ПРОБЛЕМЫ БЕЗОПАСНОСТИ

УДК 101.1:316

Д. Г. ЕВСТАФЬЕВ

РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА И ОСОБЕННОСТИ ИНФОРМАЦИОННО-ПОЛИТИЧЕСКОГО ПРОТИВОБОРСТВА НА СОВРЕМЕННОМ ЭТАПЕ*

Аннотация. В статье рассматриваются особенности современного информационного общества, построенного на технологиях цифровизированных интегрированных коммуникаций. Описан ряд процессов, включая повышение интрузивности и деструктивности информационно-политических манипуляций, на фоне повышения агрессивности внешнеполитического поведения стран коллективного Запада, которые создают ситуацию милитаризации информационного общества и информационного пространства. Обращается внимание на возникновение новой системности угроз, связанной со сращиванием информационно-политических манипуляций и киберсиловых средств воздействия на противника. Все это, по мнению автора, создает для России целый ряд новых рисков, которые уже более не могут быть купируемы в рамках традиционного инструментария превентивных мер кибербезопасности. Предложен авторский подход к формированию общегосударственного механизма нейтрализации угроз, исходящих из информационного пространства.

Ключевые слова: информационное общество; информационная безопасность; Россия; США; информационные войны, кибер-ударные методы; информационные манипуляции.

Современный этап развития системы международных отношений характеризуется резким повышением уровня военно-политической напряженности, вплоть до возникновения предпосылок к военной конфронтации на региональном уровне. Главным элементом складывающейся системы военно-политической конфронтации является усиление информационного противоборства на различных уровнях, инициированное Соединенными Штатами Америки при активном участии их сателлитов с целью сохранить военно-политическую гегемонию, о чем прямо указывал Министр обороны России С. К. Шойгу, подчеркивая, что «основная и главная цель этой войны – стремление управлять Россией и, в конечном итоге, миром» (цит. по: [8]). Гегемония (а по ряду сегментов – усиленная административными рычагами монополия) в глобальном информационном пространстве и информационном обществе как интерфейсе между человеком и информационном пространством мыслится военно-политическим руководством США и значительной частью американской элиты, причем вне зависимости от конкретной политической ориентации, в качестве критического условия сохранения американоцентричности в мировых экономических и политических отношениях.

Отметим две фундаментальные тенденции в развитии системы информационной конкуренции и противоборства в современном мире:

*Статья подготовлена на основе тезисов, представленных автором в ходе «круглого стола» «Психологическая оборона. Борьба за историю – борьба за будущее» на форуме «Армия 2020».

ЕВСТАФЬЕВ Дмитрий Геннадиевич – кандидат политических наук.
НИУ «Высшая школа экономики» (Москва). E-mail: devstafiev@hse.ru

© Евстафьев Д.Г., 2020

С одной стороны, отмечается резкий рост востребованности информационно-политических манипуляций в качестве условно «нормального», политически легализованного элемента внешней политики, вполне допустимого в отношении геополитического конкурента и, тем более, страны, объявленной потенциальным противником; с другой – за последние полтора года отмечается резкий рост агрессивности и деструктивности информационно-манипулятивных действий во всех сферах, не только в политической, сращивание информационно-политических манипуляций, экономических и социально-экономических и кибер-ударных средств воздействия на конкурентов и противников, а также, что является совершенно новым явлением, задействование в этих манипуляциях высшего руководства соответствующих стран. Что, например, происходило в ходе попыток давления на Россию в контексте «казуса Навального».

Краткосрочные информационно-политические манипуляции постепенно вытесняют из политической практики ряда государств Запада классические виды политических и даже дипломатических коммуникаций. *Информационные манипуляции различного типа начинают подменять собой принятие стратегических политических решений*, возникает быстрая и не всегда контролируемая «пиаризация внешней политики», как это происходит в отношениях России и стран Европейского Союза последние полтора года. При этом затрагиваются и гораздо более важные для глобальной безопасности сферы, например, стратегическая ядерная стабильность.

