

На сайте журнала ["Международная жизнь"](#) опубликован текст выступления Президента НИИГЛОБ, профессора МГИМО (У), МИД России А.И.Смирнова на круглом столе:

["Проблемы современных международных отношений в контексте киберпространства"](#) журнала "Международная жизнь" (в рамках Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Гармиш-Партенкирхен, Германия, 27 апреля 2016 года).

[Подробнее ...](#)

«Industry 4.0» в дискурсе международной информационной безопасности - взгляд из России»

13:45 14.06.2016 Анатолий Иванович Смирнов, Президент АНО «Национальный институт исследований глобальной безопасности», Чрезвычайный и Полномочный Посланник РФ в отставке, д.и.н. профессор МГИМО (У) МИД России



Из выступления на круглом столе: "Проблемы современных международных отношений в контексте киберпространства" журнала "Международная жизнь" (в рамках Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»)

Гармиш-Партенкирхен, Германия, 27 апреля 2016 года

Уважаемые коллеги!

Планета охвачена беспрецедентной технологической революцией. Драйвером её феномена последние полвека являются информационно-коммуникационные технологии (ИКТ). Пронизывая практически все страты цивилизации, они, наряду с несомненным позитивом, резко обострили геополитическую турбулентность.

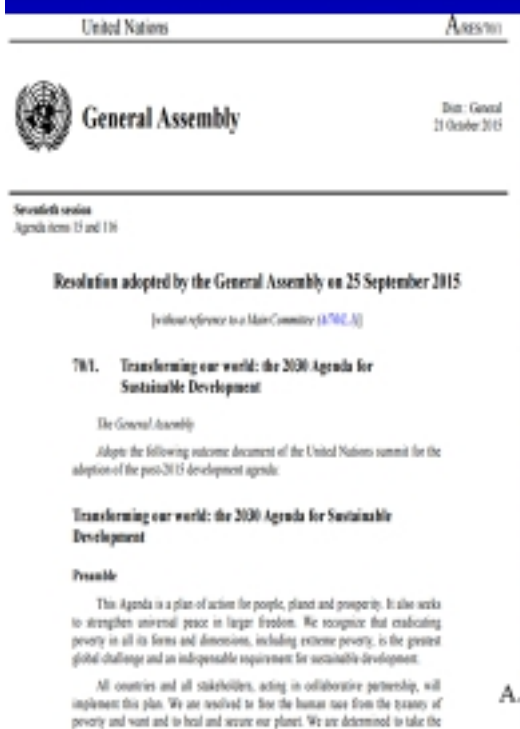
Наиболее емко сложившаяся ситуация оценена в Стратегии национальной безопасности России (утверждена Указом Президента России 31 декабря 2015 г. № 683): ««Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.»[1]

В этих условиях трудно переоценить важность принятой Генассамблеей ООН в сентябре 2015 г. резолюции «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 г.», содержащей 17 целей 169 задач.[2]

В выступлении Министра иностранных дел России С.В.Лаврова на Саммите по Глобальной повестке дня в области развития на период после 2015 года было внесено конкретное предложение: «Мы часто говорим о неделимости международного мира и безопасности. Новая социально-экономическая повестка дня должна закрепить также и понимание неделимости устойчивого развития... Особенно важно обеспечить справедливые условия торговли и расширить доступ к передовым технологиям.»[3]

Слова С.В. Лаврова были услышаны и включены в цель 9 принятой Повестки дня: «Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям».[4]

ГА ООН. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 г. (17 целей 169 задач) Transforming our world: the 2030 Agenda for Sustainable Development (17 Goals and 169 targets)



Goal 9. Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation

Цель 9. Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям

9.c Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020

9.c Существенно расширить доступ к ИКТ и стремиться к обеспечению всеобщего и недорогого доступа к Интернету в наименее развитых странах к 2020 году

Как заявил Генсек ООН Пан Ги Мун «17 целей в области устойчивого развития – это наше общее понимание путей развития человечества и социальный контракт между мировыми лидерами и населением, это перечень дел для людей и планеты и путь к успеху».[5]

В документе, вступившем в силу 1 января 2016 г., подчеркивается необходимость мобилизации средств для достижения Целей, в т.ч. финансовых ресурсов, разработки новых технологий и укрепления роли партнерств.

