А.И. СМИРНОВ

МЕГАТРЕНДЫ ИНФОРМАЦИОННОЙ ГЛОБАЛИЗАЦИИ

Смирнов Анатолий Иванович, *Президент Национального института исследований глобальной безопасности, Член Экспертного совета Комитета Государственной Думы Федерального Собрания Российской Федерации по безопасности и противодействию коррупции, Чрезвычайный и Полномочный Посланник РФ в отставке, д.и.н., профессор МГИМО МИД России*
E-mail: aismirnov@niiglob.ru

Аннотация

В статье рассматриваются мегатренды информационной глобализации как многомерного процесса. Информационно-коммуникационные технологии (ИКТ) стали драйвером пятого технологического уклада цивилизации, а основой шестого должны стать конвергенция нано-, био-, информационных и когнитивных технологий (NBIC). Наряду с несомненным позитивом для социализации человечества ИКТ породили и принципиально новые угрозы – инфогенные. Как следствие, в условиях обострения международной обстановки резко возросла роль проблемы укрепления международной информационной безопасности (МИБ).

Ключевые слова: *технологический уклад, информационная глобализация, информационно-коммуникационные технологии международная информационная безопасность, ООН, ШОС, НАТО, КНР, США.*

ВЕХИ ЦИВИЛИЗАЦИИ: ОТ ПЕЩЕРЫ ДО HOMO INFORMATICUS

Начало XXI века может остаться в истории человечества как один из самых драматичных периодов с точки зрения угроз глобальной безопасности. Планета вошла в зону геополитической турбулентности. Об этом убедительно свидетельствуют:

- «цветные революции»,
- терроризм,
- рецидивы «холодной войны» и санкций,
- всплеск локальных и региональных конфликтов,
- техногенные, природные и социогенные катастрофы,
- эпидемии новых заболеваний,
- голод.

Стремительное вступление человечества в цифровую эру своего развития, наряду с несомненным позитивом, вызвало и резкое возрастание инфогенных угроз. Это нашло отражение в целом ряде документов на международном (ООН, ШОС, СНГ, ОДКБ и др.) и национальном уровнях.

Рассмотрим кратко эволюцию человечества за хотя бы сколько-нибудь обозримые 50 тыс. лет его существования, что составляет примерно 1 600 поколений. Из числа этих поколений:

- 1 100 – провели жизнь в пещерах;
- 800 – применяют огонь;
- 400 – используют силу животных;
- 300 – владеют энергией воды и ветра;
- 150 – используют для осуществления связи поколений письменности;
- 16 – применяют порох;
- 8 – измеряют точное время;
- 6 – используют искусственные источники энергии;
- 4 – применяют электромоторы;
- 2 – владеют атомной энергией, реактивной авиацией, телевидением, лазерами, антибиотиками.

И *только одно поколение* применяет персональные компьютеры, Интернет, космические, генные, когнитивные и нанотехнологии.

Данное поколение некоторые эксперты называют поколением информационной глобализации [8, с. 8–9], его представителей – «Homo Informaticus», а молодежь – «цифровыми аборигенами».

ИКТ – ЛОКОМОТИВ ПЯТОГО ТЕХНОЛОГИЧЕСКОГО УКЛАДА ЧЕЛОВЕЧЕСТВА

Используя термин «технологический уклад» (комплекс технологий, изобретений и инноваций, лежащих в основе количественного и качественного скачка в развитии производительных сил общества), можно констатировать, что человечество, пройдя пять технологических укладов, находится в точке бифуркации, входя в шестой.

Схему технологических укладов с указанием характерных для них технологий была предложена академиком РАН С.Ю. Глазьевым [3, с. 330] (*Рисунок 1*).

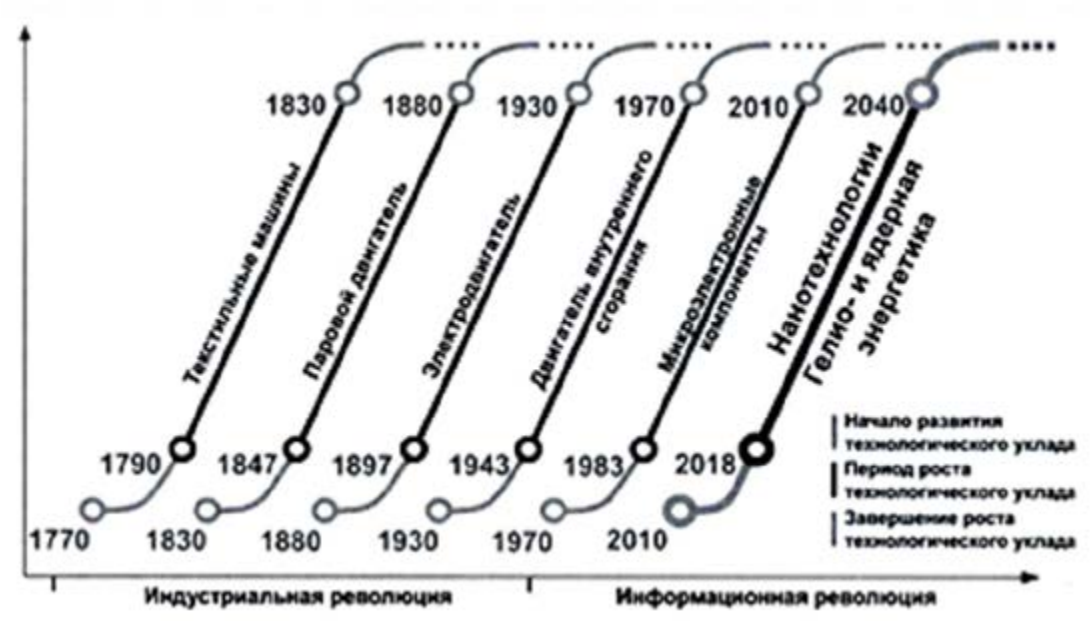

Рисунок 1. Смена технологических укладов.