Складывающаяся ситуация отражает сочетание трех взаимосвязанных процессов:

1. Повышение остроты глобального экономического и политического противоборства на фоне торможения американоцентричной глобализации и кризиса ее основных институтов. Складывающаяся в мире ситуация «предхаоса», определяется нами как ожидание крупного системного кризиса мировой экономики и крушения политических институтов, ограничивающее политическую готовность крупнейших государств мира к разрушению системы глобальной экономической взаимозависимости и объективно концентрирующее их конкуренцию в сфере непрямого противоборства.

Ситуация предхаоса объективно повышает значимость информационного противоборства и информационно-политических манипуляций в политике наиболее влиятельных государств мира.

2. Рост агрессивности поведения США и их ближайших сателлитов, стремящихся сохранить свое доминирование в геоэкономических и геополитических процессах, выход в ряде случаев США на уровень балансирования на грани войны в военно-силовых демонстрациях, снятие существовавших ранее ограничений в военно-политической деятельности, в том числе, в сфере политического давления, санкционной политики и информационно-политических манипуляций.

3. Ускоряющаяся трансформация структуры современного информационного общества, дальнейшее развитие социальной атомизации и социо-информационной анклавизации, появление новых максимально «адресных» информационных технологий, делающих информационные манипуляции существенно более социально-эффективными.

Мы столкнулись с комплексным процессом, имеющим геополитическую природу, связанным с характером трансформаций постглобального мира, но отражающим также и новые тенденции в глобальном мире и регионализированных социально-экономических пространствах, становящиеся приоритетными с точки зрения организации постглобального мира. Это определяет, с одной стороны, как минимум, среднесрочный характер процессов, а с другой – невозможность нейтрализации возникающих рисков на условно «ведомственной» основе.

Интересы США и изменение подходов к информационному противоборству

С военно-политической точки зрения предхаос как состояние современной экономики и политики значительно расширяет зону так называемых субконвенциональных силовых инструментов, существенно расширяя границы условно «допустимого». Для США сращивание силовых и информационно-манипулятивных средств и использования средств воздействия на потенциального противника является привычным и нереволюционным. Методы противоборства с противником, не доходящие

до уровня прямого военного столкновения, находились в центре внимания Пентагона еще с середины 80-х гг. XX в., когда «конфликты низкой интенсивности» были официально включены в «спектр конфликтов» Пентагона и получили доктринальное оформление в виде полевого устава FM 100-20. Сейчас происходит адаптация, безусловно, глубокая, классических американских подходов к новым технологическим и социальным условиям, связанным с высоким потенциалом социальной интрузивности современных цифровизированных интегрированных коммуникаций.

Пандемия коронавируса и связанные с этим политические и экономические процессы, до известной степени замедлившие реализацию геоэкономической и геополитической регионализации, дали США дополнительное время для консолидации своих ресурсов, главным из которых становится доминирование в технологической и контентной составляющей современного информационного общества.

Сфера цифровых коммуникационных платформ стала не просто ареной жесткой конкуренции, но и сегментом технологий, где США претендуют на полную гегемонию. Как часть этой политики мы наблюдаем политику США по усилению централизации системы управления военно-прикладными инструментами воздействия на информационное пространство [13]. Соединенные Штаты стремятся не просто сохранить доминирование в управлении информационным обществом, но и максимально активно используют возникающую «свободу рук» в применении информационно-манипулятивных средств. Такая политика может быть однозначно интерпретирована как стремление включить информационные манипуляции в число инструментов военно-силового, а не только политического воздействия на противника.

Нынешняя политика США в сфере информационного противоборства отражает стремление глобалистски ориентированного сегмента американской элиты, к окончательному отрыву операционной реальности от информационной и к переходу к информационно-политическим манипуляциям в пространстве «вирутализированной реальности», причем не только в настоящем, но и «продолженной в прошлое», что расширяет манипулятивные возможности, о чем говорил в ходе «круглого стола» «Психологическая оборона. Борьба за историю – борьба за будущее» на форуме «Армия-2020» первый заместитель министра обороны России Р. Х. Цаликов [9].