В этом контексте представляется весьма своевременным вынесение дискурса «IV промышленная революция» в качестве титульной темы Всемирного экономического форума (ВЭФ) в Давосе: (20-23.01. 2016 г.).[6]

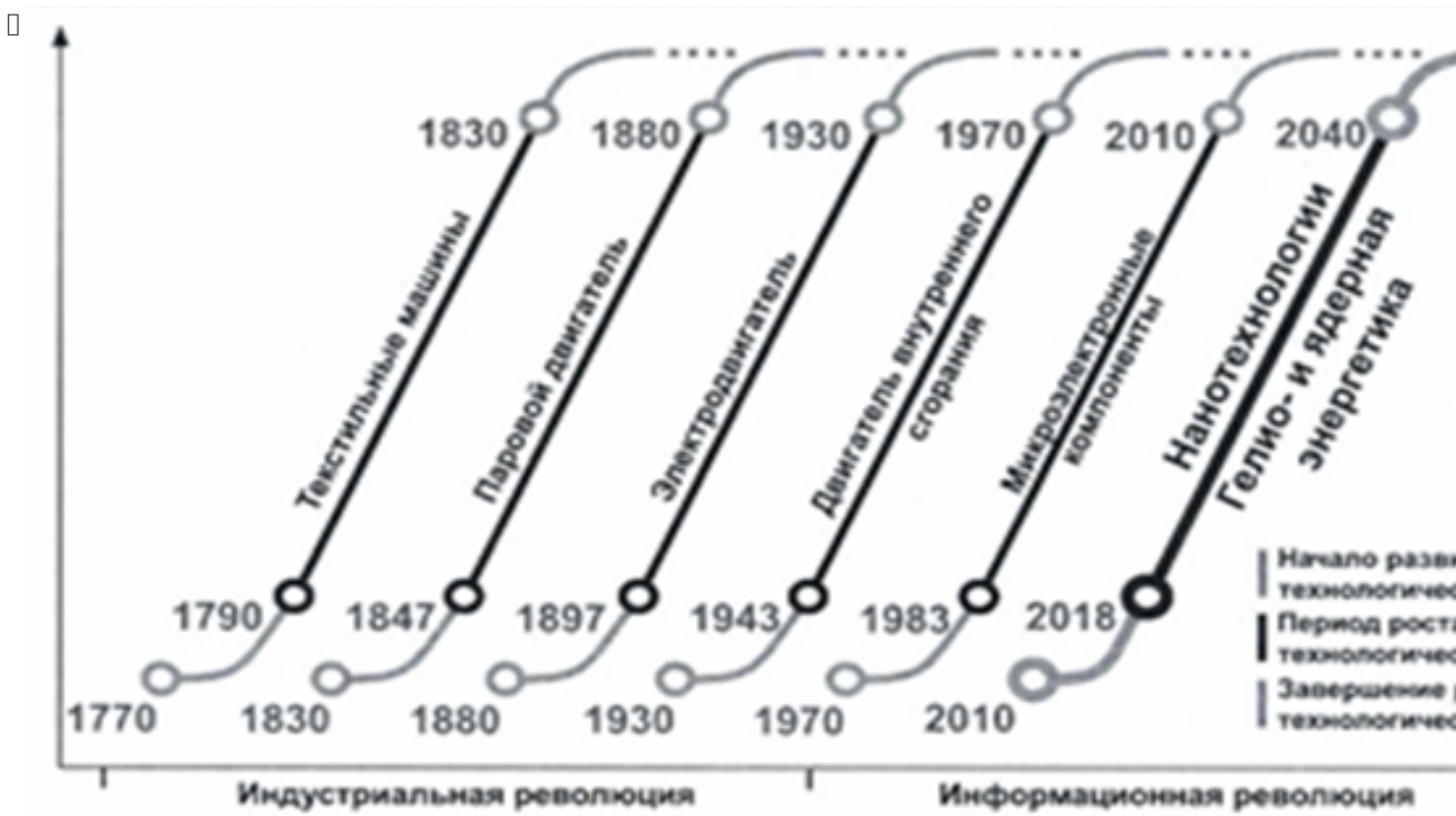
Президент и основатель ВЭФ Клаус Шваб посвятил данной теме свою новую книгу.[7] В ней он отмечает, что в первой промышленной революции сила воды и пара позволила механизировать производство. Во второй электроэнергия использовалась для организации массового производства. В третьей электроника и ИКТ автоматизировали производство.