ОСНОВНЫЕ ТРЕНДЫ ПЯТОГО ТЕХНОЛОГИЧЕСКОГО УКЛАДА

Принято считать, что пятый технологический уклад стартовал на рубеже 1940–1950-х гг., когда американскими физиками был изобретен транзистор, что положило, в частности, начало развитию микроэлектроники и созданию более надежной и не столь энергоемкой элементной базы для изобретенных несколько раньше ЭВМ. Транзистор совершил революцию в технологии радио, привел к созданию микросхем, микропроцессоров, компьютеров и многих других телекоммуникационных систем. Это был выход из «первобытного механического» века в век электронный, космический и компьютерный.

На этом этапе впервые в истории предмет конкуренции (знания, технологии и производство) перестал служить целям простой замены человеческого труда двигательной силой машин, как в предыдущих укладах. Вместо этого он стал служить целям развития доселе неизвестных интеллектуальных сил *массовой автоматизации производства, проектирования изделий и управления предприятием*. Стал закладываться принципиально другой способ преобразования ресурсов в интеллектуальную силу. В жизнь человека вошли Интернет, мобильный телефон и иные гаджеты и сервисы.

ЗАКОН МУРА

Наиболее ярко динамика ИКТ прослеживается на примере так называемого закона Мура. Инженер Гордон Мур эмпирически описал удвоение числа транзисторов на кристалле микропроцессора каждые два года[1]. Вертикальная ось имеет логарифмическую (!) шкалу, то есть кривая соответствует экспоненциальному закону – количество транзисторов удваивается практически каждые 2 года (см. *Рисунок 2*) [5].

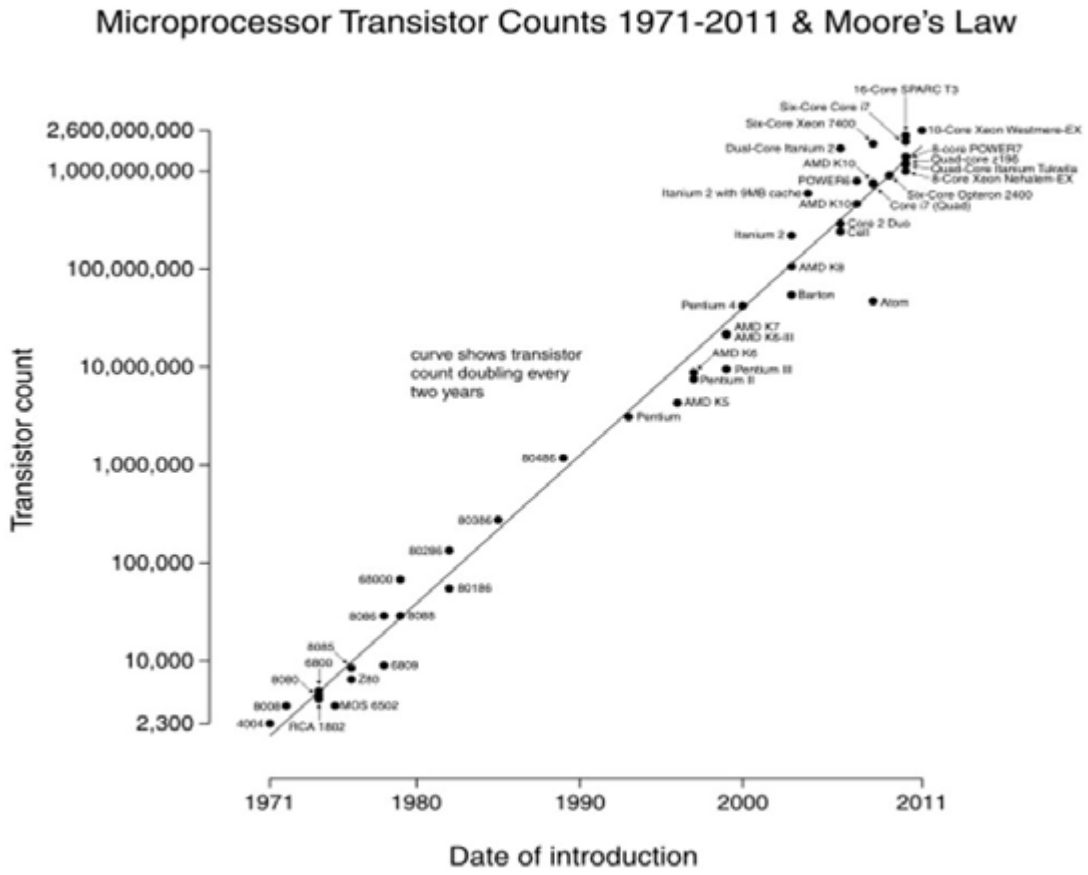

Рисунок 2. Закон Мура и рост количества транзисторов в процессорах.