Способность к неограниченному, в содержательном плане в особенности, социальному конструированию является составной частью американской политики по достижению гегемонии в современном мире, но это достижимо только при условии абсолютного доминирования США как в информационных технологиях, так и в контенте, содержательной стороне коммуникаций. США и их сателлиты не имеют реальных шансов на политическую победу в пространстве социальной деятельности и реальной действительности. Поэтому им нужна неограниченная виртуализация и создание фейковых информационных фокусов. На это направлена политика по усилению американского доминирования в информационном пространстве, отражающего доминирования американских технологических платформ в дистанционных системах обучения, управления, торговли и проч.

Ситуацию обостряет процесс легализации, формального закрепления в военно-доктринальных документах различного уровня информационно-политических и кибер-ударных средств ведения субконвенциональных боевых действий, что отражает окончательное сращивание этих двух групп инструментов. Рубежным стал доклад «RAND Corporation Operationalizing Cyberspace as a Domain: Lessons for NATO» [14], фиксировавший интеграцию кибербоевых инструментов и информационно-политических манипуляций в гибридных пространствах и во многом определивший профессиональный дискурс по теме. Появление этого доклада, относительно низкого статуса, можно рассматривать как инструмент первичной легализации новых тенденций. Учитывая, что несколько раньше уже формулировались подходы о возможности воспроизводства механизма «сдерживания» в отношении возможных кибератак [10], это может говорить о наличии планов политической легализации таких методов, естественно, «в ответ» на действия противостоящей стороны в киберпространстве.

Возникает опасная для глобального информационного пространства ситуация, с

одной стороны, максимально широкого использования коммуникационных платформ для он-лайн сервисов, которые контролируют США (от социальных сетей до платформ он-лайн обучения), с другой – подготовка к ведению информационно-политических и кибер-ударных боевых действий. В таких условиях подобные платформы будут выполнять функцию «поля боя».

Вероятно, мы можем говорить о переходе США к разработке механизмов комплексного использования информационно-политических манипуляций и кибердарных средств воздействия на противника, рассмотрению этих двух элементов информационной войны, ранее лежавших в разных плоскостях в единой системе инструментов. Это требует нового уровня осознания угроз, связанных с использованием информационных инструментов и выработки комплексной стратегии противодействия им.

Показательно, что США уже ставят вопрос о необходимости выработки активных и даже превентивных мер по нейтрализации угрозы хакерских атак со стороны России на социально-значимые системы в США, например, на энергосети [11], но в то же время за последние годы было несколько случаев, когда аварии на энергосетях в ряде стран (Иран, Венесуэла) связывались с нанесением кибердаров со стороны США и их сателлитов с использованием уязвимости произведенного американскими компаниями программного обеспечения и недостаточной защищенностью цифрового пространства.

Информационное общество как пространство конкуренции и противоборства

За последние полтора года в глобальном информационном пространстве наметились новые тенденции развития, напрямую затрагивающие сферу политико-информационных манипуляций и кибер-силового воздействия на потенциального противника:

а). Резкое ускорение процессов цифровизации экономики и социальной сферы. Этот процесс начался до пандемии коронавируса, но был ею в значительной мере ускорен, создав вполне осмысленный и освоенный на политическом уровне запрос на определенные технологии. Проблема в том, что цифровизация, в особенности социальных систем, ведется без полного учета возникающих рисков технологического и социального характера. Это, в частности, касается рисков, связанных с уязвимостью систем хранения персональных данных. Опережающее развитие виртуализации процессов управления обществом в отрыве от создания новых социальных институтов только усиливает риски социальной атомизации, что облегчает осуществление информационных манипуляций, делает систему государственного управления более уязвимой в отношении внешних манипуляций [6], а главное, создающей эффект неравномерности развития различных сегментов социально-значимых субсистем национального информационного пространства, что может выражаться и в различном уровне систем безопасности.