Четвертая промышленная революция (Industry 4.0) - это конвергенция технологий, которые размывают границы между физической, цифровой и биологической сферами.

Следует отметить, что родиной первой революции принято считать Великобританию, второй – США, третьей – США и ЕС, а четвертой – ЕС.



Ряд российских экспертов, развивая теорию циклов Кондратьева, относят Industry 4.0 к шестому технологическому укладу – конвергенции nano-био-инфо- и когнитивных технологий (НБИК-технологий). [8]



Industry 4.0 стимулирует технологические прорывы в таких областях, как искусственный разум, робототехника, «интернет вещей» (Internet of Things, IoT), 3D-печать, нанотехнологии, биотехнологии, материаловедение, хранение энергии и квантовые вычисления.

При этом элементы искусственного разума можно уже сегодня реально видеть на примере самоуправляемых автомобилей, беспилотников, виртуальных помощников и программ, способных переводить с иностранных языков, инвестировать, разрабатывать новые лекарства и, даже, прогнозировать культурные интересы.

Пионером Industry 4.0 стала ФРГ, создавшая её концепцию еще в 2011 г. По сути, - это производственная форма, эквивалентная IoT, в котором предметы (от автомобилей до тостеров) взаимодействуют минуя людей (M2M). По оценкам рыночная стоимость, генерируемая IoT, как драйвером Industry 4.0, составит к 2020 г. несколько триллионов долларов США.[9]

Industry 4.0 постепенно охватывает весь мир. Так, США в 2014 г. создали некоммерческий консорциум Industrial Internet в составе General Electric, AT&T, IBM и Intel. Открывшаяся 26 апреля 2016 г. в Ганновере выставка подтвердила данный тренд и высокую эффективность применения платформы Industry 4.0.[10]

Вместе с тем, министр экономики ФРГ З. Габриэль высказал опасение, что «большие данные» (big data), необходимые для Industry 4.0, собираются не национальными компаниями, а четырьмя фирмами из Кремниевой долины.[11] Ранее о технологическом шпионаже АНБ США против фирмы «Сименс» рассказал в интервью телеканалу ФРГ ARD Э. Сноуден.[12]