[1] Часто цитируемый интервал в 18 месяцев связан с прогнозом Давида Хауса из компании Intel, по мнению которого, производительность процессоров должна удваиваться каждые 18 месяцев из-за сочетания роста количества транзисторов и быстродействия каждого из них.

ИЗМЕРЕНИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА МЕЖДУНАРОДНЫМ СОЮЗОМ ЭЛЕКТРОСВЯЗИ

Международный союз электросвязи (International Telecommunication Union, ITU), специализированное подразделение ООН в области ИКТ, исследовал развитие ИКТ в странах мира за 2013–2014 гг. [10]. Результатом стал доклад «Измерение информационного общества 2014» (Measuring the Information Society 2014), содержащий рейтинг развития 166 стран в сфере ИКТ. Первое место у Дании, а Южная Корея, возглавлявшая данный рейтинг предыдущие три года, занимает 2-е место. Место России – 42-е.

Индекс развития ИКТ (ICT Development Index) разработан в 2007 г. на основе 11 показателей и сводится в единый критерий, который можно использовать для проведения сравнительного анализа на глобальном, региональном и национальном уровнях. Эти показатели касаются доступа к ИКТ, их использования, а также практического знания этих технологий, в т.ч.: число стационарных и мобильных телефонов на 100 жителей страны, количество домашних хозяйств, имеющих компьютер, количество пользователей Интернета, уровни грамотности и т.д.

Первые 30 мест в рейтинге занимают страны с высоким уровнем дохода, что говорит о прочной взаимосвязи между доходом и прогрессом в области ИКТ. Наряду с европейцами, к числу 30 ведущих стран относятся экономики с высоким уровнем доходов из Азиатско-Тихоокеанского региона (Австралия, Макао /Китай/, Сингапур и Новая Зеландия), а также США и Канада из региона Северной Америки.

Несмотря на широкое распространение ИКТ во всем мире, налицо значительные различия между развитыми и развивающимися странами, причем значения этого индекса в развитом мире в среднем вдвое выше, чем в развивающихся странах, в которых проживают 2,4 млрд человек. К числу таких регионов относятся африканские страны, а также некоторые густонаселенные районы Индии, Пакистана и др.

В докладе также отмечены страны, которые стремительно сокращают «цифровой разрыв». К их числу относятся: ОАЭ, Барбадос, Сейшельские Острова, Беларусь, Коста-Рика, Монголия, Замбия, Австралия, Бангладеш, Оман и Зимбабве[2].

ТРЕНДЫ ОХВАТА ПЛАНЕТЫ ИНТЕРНЕТОМ И МОБИЛЬНОЙ СВЯЗЬЮ

Как видно из диаграмм на *Рисунках 3–5* к концу 2014 г. к Интернету были подключены около 2,9 млрд человек (почти 40 % населения мира). При этом доля подключенного населения в развитых странах достигла почти 78,6 %, по сравнению с 31,5 % в развивающихся странах, а цены на фиксированную широкополосную связь в процентах от ВНД на душу населения упали за 4 года на 82 % [9].

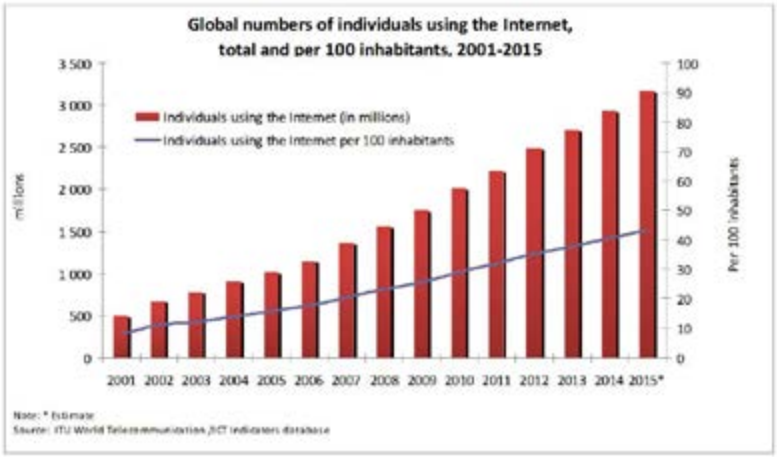

Рисунок 3. Число индивидуальных пользователей Интернета в мире (общее и в расчете на 100 человек).

[2] С полным видом Таблицы, отображающей рейтинг развития ИКТ в 2014 г. можно ознакомиться по адресу: [Электронный ресурс]. URL: http://www.itu.int/ en/ ITU-D/Statistics/Pages/publications/mis2014.aspx.