б). Расширение числа игроков в сфере информационно-политических манипуляций. В число стран, активно использующих информационно-манипулятивные технологии вошли не только крупнейшие игроки мировой политики, например, Индия, но и отмечены попытки обозначить свои возможности в сфере информационных манипуляций со стороны Германии (частично удачная попытка формирования среднесрочной системы информационной псевдо-реальности в «казусе Навального») и Турции (агрессивное и технологически фундированное участие в информационном противоборстве в ходе обострения армяно-азербайджанского конфликта в сентябре 2020 г.), а также попытки таких сателлитов США, как Польша и Литва продвигать собственную, частично независимую от Вашингтона повестку дня в ходе попыток дестабилизации политической ситуации в Белоруссии. Развитие этого процесса неизбежно приведет к усилению неконтролируемости и хаоса процессов информационного противоборства, обостренных растущей доступностью кибердарных технологий.

в). Обострение информационного противоборства не только в сегменте пропаганды или в реализации потенциала «мягкой силы», (а ее эффективность в классической форме падает), но и с точки зрения конкуренции платформ цифровизации. В особенности это характерно и для глобальной конкуренции США и КНР, сконцентрировав-

шейся в последние полтора года в сфере высоких коммуникационных технологий [15]. Факторы технологической конкуренции становятся одними из наиболее значимых и с точки зрения развития информационного общества, и в плане потенциала информационного противоборства, в том числе, с точки зрения обеспечения устойчивости важнейших общественных систем.

г). Значительное усиление прямого администрирования информационного пространства, причем не только со стороны США и их сателлитов, но и со стороны корпоративных структур (что показали выборы в США в ноябре 2020 г.) на фоне резкого усиления политизированности информационного пространства. Отмечено введение ограничений на доступ к каналам коммуникаций различных их пользователей, связанных, прежде всего, с государствами-конкурентами США, но не только. Такая политика активно использовалась для ограничения влияния российских каналов цифровизированных коммуникаций и реализовалось внесудебное ограничение их деятельности, осуществляемое в интересах государств-конкурентов России, но на основе корпоративных, а не государственных решений. Принятие Государственной Думой соответствующих решений по санкциям против цифровых платформ, осуществляющих дискриминационную деятельность в отношении Российских пользователей, может рассматриваться только как часть более широкого плана.

д). Апробация на коммерческой (в частности, на вопросах, связанных с отраслью углеводородов) и политической тематике («казус Навального») существенно более комплексных и эффективных механизмов фейковизации информационного пространства [4], позволяющее перейти от точечной реализации отдельного фейка к формированию на его основе как минимум среднесрочно актуальных информационных волн, на основе которых возможно формирование более социально-политически значимой системы коммуникационных нарративов. Обратим внимание на многовекторную информационно-манипулятивную игру на рынке углеводородов в феврале-мае 2020 г., в том числе, связанную с ситуацией резкого падения цен на нефть и последующей борьбы за перспективные рынки.

е). Первичная апробация методики управления политической активностью с использованием реальности, близкой к виртуализированной, а также полностью дистанционных методов управления политическими социальными процессами, в том числе, публичной активностью. Первоначально – точечная апробация в ходе ограниченных ударов по Сирии с формированием политического эффекта за счет «картинки», на нынешнем этапе – переход к более масштабным и долгосрочным системам, как, например, это было продемонстрировано в ходе нынешнего поствыборного кризиса в Белоруссии.

ж). Сохранение в повестке дня вопросов «нейрофикации человека» [7], но при выводе их во второй ряд приоритетов в связи с относительно высокой общественной чувствительностью. Усилия на технологическом уровне по созданию гибридных биоинформационных систем продолжаются, в частности, на технологической платформе, формально связанной с деятельностью И. Маска [5]. Важно, что разработка подобных бионейрофицированных гибридных систем ведет практически полностью вне системы международного регулирования и является скрытой, что может свидетельствовать о военно-прикладном характере подобных программ, что частично признается как минимум в аспекте разработок, связанных с искусственным интеллектом в системах управления [12]. Милитаризацию практики реализации концепции «нейрофикации человека», вероятно, следует считать одним из наиболее важных и потенциально опасных процессов в развитии современного информационного общества, как интерфейса между человеком и информационным пространством. Значение процесса сращивания автоматизированных систем управления в гражданском и военном (военизированном) секторах еще далеко не осознано ни политическими элитами, ни экспертным сообществом.