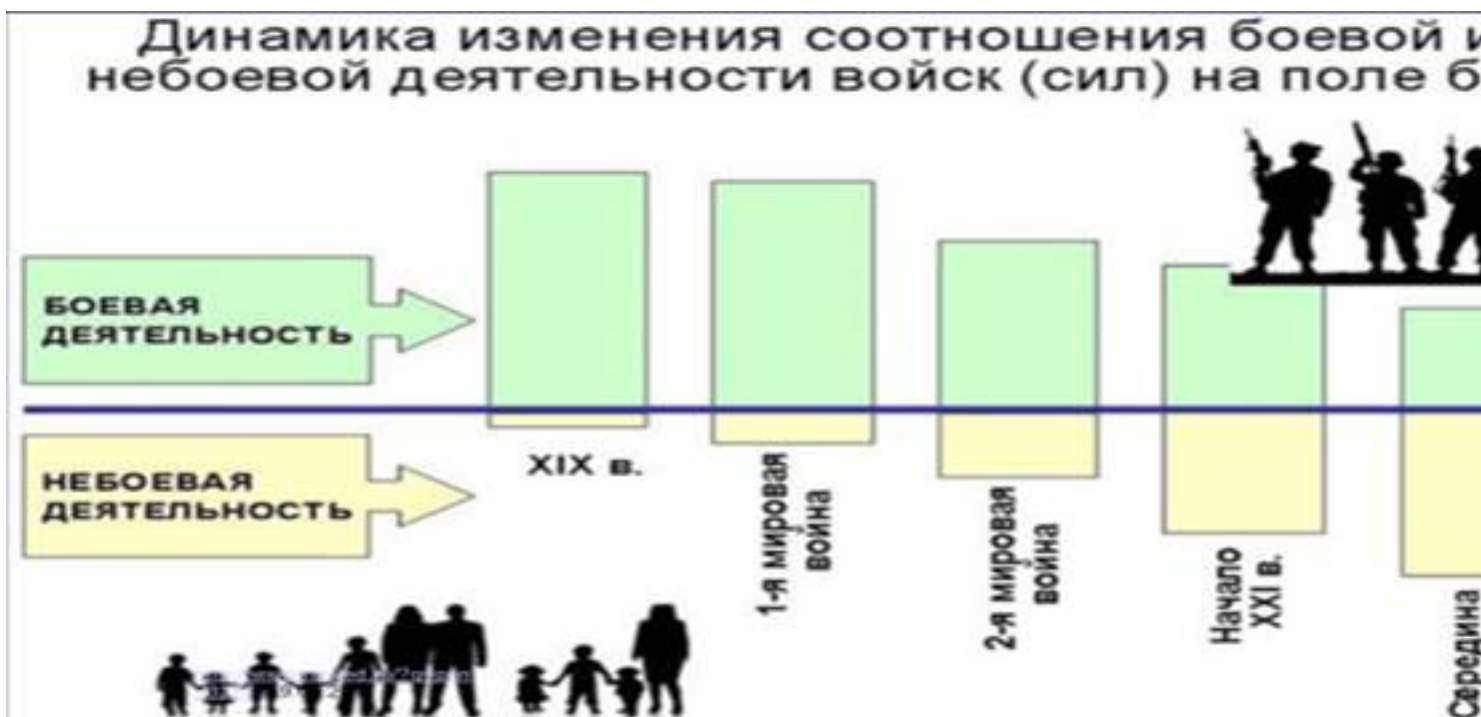
В более широком плане об угрозе для международной безопасности предупреждает в своей книге Клаус Шваб. Он предсказывает, что Industry 4.0 способна оказать сильное воздействие на национальную и международную безопасность, ибо **история войн — это история технологических прорывов**

Шваб отмечает, что конфликты между странами носят все более гибридный характер. Границы между войной и миром, воюющей и невоюющей сторонами, даже между насилием и его отсутствием (например, кибервойна) становятся все менее четкими.

При этом на сегодня нет единого понимания термина «гибридные» войны, обозначающего согласованное применение политико-дипломатических, информационно-психологических, экономических и силовых инструментов для достижения стратегических целей. Широко употребляются такие определения, как "неявные военные действия", "нелинейные", "асимметричные", "нетрадиционные", "гибридные" и т.д. операции.

Следует отметить, что в экспертных кругах НАТО для обозначения якобы негативной роли России в кризисных точках, как правило, используется понятие "гибридные войны".[13]

Наглядно эволюцию перехода человечества к войнам нового поколения дает следующая схема.[14]



В этом контексте уместно напомнить заявление Секретаря Совета Безопасности России Н.П.Патрушева «О четвертой международной встрече высоких представителей, курирующих вопросы безопасности»(г. Владивосток, 2 - 4 июля 2013 г.).[15]

В заявлении было отмечено, что в рамках встречи было с интересом заслушано сообщение российской делегации о современном этапе конвергенции наук и технологий как альтернативного ответа на новые вызовы и угрозы глобального характера. Одновременно подчеркивалась необходимость формирования нового эффективного международного механизма для обеспечения международной безопасности, в т.ч.

информационной.

Следует уточнить, что «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утверждены Президентом РФ 24 июля 2013 г. Пр-1753) определили угрозой в области международной информационной безопасности (МИБ) использование ИКТ в следующих целях:[16]

а) **в качестве информационного оружия** в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) **в террористических целях**, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) **для вмешательства во внутренние дела суверенных государств**, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;[17]

г) **для совершения преступлений**, в т.ч. связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

По оценкам экспертов Industry 4.0 не только усиливает все вышеперечисленные угрозы для МИБ, но и создает принципиально новые.