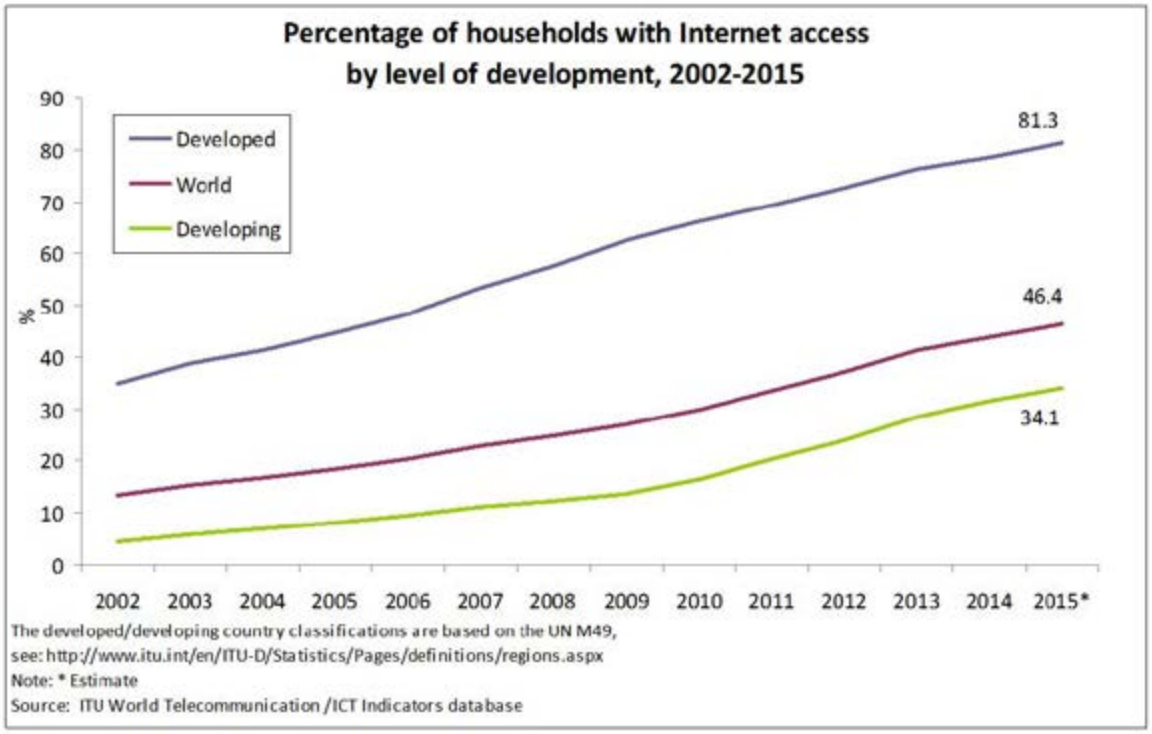

Рисунок 4. Процент домовладений с доступом к Интернету в зависимости от уровня развития (сверху вниз: развитые страны – мир в среднем – развивающиеся страны)

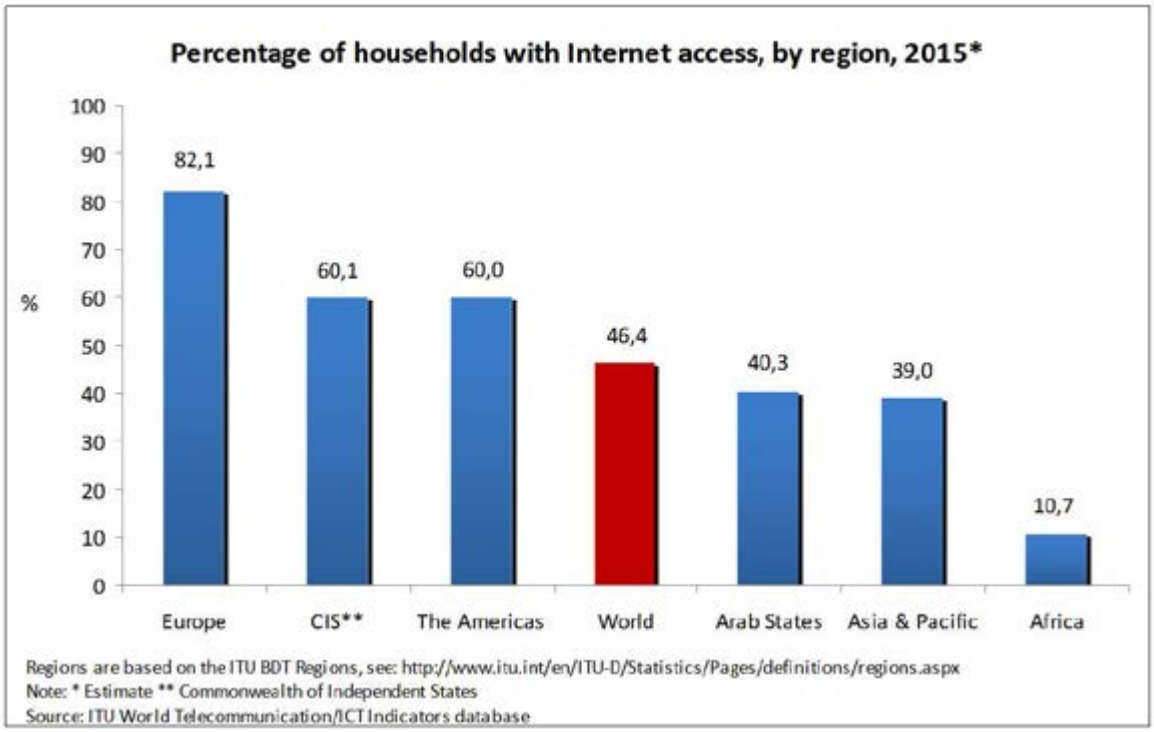

Рисунок 5. Процент домовладений с доступом к Интернету по регионам (Европа – СНГ – Америка – мир в среднем – арабские страны – АТР–Африка)

Анализ диаграмм на *Рисунках 6–7* [9] показывает, что человечество вплотную подошло к полному охвату мобильной связью. Однако это чисто количественный подход. Реально в ряде стран охват значительно ниже. Улучшается статистика там, где на каждого жителя приходится более одной SIM-карты.