з). Превращение пространств социокоммуникационной гибридности и связанные с ними сообщества (в информационном пространстве и пространстве реальной жизни) в опорные для формирования деструктивных систем, нацеленных на общественно-политическую дестабилизацию. Эта тенденция выводит модель «гибридной войны» за классические рамки, характерные для 2010-

х гг. и характеризовавшиеся чрезмерным акцентированием тематики специальных операций, что отмечали отечественные исследователи [3, с. 97–108]. Главная особенность сегодняшнего этапа в развитии методов информационных манипуляций в гибридных пространствах – существенное повышение адресности коммуникаций, ориентация на определенные социальные среды. Одновременно на Западе осознана недостаточность только информационных манипуляций и необходимость эффективной трансформации информационной протестности в социальную. В рамках такого подхода в последний год происходит интенсивная регионализация протестной «повестки дня» в России.

В совокупности развитие современного глобального информационного общества и политика стран коллективного Запада во главе с США существенно повышают риск возникновения и последующей эскалации вооруженных конфликтов, возможно, даже без четко понимаемой политической и геополитической цели. Заметим, что у современных военно-политических элит крупнейших стран Запада нет опыта управления эскалацией в условиях гибридных социо-информационных пространств. В существующих условиях несиловой переход к глобальной геополитического многополярности выглядит более, чем маловероятным. Главный вопрос состоит в том, насколько удастся удержать военно-силовые действия ниже уровня конвенциональной войны, пусть даже необъявленной, в границах информационно-политических манипуляций, дополненных ограниченными по масштабу специальными операциями и использованием кибер-ударных инструментов. Подобная ситуация создает для России очевидные вызовы не только политического, но уже и военно-политического характера.

Какие же выводы может сделать для себя Россия? Повышение значимости информационно-манипулятивных и кибербоевых средств воздействия на потенциального противника является устойчивой среднесрочной тенденцией. Это касается и организационной структуры внешней политики, и системообразующих аспектов международного права, и многих неформализованных «правил игры», соблюдавшихся глобальными и региональными игроками даже в период холодной войны.

Одновременное осуществление кибер-силовых операций по подрыву дееспособности социально и экономически значимых опорных систем и проведение информационно-манипулятивных мероприятий в отношении значительных общественных групп может создать колоссальный синергичный эффект. Основополагающим вопросом национальной безопасности в современном мире с учетом, как тенденций развития информационного общества, так и особенностей геополитического и геоэкономического противоборства, является сохранение геоэкономической и социальной связности государства, что вполне осознано на официальном уровне в России [2]. Но понятие «связность», безусловно, включает и высокий уровень защищенности от угрозы информационно-политических манипуляций и использования против России кибердарных средств. Это предполагает комплексность подхода и интеграцию различных мер противодействия – от повышения уровня технологической защищенности соответствующих систем до новых методов социального конструирования в проблемных регионах страны – на общей ценностной основе.

Опасность современного состояния информационно-манипулятивной сферы в том, что в настоящее время и в обозримой перспективе она будет находиться вне пространства какого-либо правового или политического регулирования. Это будет серой зоной военно-силового противостояния, куда неизбежно встраивание «третьих сил» (или закамуфлированных под «третьи силы»), а также игроков, прямо не связанных с государственными структурами и действующих вне поставленных политическим руководством той или иной страны задач (такая ситуация уже сейчас сложилась в США, что и доказала ситуация на Ближнем Востоке, начинают возникать схожие признаки и в Германии). Стратегическая опасность состоит в том, что информационное общество в таком случае станет центральной площадкой для борьбы между иерархическими структурами (государствами) и сетевыми структурами, зачастую деструктивного свойства. С учетом процессов регионализации мировой экономики это может иметь очень тяжелые последствия, и они не могут быть купированы только за счет пассивных мер обеспечения информационной безопасности.

