эскалации любого конфликта, даже основанного на слухе, подтасовке фактов или лжи. Растет актуальность изменений в международно-правовой базе, которая регулирует отношения субъектов в информационном пространстве, а также создания специальных правовых институтов, обладающих особыми компетенциями в области ИКТ. В этой связи видится правильным принятие в России отдельного федерального закона, регулирующего вопросы критической информационной инфраструктуры.

Природа государств, в основе которой лежит понятие о суверенитете и границах, в ходе развития и цифровизации вступает в противоречие с трансграничной природой ИКТ. На текущий момент сложно оценить вероятность развития глобального информационного кризиса или информационной войны, но определенно можно сказать, что по мере цифровизации число информационных конфронтаций между всеми субъектами будет увеличиваться.

Список литературы

Зиновьева Е.С. 2016. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. – *Вестник МГИМО Университета*. № 4. С. 235-247.

Кучерявый М.М. 2013. Основные направления государственной политики РФ в области обеспечения международной информационной безопасности. – *Власть*. № 12. С. 54-59.

Buzan B., Wæver O., De Wilde J. 1998. *Security: a New Framework for Analysis*. Lynne Rienner Publishers. 239 p.

NEZHEL'SKY Aleksandr Aleksandrovich, *postgraduate student, Primakov National Research Institute of World Economy and International Relations (23 Profsoyuznaya St, Moscow, Russia, 117997; nejel@mail.ru)*

THEORETICAL BASES OF RESEARCH OF INFORMATION WARS AND INFORMATION SECURITY OF THE STATE

Abstract. *The article is devoted to the issues of international information security in the context of information confrontations between modern states. The author tries to assess the place of information security of the state in information and communication technologies and in the modern world. Such phenomena as information gap and paradox of power in the network age are considered. The author pays particular attention to critical information infrastructure: to different approaches to the formulation of the term and existing discussions on this issue.*

Keywords: *information, security, state, information society, information gap, infrastructure, cybersecurity, power, network*