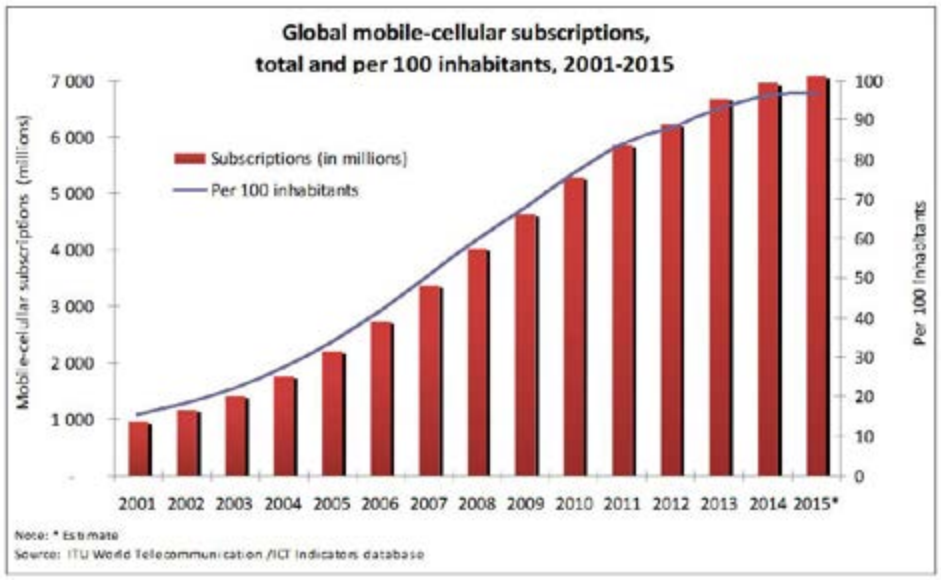

Рисунок 6. Количество подписчиков на услуги сотовой связи в мире (общее и в расчете на 100 человек).

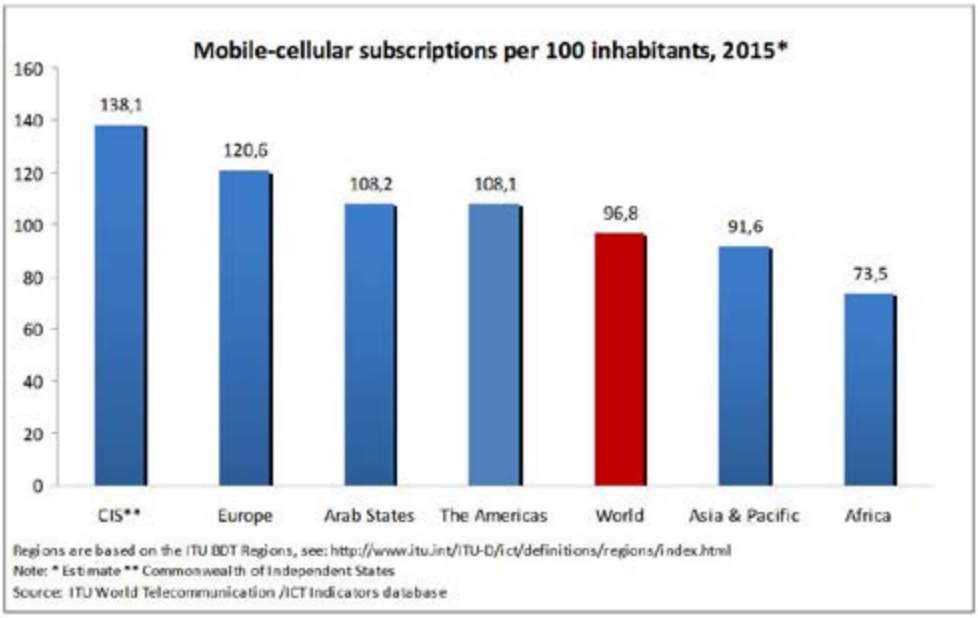

Рисунок 7. Количество подписчиков на услуги сотовой связи по регионам, в расчете на 100 человек (Европа – СНГ – Америка – мир в среднем – арабские страны – АТР – Африка).

ИНТЕЛЛЕКТУАЛЬНЫЕ СИЛЫ ЧЕЛОВЕКА КАК ОСНОВА ШЕСТОГО ТЕХНОЛОГИЧЕСКОГО УКЛАДА И СБОЙ БРЕТТОН-ВУДСКОЙ СИСТЕМЫ

Как уже отмечалось, цивилизация находится на пороге шестого технологического уклада. В отличие от предыдущих укладов, в его основе не двигательная сила, направленная на базовые элементы глобальной конкуренции, а интеллектуальные силы человека.

В рамках четвертого и пятого технологических укладов глобальная конкуренция поддерживалась с помощью мощного финансового ресурса (долларов), исходящего главным образом из США.

При переходе мировой экономики к шестому технологическому укладу происходит *системный сбой*, выражающийся в истощении и потенциала, и кредитного ресурса Бреттон-Вудской системы (позднее Ямайской валютной системы, предполагающей свободную конвертацию валют).

Этот сбой приводит к кризисным явлениям в мировой финансовой системе и на рынке инвестиций. В силу этого многие эксперты работают над новой моделью, ориентированной на системные инновационные прорывы.

Это означает, что в шестом технологическом укладе кредит как двигательная сила экономики *уступает место интеллектуальной силе, направленной на конвергенцию высоких технологий* (NBIC – нано-, био-, информационных и когнитивных технологий[3]).