Россия, вероятно, должна исходить из необратимости процессов милитаризации информационного пространства и фактической политической легализации кибер-силовых методов воздействия на конкурентов и противников в глобальных экономических процессах и политической игре. В частности, отмечено активное использование кибер-силовых средств в сочетании с методами гибридной войны в ходе попыток смещения президента Н. Мадуро Венесуэле. Главные усилия России должны быть направлены не на то, чтобы предотвратить уже сложившуюся ситуацию или реверсировать ее, а на то, чтобы в сжатые сроки формировать адекватную систему мер противодействия возникающим рискам, попытавшись одновременно перевести процессы развития технологий информационного противоборства в управляемый формат за счет приглашения ключевых стран Запада к международному диалогу, хотя бы и первоначально на высоком экспертном уровне.

Россия не должна быть инициатором распада глобального «свободного», хотя по факту оно таковым не является, «информационного общества», несмотря на очевидно антироссийский характер действий, предпринимаемых США и их сателлитами по укреплению своего контроля над глобальным информационным пространством и ограничению информационных возможностей России. Усилия России должны быть сконцентрированы в сфере формирования потенциала сдерживания киберугроз. Он создается и апробируется через допущение не только превентивных, но и приэмптивных, существенно опережающих действий, направленных не на ликвидацию угрозы, а на снятие возможности ее формирования в отношении стран и иных структур (в том числе, транснациональных компаний, а также сетевизированных социальных сообществ), задействованных в информационно-дестабилизирующих действиях против России.

Россия рассматривается в качестве главной угрозы безопасности «коллективного Запада», о чем прямо говорил С. К. Шойгу, характеризуя эволюцию военной политики блока НАТО [1], а истерия, инициированная еще в 2016 г., с обвинениями в якобы начатой Россией против стран Запада гибридной информационной войны сочетает пропаганду и действия связанных с государством хакеров [16], приобретает новые формы. Это касается вопроса о допустимости превентивных действий в отношении нашей страны в ответ на подозрения во враждебных действиях в киберпространстве. Нагнетание военно-политической напряженности в отношении России, открытая политическая демонизация нашей страны свидетельствуют о готовности, как минимум, части элит Запада снять политические ограничения на применение в отношении России силовых инструментов. Очевидная легализация кибер-ударных средств как военно-силового инструмента мирного времени вполне вписывается в этот сценарий.

Острота проблемы для России определяется тем обстоятельством, что пространство реакции на возникающие в связи с новым потенциалом комплексных информационных средств дестабилизации риски во многом выходит за пределы конституционной сферы ответственности Вооруженных Сил Российской Федерации. Опираясь на организационный и управленческий потенциал Министерства обороны Российской Федерации система противодействия гибридным рискам, включая и риски, связанные с с использованием информационно-манипулятивных средств борьбы с противником, может быть создана в наиболее короткие сроки и с высокой эффективностью. Ключевым вопросом становится переосмысление пространства конкуренции и противоборства в постглобальном мире и особенностей внутриведомственного взаимодействия в условиях доминирования гибридных, то есть, включающих и военно-силовой элемент, механизмов борьбы с конкурентами.

Необходим пересмотр традиционных воззрений на возможный характер ответной реакции, на применение против России методов информационного и кибер-силового воздействия, в особенности, если они нацелены на нанесение значимого урона системам государственного управления, социального обеспечения и взаимодействия с обществом. Например, на подрыв устойчивости функционирования государственных СМИ. Такие действия должны рассматриваться как угроза военно-политического характера, часть гибридной войны против России. Если же кибер-силовое воздействие затрагивает важные инфраструктурные элементы (системы энергоснабжения,

как это произошло в Венесуэле) или нацелено на дестабилизацию важнейших систем государства и общества (пенсионной системы или системы здравоохранения) даже без использования кибер-силовых средств, то такие действия целесообразно рассматривать как военную угрозу низкой интенсивности, имея в качестве ответа на нее не только условно «оборонительный», но и условно «наступательный» инструментарий, хотя эти понятия в информационном и киберпространствах условны. Сам факт принятия Россией решения о формировании комплексной системы противодействия гибридным – политико-манипулятивным и кибер-ударным – угрозам безопасности и интересам России в информационном пространстве может оказать существенное сдерживающее воздействие на партнеров России среди стран Запада.

* * *

1. Западные СМИ развернули масштабную кампанию против России, заявил Шойгу // РИА Новости: сайт. URL: https://ria.ru/20200905/shoygu-1576829830.html (дата обращения: 15.09.2020).