[18]

Действительно, интеграция физических систем с Интернетом делает их весьма

уязвимыми к кибератакам. Автоматизированные системы управления, в т.ч. критически важных объектов, способны стать легкой добычей кибертеррористов, которые смогут манипулировать протоколом производства или просто парализовать этот процесс.

Абсолютно новые возможности появляются для разработчиков и обладателей информационного оружия, ибо кроме США, ещё около 100 стран мира имеют в составе Вооружённых сил подразделения для проведения операций в киберпространстве.[19]

Для понимания разницы между видами информации и видами войн рассмотрим следующую схему.[20]



Киберпространство (англ. cyberspace) — метафорическая абстракция, используемая в философии и в компьютерных технологиях, является (виртуальной) реальностью, которая представляет мир как «внутри» компьютеров так и «внутри» компьютерных сетей. Ему соответствует **кибервойна, т.е. технологическое противоборство.**

Инфосфера – это киберпространство плюс контент. Ей соответствует **информационная война**. В

современных веб-сервисах весьма трудно отделить технологии от контента. Так, многие браузеры используют агрегаторы новостей со своей иерархией их важности.

Вот почему Россия выступает за достижение договоренности по информационной безопасности, а оппоненты – за кибербезопасность, чтобы развязать себе руки для вмешательства медиаконтентом во внутренние дела суверенных государств.

Ноосфера ("Ноос" в переводе с греческого - разум) - это оболочка разума вокруг планеты. Ей соответствует **сетецентрическая война** (СЦВ). Концепция СЦВ появилась в США в конце 1990-х годов. В СЦВ все рода войск, средства связи и разведки, в т.ч. военные спутники и беспилотные летательные аппараты объединяются в одну систему. В СЦВ используются суперсовременные информационные и сетевые технологии для интеграции географически рассредоточенных органов управления, средств разведки, наблюдения и целеуказания, а также группировок войск и высокоточных средств поражения в высокоадаптивную, глобальную систему с широким использованием средств радиоэлектронной борьбы.

Примером сетецентрических операций стран-членов НАТО против Союзного государства может быть следующая схема.[21]



Рис. 1.3.1. Матрица сетевых воздействий против Союзного государства

В связи со вскрытым лабораторией Касперского фактом кибератак на государственные и дипучреждения России особое место занимает **Указ Президента России от 15 января 2013 г. № 31с** [22]. Указ возложил на ФСБ России создание «государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом».

На основе Указа была разработана и утверждена Президентом России (12 декабря 2014 г. № К 1274) «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [23] (СОПКА).

СОПКА - это технологии, а также технические, программные, правовые, лингвистические, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры), предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак на информресурсы России.

Вышеизложенное убедительно показывает, что та страна, которая овладеет всем потенциалом НБИК-технологий, в том числе в военно-политической сфере, способна получить неоспоримые преимущества в геополитической конкуренции.

В силу этого среди приоритетов Стратегии национальной безопасности России (п.70) поставлена задача развития перспективных высоких технологий (геновая инженерия, робототехника, биологические, информационные и коммуникационные, когнитивные технологии, нанотехнологии, природоподобные конвергентные технологии).

Одновременно Россия продолжает инициировать создание комплексной системы МИБ в различных форматах сотрудничества: ООН, БРИКС, ОБСЕ, СНГ, ШОС, ОДКБ и других важных международных и региональных площадках, а также в двусторонних отношениях со всеми заинтересованными государствами.

Убежден, что данная проблема станет предметом самого пристального дискурса в работе Группы правительственных экспертов ООН по проблематике МИБ в 2016-2017 гг.

В конце мая 2016 г. в г. Грозном прошла VII Международная встреча высоких представителей, курирующих вопросы безопасности. В её работе участвовали делегации из ООН и из 75 стран мира, численность населения которых более 70% от всех проживающих на планете. Секретарь Совета Безопасности Российской Федерации Н.П.Патрушев по итогам встречи заявил следующее.[24]

« ... подробно рассмотрены вопросы международной информационной безопасности. В частности, говорилось об основных принципах и правилах поведения государств в глобальном информационном пространстве.

Подчеркнуто, что возросло число угроз национальной и международной информационной безопасности. К примеру, компьютерные атаки на государственные интернет-ресурсы крупнейших стран мира ежегодно исчисляются десятками миллионов.

Противостоять данным угрозам в одиночку не под силу ни одной мировой державе... Первоочередной задачей может стать выработка универсальных правил ответственного поведения государств в информационном пространстве и их последующее принятие под эгидой ООН.

Отмечу, что число сторонников этой идеи неуклонно растет. Подтверждением этому служит согласованное принятие на 70-й сессии Генассамблеи ООН российского проекта резолюции о начале работы нового состава Группы правительственных экспертов.

Соавторами документа стали 84 государства, что позволяет надеяться, что Группа со своей основной задачей - выработкой указанных правил - справится.

В цифровой сфере должны действовать такие общепризнанные международно-правовые принципы, как неприменение силы или угрозы силой, уважение суверенитета, невмешательство во внутренние дела государств. Однако с учетом специфики информационно-коммуникационных технологий может потребоваться разработка новых норм международного права...».

[1] <http://kremlin.ru/acts/news/51129>

[2] <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/285/75/PDF/N1528575.pdf?OpenElement>

[3] http://www.mid.ru/general_assembly/-/asset_publisher/lrzZMhfoyRUj/content/id/1794073

[4] <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/285/75/PDF/N1528575.pdf?OpenElement>

[5] <http://www.un.org/russian/news/story.asp?newsID=25172#.V10PNfmLShc>

[6] <http://ria.ru/spravka/20160120/1361326733.html>

[7] <https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab/>

[8] См. Глазьев С.Ю. Уроки современной революции: крах либеральной утопии и шанс на «экономическое чудо»/С.Ю. Глазьев.-М. Издательский дом «Экономическая газета», 2011.- С.330

[9] <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-E.pdf>
22.12.2015

[10] <https://www.plattform-i40.de/I40/Redaktion/EN/PressReleases/2016/2016-04-26-plattform-presents-positive-annual-results-hmi.html>

[11] <http://hi-news.ru/business-analitics/industriya-4-0-cto-takoe-chetvertaya-promyshlennaya-revolyuciya.html>

[12] <http://www.bbc.com/news/25907502>

[13] http://factmil.com/publ/strana/nato/teorija_t_praktika_vedenija_gibridnykh_vojn_po_vzgljadam_nato_2015/61-1-0-730

[14] См. Подберезкин А.И. Евразийская воздушно-космическая оборона. М.: МГИМО–Университет, 2013. - 488 с. <http://www.nasled.ru/?q=print/3274>

[15] <http://www.scrf.gov.ru/news/794.html>

[16] <http://www.scrf.gov.ru/documents/6/114.html>

[17] Данная угроза четко изложена в п.21.Стратегии национальной безопасности Российской Федерации (утверждена Указом Президента России 31 декабря 2015 г. № 683) «Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.»

[18] <http://hi-news.ru/business-analitics/industriya-4-0-cto-takoe-chetvertaya-promyshlennaya-revolyuciya.html>

[19] См. Микрюков В. Ю. Информационные войны <http://nic-pnb.ru/operational-analytics/informatsionnye-vojny/>

[20] См. Глобальная безопасность в цифровую эпоху: стратегемы для России. Под общ. ред. Смирнова А.И.-М.: ВНИИГеосистем, 2014. С.114 <http://niiglob.ru/ru/2011-01-15-10-08-52/507-kniga-qglobalnaya-bezopasnost-v-czifrovuyu-epochu-stratagemy-dlya-rossiiq.html>

[21] См. Глобальная безопасность в цифровую эпоху: стратегемы для России. Под общ. ред. Смирнова А.И.-М.: ВНИИГеосистем, 2014. С.116 <http://niiglob.ru/ru/2011-01-15-10-08-52/507-kniga-qglobalnaya-bezopasnost-v-czifrovuyu-epochu-stratagemy-dlya-rossiiq.html>

[22] <http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html>

[23] <http://www.scrf.gov.ru/documents/6/131.html>

[24] <http://www.scrf.gov.ru/news/1083.html>

[Источник ...](#)