ШЕСТОЙ ТЕХНОЛОГИЧЕСКИЙ УКЛАД: НОВЫЕ ВОЗМОЖНОСТИ И СТРАТЕГИЧЕСКИЕ РИСКИ ДЛЯ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

С учетом появления принципиально новых вызовов и стратегических рисков для глобальной безопасности при переходе в шестой технологический уклад представляется оправданным привести заявление Секретаря Совета Безопасности России Н.П. Патрушева от 4 июля 2013 г. «О четвертой международной встрече высоких представителей, курирующих вопросы безопасности», состоявшейся 2–4 июля 2013 г. в г. Владивостоке [6].

В этом заявлении было подчеркнуто, что в рамках «Четвертой международной встречи высоких представителей, курирующих вопросы безопасности» было «с интересом заслушано сообщение делегации Российской Федерации о современном этапе конвергенции наук и технологий как альтернативного ответа на новые вызовы и угрозы глобального характера. Подчеркивалась необходимость формирования нового эффективного международного механизма обеспечения безопасного развития и использования конвергентных технологий».

Как представляется, то государство, которое первым массово овладеет НБИК-технологиями, в том числе в военных целях, сможет диктовать свои правила игры в мировой политике. Ведущие государства разработали доктринальные основы использования ИКТ- и НБИК- технологии в противоборстве за глобальное информационное доминирование, в том числе путем гибридных войн и «цветных революций».

Именно данное обстоятельство побудило руководство России разработать «Основы государственной политики в области международной информационной безопасности на период до 2020 г.» (утверждены Президентом Российской Федерации В. Путиным 24 июля 2013 г. № Пр-1753). В «Основах», наряду с традиционной триадой угроз ИКТ (военно-политическая, киберпреступность и кибертерроризм), зафиксирована угроза использования ИКТ для вмешательства во внутренние дела.

Учитывая стратегическую важность данной проблемы, 1 октября 2014 г. на заседание Совета Безопасности России был внесен вопрос «О противодействии угрозам национальной безопасности РФ в информационной сфере». Выступая на нем, президент В.В. Путин подчеркнул: «Надёжная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России» [2].

На заседании Коллегии ФСБ России 26 марта 2015 г. В.В. Путин конкретизировал данные угрозы. «Количество кибератак на официальные сайты и информационные системы органов власти России не уменьшается, только в прошлом году их пресечено около 74 миллионов.

Кроме того, выявлено свыше 25 тысяч Интернет-ресурсов с публикациями, нарушающими закон. Прекращена работа более полутора тысяч экстремистских сайтов. Нужно продолжать очищать российское Интернет-пространство от незаконных, преступных материалов, более активно использовать для этого современные технологии, участвовать в формировании системы международной информационной безопасности» [1].

В целях противодействия угрозам информационной безопасности России при использовании информационно-телекоммуникационной сети Интернет Указом Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» сегмент международной компьютерной сети Интернет

[3] Перспектива включения в системную конвергенцию и, соответственно, в обозначающую ее аббревиатуру пятого компонента – Социо (S) пока только обсуждается.

для федеральных органов госвласти и органов госвласти субъектов Российской Федерации, находящийся в ведении ФСО России, преобразован в российский государственный сегмент Интернета, являющийся элементом российской части сети Интернет.

Порядком определено, что:

- Подключение информсистем и информационно-телекоммуникационных сетей к сети Интернет и размещение (публикации) в ней информации через российский госсегмент информационно-телекоммуникационной сети Интернет осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств (далее – защищенные каналы).
- Защита информации в информсистемах и информационно-телекоммуникационных сетях, подключаемых к сети Интернет через российский сегмент, в том числе с использованием средств госсистемы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информресурсы России, обеспечивается в соответствии с законодательством России.

Принятие столь жестких мер Россией диктуется тем, что в США взят курс на *наступательную* стратегию кибервойны (разоблачения Э. Сноудена лишь подтверждают правильность данных мер).

Так, в начале 2015 г. Минобороны США приняло новую, по сути наступательную, стратегию кибервойны (стратегия кибербезопасности 2011 г. носила оборонительный характер).

В новой стратегии предусмотрены кибератаки на военные вычислительные сети и инфраструктуру противника в регионах, где США имеют свои интересы. Решение о кибератаке принимают президент США и министр обороны (например, вывести из строя командно-контрольные сети противника и лишить его способности применять оружие). За кибероперации отвечает Киберкомандование США (USCYBERCOM), созданное в рамках вооруженных сил США в 2010 г. К 2016 г. в USCYBERCOM должно быть около 6,2 тыс. человек.

Новую стратегию представил министр обороны Эштон Картер и назвал четыре государства, представляющие для США наибольшую угрозу в киберпространстве – это Китай, Россия, Иран и Северная Корея.

КИБЕРПРОЕКТЫ НАТО

Наибольшую угрозу миру представляют киберпроекты НАТО. Если в Декларация саммита НАТО в Лиссабоне (2010 г.) кибербезопасность была упомянута только один раз, то на саммите НАТО в Уэльсе (4–5.09.2014), кибербезопасность стала ключевой проблемой – 21 упоминание!