2. *Ильницкий А. М.* Ответить на вызовы времени: необходимо пространственно-территориальное переосваивание страны // Национальная оборона. 2020. № 9 (174). С. 20–28.

3. *Кокошин А. А.* Вопросы прикладной теории войны. 2-е изд. М. : Изд. дом Высшей школы экономики, 2019. 227 с.

4. *Манойло А. В.* Цепные реакции каскадного типа в современных технологиях вирусного распространения «фейковых новостей» // Вестник Московского государственного областного университета: электронный журнал. 2020. № 3. URL: https://evestnik-mgou.ru/ru/Articles/View/1027?fbclid=IwAR2u9XOHLOirF6kmY76c5xvFhR1fHyBxxI7j8mQ7jvKfKdGstyAat-EsUNQ (дата обращения: 10.09.2020).

5. Маск заявил об успешном вживлении чипа для подключения мозга к компьютеру // РБК: сайт. URL: https://www.rbc.ru/technology_and_media/29/08/2020/5f49c0209a79474750ef91d3 (дата обращения: 15.09.2020).

6. *Чернавин Ю. А.* Современная цифровизация: преимущества и риски для российского общества и его безопасности // Военный академический журнал. 2020. № 2(26). С. 76–84.

7. *Шваб К., Дэвис Н.* Технологии четвертой промышленной революции / пер. с англ. М.: Эксмо, 2018. 320 с.

8. Шойгу назвал цель информационной войны Запада против России [26.06.2019] // Информационное агентство ТАСС: сайт. URL: https://tass.ru/armiya-i-opk/6596144 (дата обращения: 20.09.2020 г.).

9. *Щербакова М.* Против России ведётся информационная война, но аргументы наших оппонентов не выдерживают столкновения с реальностью [Электронный ресурс] // Красная звезда. 2020. 2 сент. URL: http://redstar.ru/borba-za-istoriyu-borba-za-budushhee/?fbclid=IwAR33U0_1q9brE6NwnAE0H2CsVhuID6gTIg_LEjO-7labUGCVWFixq05nvD7Q (дата обращения: 21.09.2020 г.).

10. *Hennesey S.* Deterring Cyberattacks. How to Reduce Vulnerability [Электронный ресурс] // Foreign Affairs. 2017. November/December. URL: https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks (дата обращения: 20.09.2020).

11. *Knake R.* The Next Cyber Battleground. Defending the U.S. Power Grid from Russian Hackers [Электронный ресурс] // Foreign Affairs. 2018. July. URL: https://www.foreignaffairs.com/articles/north-america/2018-07-19/next-cyber-battleground (дата обращения: 21.09.2020.).

12. *Muniz C.* DARPA sees 'rich space' for advanced AI in cyber operations [Электронный ресурс] // Jane's Defence Weekly. 2020. August. URL: https://www.janes.com/defence-news/news-detail/darpa-sees-rich-space-for-advanced-ai-in-cyber-operations (дата обращения: 19.09.2020).

13. *Nakasone P., Sulmeyer M.* How to Compete in Cyberspace. Cyber Command's New Approach [Электронный ресурс] // Foreign Affairs. 2020. August. URL: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity (дата обращения: 20.09.2020).

14. Operationalizing Cyberspace as a Domain: Lessons for NATO / L. Ablon, A. Binnendijk, Q. Hodgson, B. Lilly, S. Romanosky, D. Senty, J. Thompson // RAND Corporation: сайт. URL: https://www.rand.org/pubs/perspectives/PE329.html (дата обращения: 20.09.2020).

15. *Segal A.* The Coming Tech Cold War With China. Beijing Is Already Countering Washington's Policy [Электронный ресурс] // Foreign Affairs. 2020. September. URL: https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-hina (дата обращения: 19.09.2020).

16. *Soldatov A.* Cyber Showdown How Russian Hacking Works [Электронный ресурс] // Foreign Affairs. 2016. July. URL: https://www.foreignaffairs.com/articles/russian-federation/2016-07-31/cyber-showdown (дата обращения: 18.09.2020 г.).