В Стратегической концепции НАТО, принятой в Лиссабоне, говорится о необходимости создания потенциала для выявления, предотвращения и защиты от кибернетических атак. Для этого требуется задействовать механизмы объединенного планирования, координировать национальные программы защиты киберпространства, включая совместную работу систем предупреждения и реагирования на кибератаки, а также создать единую систему информационной безопасности для всех структур НАТО. Таким образом, в стратегическую концепцию НАТО впервые включено положение о киберпространстве как новой сфере военной деятельности альянса. При этом в экспертных кругах полагают, что компьютерные атаки могут быть приравнены к началу боевых действий .

Особую роль в подготовке данной позиции сыграл созданный НАТО в 2008 г. в Таллине Объединенный Центр перспективных исселований НАТО в области киберзащиты (NATO Cooperative Cyber Defence Center of Excellence, см. URL: https://ccdcoe.org/).

Центр имеет статус военной организации, входит в систему 20 Центров перспективных исследований НАТО и насчитывает 48 экспертов из 16 стран. Цель – консультирование, обучение специалистов, исследования в области кибербезопасности.

Основные направления деятельности Центра: исследования, правовая поддержка, требования и стандарты для НАТО, разработка учебных программ, мониторинг и сбор данных, практическая поддержка учений НАТО.

Основным результатом экспертной работы центра стала публикация в 2013 г. Таллинского руководства по применению международного права к ведению кибервойн («Tallinn Manual on

the International Law Applicable to Cyber Warfare»), содержащего 95 правил, регламентирующих применение международного гуманитарного права к конфликтам в цифровой среде.

В начале 2016 г. ожидается выход второго издания, посвященного маргинальным кибератакам в мирное и военное время, в том числе правовому реагированию на киберпреступления.

Центр имеет мощную информационную базу, в том числе интерактивную базу данных INCYDER, электронную библиотеку публикаций, включая ведущие международные и национальные ресурсы, глоссарий и т.д.

Крупнейшие в истории НАТО транснациональные военные киберучения (Cyber Coalition) в ноябре 2014 г. и в апреле 2015 г. собрали свыше 1 000 экспертов из 16 стран НАТО. В ходе маневров были использованы реальные технологии, компьютерные сети и методы отражения кибератак.

По сценарию зарубежные атаки на условное государство дополнялись давлением со стороны СМИ и правовыми ограничениями.

Задачей экспертов была проверка готовности к оперативному обмену защищенной информацией о киберинцидентах, а также к координации усилий по обороне от целевых атак непосредственно на компьютерные сети НАТО.

Эксперты Центра принимали участие не только в учениях, но и в практических мероприятиях. Одним из них стало участие в виртуальном украинском фронте против «Киберберкута» под ником «Киберсотня».

Характерно, что в г. Риге НАТО создала еще один центр – Центр перспективных исследований в области стратегических коммуникаций (NATO Strategic Communication Center of Excellence, см. URL: http://www.stratcomcoe.org/). Центр представляет собой международную организацию, объединившую семь стран, включая прибалтийские государства, Великобританию, Италию, Германию и Польшу. США в проекте формально не участвуют.

Одним из первых результатов деятельности Центра перспективных исследований в области стратегических коммуникаций стало исследование деятельности русских троллей в социальных сетях[4].

НАТО в 2013 г. завершила развертывание единой системы по реагированию на компьютерные угрозы, которая предназначена для своевременного выявления и нейтрализации киберугроз, а при необходимости и восстановления в работоспособности компьютерных сетей органов управления стран-участниц.

При этом остается открытым вопрос о разделении полномочий и сфер деятельности между национальными органами и альянсом. США и Великобритания выступают за возложение на НАТО всей ответственности за обеспечение защиты от киберугроз, что приведет к выстраиванию системы коллективной кибероборонs на базе американских технологий и максимальном привлечении их IT-компаний. Однако наиболее развитые в области кибербезопасности европейские страны (Германия, Франция, Италия и Испания) относят вопросы строительства и управления киберпотенциалом к национальной сфере компетенции, отводя НАТО лишь роль координатора.

ПОЗИЦИЯ РОССИИ И ЕЕ ПАРТНЕРОВ

Россия и ее партнеры не могли не отреагировать на новые угрозы кибер-НАТО. В утвержденной 25.12.2014 г. Военной доктрине Российской Федерации определены характерные черты и особенности современных военных конфликтов.

Среди них особое место занимает информационная составляющая:

- комплексное применение военной силы, политических, экономических, информационных и иных мер невоенного характера, реализуемых с широким использованием протестного потенциала населения и сил специальных операций;
- воздействие на противника на всю глубину его территории одновременно в глобальном информационном пространстве, в воздушно-космическом пространстве, на суше и море;

[4] URL: http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia

В этих условиях в январе 2015 г. по инициативе стран – членов ШОС в ООН внесены «Правила поведения в области обеспечения международной информационной безопасности». Документ опирается на проект «Правил поведения в области обеспечения МИБ ШОС (был направлен 66-й сессии ГА ООН в 2011 г.) с учетом изменившихся реалий и предложений от заинтересованных государств.

Его особенность – миротворческий характер: в отличие от концепций НАТО по регулированию кибервойн, документ нацелен на их предотвращение. Он предлагает:

- не применять ИКТ для нарушения мира и для вмешательства во внутренние дела других государств и подрыва их политической, экономической и социальной стабильности;
- воздерживаться от применения силы или её угрозы при разрешении споров, возникающих в цифровой сфере;
- признать, что права человека должны защищаться не только в оффлайне, но и в онлайне согласно ст. 19 Международного пакта о гражданских и политических правах;
- включить в понятие международной информационной безопасности также интернационализацию управления сетью Интернет, «наращивания потенциала» в сфере информбезопасности и преодоления «цифрового разрыва».

«Правила поведения» открыты для присоединения других государств.

8 мая 2015 г. в ходе визита Председателя КНР в Россию министры иностранных дел РФ и КНР подписали межправительственное соглашение о сотрудничестве в области МИБ [4].

Документ носит прорывной характер и выводит взаимодействие двух стран на принципиально новый уровень и предполагает, в частности:

- прикладной характер сотрудничества (совместное решение конкретных задач по обеспечению национальной и международной ИБ);
- диалог заинтересованных ведомств по вопросам МИБ;
- совместное реагирование на острые угрозы, включая противодействие использованию ИКТ в нарушение принципов международного права, в том числе для вмешательства во внутренние дела государств, подрыва суверенитета, политической и экономической стабильности, разжигания межнациональной и межконфессиональной вражды;
- борьбу с использованием ИКТ в террористических и иных противоправных целях;
- обмен информацией о рисках и угрозах;
- взаимодействие по совершенствованию международно-правовой базы;
- совместные меры укрепления доверия, научные исследования, подготовку и обмен студентами, аспирантами, преподавателями;
- суверенное право государств проводить госполитику по вопросам Интернет, в т.ч. его интернационализации;
- углубление сотрудничества в рамках ООН, МСЭ, ШОС, БРИКС и форума АСЕАН по безопасности.

18 мая 2015 г. под председательством С.В. Лаврова состоялось заседание коллегии МИД России по теме «Глобальные вызовы в области информационных технологий. Задачи МИД по обеспечению международной информационной безопасности» [7]. В работе коллегии приняли участие высокопоставленные представители всех заинтересованных ведомств.

На заседании, в частности, было отмечено, что:

- современная обстановка характеризуется нарастанием угрозы использования ИКТ в противоправных целях и в нарушение общепризнанных норм международного права;
- современные военно-политические, террористические и криминальные угрозы в информационной сфере носят глобальный характер, и борьба с ними требует принятия адекватных мер в самом широком масштабе;
- приоритетом России остается выработка универсальных правил ответственного поведения государств в информпространстве, которые бы препятствовали попыткам совершения актов агрессии, закрепляли бы принципы уважения государственного

суверенитета, невмешательства во внутренние дела других государств, основных прав и свобод человека;
- взаимодействие со всеми государствами, проявляющими готовность противостоять попыткам милитаризации информационной сферы, содействовать выработке международных норм по мирному использованию ИКТ.

Резюмируя, следует подчеркнуть, что доминантой развития цивилизации в среднесрочной перспективе *останутся ИКТ* и *НБИК-технологии*. При этом резко возрастает значение фактора *обеспечения информационной безопасности России*.

В силу этого требуется ускорить корректировку действующей Стратегии национальной безопасности (2009 г.), а также разработку и принятие новой Доктрины информационной безопасности России. Одновременно, совместно с партнерами по ОДКБ, ШОС и БРИКС необходимо договариваться о взаимодействии, в том числе в формате группы правительственных экспертов ООН по МИБ.

Альтернатива иррациональна – кибер-Армагеддон.

MEGATRENDS OF THE INFORMATION GLOBALIZATION

Anatoly I. Smirnov, *PhD, Professor,*
President-Chairman of Scientific Council,
Extraordinary and Pleanipotentionary Envoy,
member of Presidium of Russian academy of natural science
E-mail: aismirnov@niiglob.ru

Summary

This article discusses megatrends of information globalization as a multidimensional process. Information and communication technologies (ICTs) have become the driver of the fifth technological order of civilization and the foundation of the sixth. In addition to the undoubted positive for socialization of humanity ICT have generated a fundamentally new threats - infogens. In the face of the deteriorating of international situation has sharply increased role of strengthening of the international information security (IIS). Offensive approaches of NATO and the United States to the problem of the IIS are radically different from the peace approaches of Russia and its partners in the SCO.

Key words: *technological way, the information globalization, information and communication technologies, international information security, the UN, SCO, NATO, China, USA.*

ЛИТЕРАТУРА / REFERENCES

1. Выступление В.В. Путина на заседании Коллегии ФСБ России 26.03.2015. [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/49006
2. Выступление В.В. Путина на заседании Совета Безопасности Российской Федерации 01.10.2014. [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/46709
3. Глазьев С.Ю. Уроки современной революции: крах либеральной утопии и шанс на «экономическое чудо» / С.Ю. Глазьев.- М.: Издательский дом «Экономическая газета», 2011.
4. Документы, подписанные по итогам российско-китайских переговоров 08.05.2015. [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/4972
5. Закон Мура. [Электронный ресурс]. URL: http://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9C%D1%83%D1%80%D0%B0 10.01.2014
6. Заявление Н.П. Патрушева «О четвертой международной встрече высоких представителей, курирующих вопросы безопасности».[Электронный ресурс]. URL: http://www.scrf.gov.ru/news/794.html

7. О заседании Коллегии МИД России. [Электронный ресурс]. URL: http://www.mid.ru/zasedaniya_kollegii/-/asset_publisher/0kH5iObaLN9H/content/id/1283623
8. *Смирнов А.И.* Информационная глобализация и Россия: вызовы и возможности. – М.: Издательский Дом «Парад». 2005.
9. ITU Statistics URL: http://www.itu.int/ict/statistics)
10. Measuring the Information Society 2014. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf