ИНСТИТУТ МИРОВОЙ ЭКОНОМИКИ И МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
имени Е.М. ПРИМАКОВА
РОССИЙСКОЙ АКАДЕМИИ НАУК

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРИЗИСАХ И КОНФЛИКТАХ XXI ВЕКА

Под ред.
А.В. Загорского,
Н.П. Ромашкиной

Москва
ИМЭМО РАН
2015

УДК 327
ББК 66.4(0)
Угро 274

Серия «Библиотека Института мировой экономики и международных отношений имени Е.М. Примакова»

Рецензенты:
доктор юридических наук, доктор технических наук, профессор А.А. Стрельцов,
доктор исторических наук А.Н. Калядин,
доктор военных наук А.В. Агапов

Угро 274
Угрозы информационной безопасности в кризисах и конфликтах XXI века / Под ред. – А.В. Загорского, Н.П. Ромашкиной. – М.: ИМЭМО РАН, 2015. – 151 с.
ISBN 978-5-9535-0450-8

В публикации проводится анализ угроз в информационной сфере в современной системе международных отношений, которые выражаются в применении различных методов информационного воздействия, новых концепций противоборства с использованием информационно-телекоммуникационных средств. Исследуются примеры информационно-психологического противоборства и их политические последствия в периоды грузино-южноосетинского конфликта 2008 года и кризиса на Украине в период с 2013 по 2015 годов, а также методы кибервоздействия на критически важные инфраструктуры в конфликтных регионах мира. Анализируется внутригосударственная деятельность России по обеспечению информационной безопасности в XXI веке, а также роль РФ в международных структурах многостороннего взаимодействия в борьбе с новыми угрозами информационной безопасности, приоритетные направления, содержание и формы такого сотрудничества. В ходе исследования угроз информационной безопасности в кризисах и конфликтах XXI века авторами применялся широкий спектр научных методов. Публикация предназначена для представителей российского политического и экспертного сообщества, преподавателей ВУЗов, аспирантов и студентов, СМИ, а также для широкого круга читателей, интересующихся мировой политикой и проблемами безопасности.

Informational Security Threats in Crises and Conflicts of XXI Century / A.V. Zagorskii, N.P. Romashkina, eds. – Moscow, IMEMO, 2015. – 151 p.
ISBN 978-5-9535-0450-8

Analysis of threats in informational sector of current international relationships system is presented in the publication. These threats are expressed in application of different informational influence methods and new concepts of opposition with usage of informational and tele-communicational tools. Examples of informational and psychological opposition and their political consequences in periods of Georgian- Ossetic conflict in 2008 and Ukrainian crisis in 2013–2015 as well as cyber action methods on critically important infrastructures in conflict regions of the world are investigated in the study. Domestic activity of Russia on ensuring informational security in XXI century and role of Russian Federation in international structures of multilateral interaction in fight against new threats of informational security along with priority directions, content and form of this interaction are analyzed. Wide range of scientific methods was used during analysis of informational security threats in crises and conflicts of XXI century. Publication is recommended for representatives of Russian political and expert community, university instructors, undergraduate and graduate students, media and wide range of readers interest in international politics and security problems.

Публикации ИМЭМО РАН размещаются на сайте http://www.imemo.ru

ISBN 978-5-9535-0450-8

© ИМЭМО РАН, 2015

Оглавление

Обращение к читателям……...5

Сокращения……9

Введение…… 10

Глава 1. Современные угрозы информационной безопасности: от практики к теории. *Ромашкина Н.П.* 16

Глава 2. Информационный фактор вооруженной борьбы: от исторических истоков к новым методам противоборства в XXI веке. *Ковалев В.И.* 26

Глава 3. Примеры информационно-технических методов противоборства XXI века 36

3.1. Кибервойна против ядерной программы Ирана. *Ромашкина Н.П.* .. .38

3.2. Индийский опыт противодействия угрозам в кибернетическом пространстве. *Топычканов П.В.* . . . . .

Обращения к читателям

Уважаемые читатели!

Россия является автором идеи создания режима обеспечения международной информационной безопасности и инициатором международного обсуждения проблем в информационной сфере на официальном уровне в рамках ООН. Еще в 1998 году в письме Генеральному секретарю ООН с российской стороны акцентировалась необходимость учитывать потенциальную на тот период опасность использования достижений в информационной сфере в целях, не совместимых с задачами обеспечения стратегической стабильности, принципов неприменения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека. Сегодня такая опасность стала очевидной и требует принятия безотлагательных мер. К сожалению, процесс формирования такого режима идет значительно медленнее нарастания угроз. Все более опасные информационные операции требуют постоянного мониторинга, глубокого анализа и активного международного сотрудничества.

Работа в рамках ООН по обсуждению проблем международной информационной безопасности в течение нескольких лет содействовала продвижению российских взглядов на эти вопросы. Выдвигаемые Россией политические резолюции под общим названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» получали консенсусное одобрение в ходе голосований на Генеральной Ассамблее ООН и все большее число соавторов. Это стало возможным в силу растущего понимания реальности угроз использования современных информационно-коммуникационных технологий в целях подрыва мира, политической и экономической стабильности, вмешательства во внутренние дела государств, разжигания межнациональной и межконфессиональной вражды. Безусловно, для российской стороны приоритетом остаются вопросы мира и безопасности. Нельзя допустить, чтобы кибероружие можно было бы использовать проще и легче, чем любое другое оружие. Именно вопросам обеспечения международной информационной безопасности в условиях глобальных вызовов в области информационных технологий было посвящено недавно состоявшееся специальное заседание коллегии МИД России. Особое значение сейчас приобретает выработка универсальных правил ответственного поведения государств в информационном пространстве, закрепляющих принципы уважения государственного суверенитета, невмешательства во внутренние дела других государств, основных прав и свобод человека, а также равные права для всех государств на участие в управлении сетью «Интернет».

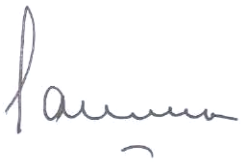
Стремлением сделать еще один шаг в разработке проблем информационной безопасности продиктовано издание настоящей монографии. Она подготовлена коллективом экспертов авторитетных научных учреждений. В ней предпринята попытка охарактеризовать основные угрозы проблемы и дать необходимые сведения, в том числе справочного характера.

Публикация могла бы оказать помощь государственным деятелям и общественности в понимании основных аспектов проблемы информационной безопасности, как в национальном, так и в международном ее измерениях, а также в осознании тех конкретных опасностей, которые возникают при использовании достижений в информационной сфере в качестве оружия.

Кроме того, это издание могло бы служить источником информации по проблеме обеспечения международной информационной безопасности и отдельным ее аспектам для политиков, дипломатов, военных, научных работников и представителей бизнеса, государственных и общественных организаций, а также студентов и аспирантов.

С удовольствием рекомендую эту публикацию и выражаю надежду, что исследовательская работа российских специалистов поможет читателям лучше осознать угрозы, которые несет с собой применение современных информационных технологий в политических, военных, криминальных, террористических и всех других противоправных целях.

Специальный координатор МИД России по вопросам политического использования информационно-коммуникационных технологий,
кандидат исторических наук



Лапшин В.А.

Уважаемые читатели!

С большим удовольствием рекомендую вам монографию российских ученых «Угрозы информационной безопасности в кризисах и конфликтах XXI века».

Со времен Клаузевица было принято считать, что война – это продолжение политики иными, насильственными средствами. Сегодня все чаще встает вопрос о том, можно ли в полной мере использовать такое понимание войны в 21 веке. Очевидно, что далеко не все противоречия в мире удается разрешать политическим путем, и применение вооруженного насилия в различных формах продолжается и в новом столетии. По-прежнему нет гарантии того, что многочисленные локальные войны и конфликты не перерастут в более крупные вооруженные столкновения, в том числе с применением ядерных вооружений. Как и прежде, мир переполнен различными социально-политическими, экономическими, межэтническими, религиозными и другими противоречиями. Разворачивается соперничество мировых держав за энергетические и, прежде всего, нефтяные и газовые ресурсы. Однако все большую роль играют новые угрозы международной безопасности и национальной безопасности государств. Среди них, безусловно, неправомерное использование информационных технологий.

Можно ли считать эти, так называемые, нетрадиционные методы исключительно новыми инструментами межгосударственного противоборства? Безусловно, нет. Всегда и везде войны велись не только боевыми средствами, но и путем хитрости, обмана и дезинформации. Еще 10 веков назад Древняя Византия выигрывала многие войны, используя военные операции только как вспомогательное средство или как угрозу. А основным оружием при этом было то, которое сегодня принято называть нетрадиционным. Политико-дипломатические и информационные возможности использовались и будут использоваться в борьбе между государствами. Поэтому делить войны на традиционные и нетрадиционные просто невозможно. Но в настоящее время роль и значение невоенных методов противостояния существенно возросло. Все сферы деятельности общества сегодня испытывают на себе вредоносное воздействие информационно-психологических и кибертехнологий.

Россия относит неправомерное использование информационных технологий к угрозам своей национальной безопасности. И это отражено в новой редакции военной доктрины, в которой дан анализ военно-политической обстановки в мире. В последние годы наблюдается череда «цветных революций», гражданская война на Украине, активизация террористической деятельности, «расцвет» «Исламского государства» и многое другое, что заставляет мировое сообщество жить в тревоге. И все эти процессы развиваются в условиях стремительно возрастающего влияния информационно-коммуникационных средств.

Сегодня существует два пути. Можно отмахнуться от нарастающих угроз в информационной сфере и рассматривать их в качестве обычного естественного процесса. Тогда не понадобится их детальный многосторонний анализ. Но от нашего непризнания, осуждения или непонимания тех или иных явлений, они не перестают существовать. И для того, чтобы правильно на них реагировать, надо знать их подлинную сущность. В связи с этим необходимо выбрать второй путь – поиск и разработка ответов на современные информационные вызовы. И в этом случае профессиональное исследование и оценка таких угроз со стороны научного сообщества неизбежны, обязательны и крайне важны.

Именно к таким исследованиям относится предлагаемая вниманию читателей публикация, представляющая собой оригинальную работу как по существу рассматриваемой проблемы, так и по избранному авторами профессиональному методологическому подходу. Монография, действительно, отражает современный уровень политического анализа. Возможно, какие-то главы могут показаться слишком сложными и непривычно

изложенными, но если мы хотим на равных разговаривать с членами международного научного сообщества, придется приложить известные усилия.

Хотел бы поблагодарить авторов за добросовестную и архиактуальную работу. Как военный специалист по стратегическому планированию с многолетним стажем и как президент Академии военных наук вижу большую практическую ценность исследования не только в анализе угроз информационной безопасности в 21 веке, построенном на интереснейшем факторном материале, но и в самой постановке исключительно важной для современной России проблемы, требующей безотлагательного решения. А также в использовании междисциплинарных методов ее изучения, что само по себе уже определяет новизну и своеобразие, и являются стимулом для реальных практических действий и новых научных исследований.

Публикация окажет помощь специалистам, чья деятельность непосредственно связана с проблемой обеспечения информационной безопасности, и в первую очередь, новому поколению политиков, ученых, военных и гражданских экспертов, представителей оборонно-промышленного комплекса. Она будет интересна и более широкому кругу читателей – всем, кто, располагая достаточными знаниями, занимается вопросами безопасности и стабильности в России и за рубежом.

Президент Академии военных наук,
лауреат Государственной премии им. Г.К. Жукова,
доктор военных наук, доктор исторических наук, профессор,
генерал армии



Гареев М.А.

Сокращения

АПЛ – атомная подводная лодка
АСЕАН – Ассоциация государств Юго-Восточной Азии (англ. Association of SouthEast Asian Nations)
АЭС – атомная электростанция
БПЛА – беспилотный летательный аппарат
БРИКС – группа из пяти стран: Бразилия, Россия, Индия, Китай, Южно-Африканская Республика, глобальный форум партнерского диалога и сотрудничества
ВП – вредоносная программа
ВС – вооруженные силы
ВВС – военно-воздушные силы
ИБ – информационная безопасность
ИКТ – информационно-коммуникационные технологии
ИО – информационное оружие
ИП – информационное пространство
ИПВ – информационно-психологическое воздействие
КБ – кибернетическая безопасность
КНШ – Объединённый комитет начальников штабов США
КП – кибернетическое пространство
КС – компьютерная сеть
ЛК – Лаборатория Касперского
МАГАТЭ – Международное агентство по атомной энергии
МИБ – международная информационная безопасность
МИД – министерство иностранных дел
МО – министерство обороны
ОДКБ – Организация Договора о коллективной безопасности
ОМУ – оружие массового уничтожения
ПК – персональный компьютер
ПО – программное обеспечение
СМИ – средства массовой информации
СНГ – Содружество независимых государств
ШОС – Шанхайская организация сотрудничества

Введение

К концу XX века процесс стремительного развития и внедрения новых информационных технологий, получивший название «информационная революция», стал естественным этапом экономического и научно-технического прогресса, необходимым условием дальнейшего развития общества. Закономерно с такой же интенсивностью нарастают случаи применения информационных средств в деструктивных целях: направленные против отдельных, лиц, групп и, наконец, против структур управления государством, экономикой и вооруженными силами. В результате меняются понятия конфликта, войны и оружия, а также грань между войной и миром, сращиваются военные и мирные технологии. У нападающей стороны появляется реальная возможность нанести разрушительный ущерб противнику без проникновения на его территорию, одержать победу без собственных потерь.

Россия стала инициатором международного обсуждения возникших проблем в информационной сфере. Однако этот процесс идет значительно медленнее нарастания угроз. Все новые вредоносные и опасные информационные операции требуют постоянного мониторинга и глубокого разностороннего анализа в целях обеспечения как национальной безопасности России, так и международной безопасности.

Поэтому общей целью этой публикации является исследование на междисциплинарном уровне проблем обеспечения безопасности национальных интересов России в глобальном информационном пространстве на основе анализа угроз и практических примеров нарушения информационной безопасности в кризисах и конфликтах XXI века.

Какие из описанных в предложенной читателю публикации опасностей угрожают или могут в будущем угрожать России? Какие из угроз представляют наибольшую опасность? В какой сфере Россия более уязвима для подобных методов информационного противоборства? В какой области уже существуют достаточная научная, законодательная, техническая и другие основы для противодействия подобным угрозам, а какие меры необходимо выработать как можно скорее? Какие выводы из этого анализа нужно сделать сегодня с целью обеспечения информационной безопасности России завтра?

Обоснование необходимости дальнейшего научного поиска ответов на эти и другие вопросы является основной задачей авторов этой работы.

В первой главе публикации проводится факторный анализ различных методов информационного воздействия, применяемых в кризисах и конфликтах конца прошлого – начала нынешнего века. Кроме того, к работе прилагается обширная подборка осуществленных с начала XXI века примеров кибератак в разных регионах мира на различные информационные носители, начиная с домашних персональных компьютеров и заканчивая целевыми атаками на крупные информационные агентства, банковские и бизнес-структуры, разведывательные, государственные и правительственные ведомства, международные организации и промышленные критически важные объекты. Все эти данные доказывают всеобъемлющий масштаб современных угроз информационной безопасности.

Столь глобальные темпы развития и распространения вредоносного информационного воздействия в современной обстановке информационной революции обусловили отставание теории (научной, интеллектуально-политической и нормативно-правовой) от практики. С этим связано и недостаточное развитие соответствующих международных механизмов контроля над разрушительными информационными технологиями: разработка, производство, распространение и применение информационных технологий в военных целях не регулируются международным правом. Такое положение вещей на современном этапе пока не позволяет говорить о возможности применения хорошо разработанной теории к практике. В Российской Федерации теоретическая основа в данной области формируется на прецедентной основе: от практики к теории. Поэтому сегодня

существует необходимость постоянного мониторинга и детального разностороннего анализа практических примеров нарушения информационной безопасности для создания базовой теории, ее применения на практике и дальнейшего усовершенствования.

При этом анализ уже существующей теоретической базы, разработанных понятий, которыми пользуются отдельные государства, является важной научной задачей. В рамках ее решения проводится исследование причин возникновения и развития базовых терминов и их определений в сфере информационной безопасности.

Первые практические и теоретические разработки в политико-информационной сфере проведены в Соединенных Штатах Америки. В 1992 году в США были сформулированы основы стратегии информационного противоборства, проанализированные и дополненные специалистами из Корпорации RAND.[1] До настоящего времени США являются общепризнанным лидером по созданию технологий информационного противоборства и противодействия таковым. Кроме того, заметное повышение интереса политиков и экспертов к проблематике информационной безопасности в последние годы во многом связано с тем, что в Соединённых Штатах на высшем уровне было принято множество директив и официальных документов, регламентирующих политическую и военную деятельность в информационном пространстве. Среди них «Доктрина борьбы с системами управления» Объединенного комитета начальников штабов (КНШ) США, «Объединенная доктрина информационных операций» МО США, «Обзор кибернетической политики», «Международная стратегия по киберпространству», «Стратегия Министерства обороны по действиям в киберпространстве 2011», доктрина КНШ США «Информационные операции» 2014 года и др. Анализу причин возникновения и дальнейшего развития в официальных документах США понятий и концепций «информационной войны», «информационной операции», «информационного оружия», «стратегического информационного противоборства», «сетецентрической войны» и др. уделяется внимание в нескольких статьях публикации.

Сделанные выводы необходимы для усовершенствования российской понятийно-теоретической базы в сфере информационной безопасности, ее научного и нормативного развития.

Хотя понятийно-теоретический аппарат информационной безопасности только формируется в большинстве стран мира, идея информационной составляющей стратегического ведения войны не является новой. На самом деле, достаточно сложно найти какой-либо конфликт, в котором бы не присутствовал информационный аспект. Еще китайский основатель мировой стратегической теории Сунь-Цзы рекомендовал использовать информацию для достижения стратегических целей, избегая при этом вооруженных столкновений. Существует множество исторических примеров, в которых изменения в технологической сфере повлекли фундаментальные изменения в характере информационной составляющей войны. В главе 2 этой публикации приводится один из примеров использования психологических методов в ходе Второй мировой войны, объясняющий, каким образом эти и другие технологии прошлого века стали базой для концепций

[1] DoD Directive TS-3600.1, "Information Warfare," December 21, 1992.
(http://www.dtic.mil/whs/directives/corres/pdf/300003p.pdf).
Molander, Roger C. Strategic information warfare: a new face of war / Roger C. Molander, Andrew S. Riddile, Peter A. Wilson. Library of Congress Cataloging in Publication Data, RAND (Firm). 1996.
(http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf).
Molander, Roger C. Strategic information warfare rising war / Roger C. Molander, Peter A. Wilson, B. David Mussington, Richard Mesic. Library of Congress Cataloging in Publication Data, RAND (Firm). 1998.
(http://www.rand.org/content/dam/rand/pubs/monograph_reports/2009/MR964.pdf).

современных информационных войн, постоянно развивающихся и совершенствующихся в развитых странах мира.

Примерам применения методов противоборства XXI века, которые по направленности воздействия можно разделить на два основных вида: информационно-технические и информационно-психологические, посвящены третья и четвертая главы монографии.

В третьей главе в качестве одного из самых показательных, но не достаточно изученных и описанных примеров применения вредоносных методов в информационно-технической сфере представлена проблема кибератак на критически важные объекты атомной инфраструктуры Ирана в 2010-2012 годах. Кибервоздействия на несколько ядерных предприятий ИРИ, наиболее значимыми из которых были кибернападения на атомную станцию в г. Бушер и завод по обогащению урана в г. Натанз, по мнению специалистов, впервые могут рассматриваться не просто как киберпреступление, а как кибервойна с применением полноценного кибероружия. Эти прецеденты стали достоянием общественности и привели к важным последствиям, повлиявшим на дальнейший ход событий вокруг иранской ядерной проблемы. Кибертехнологии в этой войне дополняли и, возможно, не уступали по силе воздействия не только политическим и экономическим санкциям, но и военным мерам. Совершенно очевидно, что для России по целому ряду причин в целях прогнозирования будущих возможных угроз исключительно важен глубокий междисциплинарный анализ такого рода примеров. В частности, это необходимо еще и потому, что подобное комплексное кибервоздействие может быть нацелено на критически важные государственные объекты военного назначения, что также грозит серьезными разрушительными последствиями.

В качестве примера противодействия государства современным киберугрозам был выбран опыт Индии. Его изучение важно по ряду причин. Во-первых, находясь в сложных отношениях с Пакистаном и Китаем, Индия является одной из тех стран, против которых наиболее часто предпринимаются атаки в киберпространстве. Во-вторых, Индия наращивает наступательные и оборонительные киберсредства, располагая одним из наиболее развитых в Азии сектором информационных технологий. В-третьих, Индия является одним из государств, которые активно выступают на мировой арене за выработку международных норм в области информационных технологий. В-четвертых, Индия выступает «стратегическим партнером» Российской Федерации, однако вопросы информационной безопасности занимают все еще недостаточно адекватное место в повестке двусторонних отношений. Изучение индийского опыта поможет России не только расширить знание о возможных киберугрозах и способах реагирования на них, но и найти «точки соприкосновения» в подходах Индии и России к обеспечению безопасной информационной среды, чтобы более эффективно отстаивать интересы двух стран на международном уровне. Превращение информационной безопасности в одну из обязательных тем стратегического диалога между Москвой и Дели поможет адаптировать «стратегическое партнерство» к реалиям современного мира.

Задача исследования проблем обеспечения информационно-психологической безопасности личности и общества указана в качестве одной из приоритетных для научных исследований в области обеспечения информационной безопасности Российской Федерации во многих официальных документах Российской Федерации, в том числе, в материалах научного совета при Совете Безопасности РФ. Это обосновано тем, что в настоящее время информационно-психологические операции, осуществляемые насильственными средствами воздействия на соответствующую сферу противника с целью решения стратегических задач нападающего, представляет собой наиболее социально опасную форму противоборства. Политико-психологическое воздействие одних государств на другие, зародившееся еще на ранней стадии человеческой истории в виде отдельных разрозненных операций по дезинформированию противника, в процессе развития претерпело существенные изменения

и превратилось в постоянно действующий фактор внешней политики – подрывную информационно-психологическую деятельность, которая ведется не только в боевой, но и в мирной фазе кризисов и конфликтов. Этот новый вид противоборства стал в конце XX и в наступившем XXI веке превалирующим в политике многих государств. В связи с этим четвертая глава публикации посвящена современным методам информационно-психологического противоборства, а также решению задачи мониторинга информационной безопасности в интересах Российской Федерации, объединяющей все части публикации. В качестве наиболее важных для интересов России примеров применения вредоносного информационно-психологического воздействия, выбраны грузино-южноосетинский конфликт 2008 года и кризис на Украине 2013-2015 годов. Охватывая лишь некоторые аспекты проблемы, авторы обращают внимание на необходимость дальнейшего разностороннего исследования проблем защиты индивидуального, группового и массового сознания российского общества от деструктивных воздействий средств массовой информации, интернета и других информационных источников, обозначенных в качестве значимых в официальных документах РФ.

Информационно-психологическая операция в ходе грузино-южноосетинского конфликта началась задолго до событий 8 августа 2008 года. Этому предшествовала большая подготовительная работа со стороны Грузии и стран Запада. В качестве примеров можно рассматривать шпионский скандал против двух российских военнослужащих (сентябрь – октябрь 2006 года), обвинение России в международной агрессии и бомбардировке грузинской территории (март – апрель 2008 года), заблаговременную подготовку медиаплощадок для зарубежных журналистов в г. Гори и сформированное на Западе общественное мнение об агрессивности России. В период вооруженного конфликта это создало для грузинского руководства существенные преимущества в информационном противоборстве, что стало для России серьезным уроком.

Дальнейшее развитие событий продемонстрировало использование на практике широкого арсенала различных информационных методов: от «наклеивания ярлыков», публичной интерпретации, гиперболизации и подмены видеоряда до дезинформации и клеветы. Даже в таких условиях Россия смогла сформировать объективное общественное мнение внутри страны. Но этого не удалось сделать в рамках глобального медиапространства, где позиция Российской Федерации целенаправленно заглушалась и не получала должного распространения, что стало важным уроком информационной борьбы.

В качестве других уроков следует отметить необходимость более тесного сотрудничества не только с отечественными, но и с зарубежными журналистами, целесообразность формирования благоприятного имиджа страны для западной аудитории, завоевания места в рамках глобальной медиа-политической системы, улучшения работы отечественной журналистики за рубежом. Очень многое зависит также от эффективности деятельности законодательных и исполнительных органов власти. Исходя из этого опыта, в России идет формирование системы обеспечения информационной безопасности. Однако есть еще немало проблем.

Методы информационного противоборства, применявшиеся в ходе грузино-южноосетинского конфликта, вновь приобрели актуальность в период трагических событий на Украине в 2013-2015 годах. Насколько полезными оказались уроки 2008 года для России в ходе украинского кризиса, еще предстоит исследовать в будущем. Однако проводить сравнительный анализ тех методов, которые применялись в обоих случаях, необходимо уже сейчас. Выводы о том, какие ошибки были исправлены, а какие еще требуют дальнейших усилий, можно сделать на основе представленного в четвертой главе анализа, сравнивая информационно-психологические технологии, применявшиеся в Грузии и на Украине. Однако необходимо учитывать, что уроки были извлечены не только Россий, но и субъектами, осуществлявшими разрушающее информационное воздействие. Подчиняясь

единой логике, информационно-психологические операции разрабатываются нападающей стороной для каждого конкретного случая с учетом предыдущего опыта. Так, специалисты выделяют новые методики информационно-психологического воздействия в ходе украинского кризиса. При этом их эффективность повышается за счет более масштабного комплексного применения экономических, технических, военных и политических механизмов.

Современные события на Украине дестабилизируют международные отношения, угрожают безопасности России и Европы, негативно влияют на ситуацию внутри нашего государства, не отвечают интересам российских граждан. Кроме того, Совет Безопасности РФ отмечает: «Все более широкое распространение для устранения неугодных США политических режимов приобретут усовершенствованные технологии «цветных революций» с высокой вероятностью применения их в отношении России».[2] Следовательно, необходимо вести постоянную работу по стабилизации ситуации в интересах Российской Федерации на всех уровнях, в том числе, на уровне исследований на базе государственных научных организаций и институтов. Поэтому важное место в публикации занимает раздел, посвященный анализу информационно-психологического воздействия в период кризиса на Украине 2013-2015 годов.

Исходя из насущной необходимости разработки средств противодействия современным информационным угрозам и технологий их предотвращения, особое значение приобретает проблема научного планирования и прогнозирования в сфере информационно-коммуникационных технологий, что не достижимо в рамках только одного научного направления и только одной науки. Решение этой задачи в интересах безопасности России требует отдельных исследований. Приведенные в публикации примеры применения широкого спектра научных методов: различных видов анализа (от факторного и контент-анализа до статистического и системного), элементов математического моделирования политических процессов и др. призваны проиллюстрировать возможности такого мультидисциплинарного подхода.

Так, во второй главе монографии приводится пример применения некоторых компонентов метода математического моделирования к изучению информационно-психологических параметров войны. А в четвертой главе для исследования информационно-психологического воздействия в период кризиса на Украине применяется метод содержательного контент-анализа, который позволяет не только сделать важные выводы, но и научно подтвердить предположения и гипотезы относительно эффективности применения методов ИПВ.

В ходе контент-анализа исследованы СМИ:

- Украины, как основного субъекта кризиса,
- России, как государства, для которого кризис является угрозой национальной безопасности,
- Соединенных Штатов Америки, как государства, заинтересованного в своем влиянии на постсоветском пространстве,
- Великобритании, как главного союзника Соединенных Штатов в Европе и одного из лидеров Евросоюза, ассоциация с которым явилась лозунгом протестного движения на Майдане в ходе эскалации кризиса на Украине,
- Казахстана – союзника России и государства, для которого подобные методы информационного воздействия также могут представлять угрозу в будущем.

Список заинтересованных стран и их СМИ, безусловно, может быть расширен. Однако данный пример применения этого научного метода для анализа информационно-

[2]О Стратегии национальной безопасности США. 25.03.2015. Сайт Совет Безопасности Российской Федерации. (http://www.scrf.gov.ru/news/865.html).

психологического воздействия на граждан разных стран может стать основой для дальнейших исследований.

Пятая глава публикации посвящена решению задач использования механизмов международного сотрудничества для предотвращения развязывания гонки вооружений в области информационного противоборства и формирования системы международной информационной безопасности. В документах Совета Безопасности РФ эти задачи выделены в качестве приоритетных.

Став инициатором обсуждения проблем обеспечения международной информационной безопасности на уровне ООН, Россия последовательно выступает за демилитаризацию международного информационного пространства, за необходимость доработки и адаптации механизмов международного права применительно к информационно-коммуникационным технологиям, подчеркивая, что гонка информационных вооружений способна дестабилизировать сложившиеся договоренности о разоружении и международной безопасности и в других сферах. Формирование соответствующей теоретической базы и разработка практических мер по обеспечению безопасности информационной среды являются насущными и неотложными задачами современности, непременным условием разработки международных политико-правовых механизмов глобального управления и регулирования в данной области.

Глава 1. Современные угрозы информационной безопасности: от практики к теории

Информационное воздействие на практике

Уже в древности воздействие на психологию противника считалось зачастую более важным, чем его физическое уничтожение. Два тысячелетия назад великий китайский стратег Сунь-Цзы писал: «Война – это путь обмана. Поэтому, даже если [ты] способен, показывай противнику свою неспособность. Когда должен ввести в бой свои силы, притворись бездеятельным. Когда [цель] близко, показывай, будто она далеко; когда же она действительно далеко, создавай впечатление, что она близко».[3]

Современная глобальная информационная революция предоставила для такой деятельности поистине безграничные возможности. Информационно-коммуникационные технологии (ИКТ) становятся ключевым фактором мировой политики, экономики и систем безопасности. Информационное оружие (ИО) превращается во все более важный элемент военного потенциала государств, дополняющий обычные военные средства. Информационные диверсии в киберпространстве стали новым орудием негосударственных коллективных и индивидуальных субъектов. А кибервойны одних государств против других могут оказаться не менее разрушительными и жестокими, чем традиционные.

ИКТ в ходе боевых действий, включая длительный этап информационно-психологического давления и комплексное применение средств разведки, управления, связи, навигации и радиоэлектронной борьбы, были впервые использованы Соединенными Штатами Америки в операции «Буря в пустыне» в 1991 году в Ираке. После этого информационное воздействие (и блокада) в нарастающем масштабе применялось в операциях в Югославии (1999 год), Афганистане (2001 год), Ираке (2003 год), Ливии (2011 год).

Деструктивное информационно-психологическое воздействие с достаточно высокой эффективностью велось западными странами в ходе грузино-южноосетинского конфликта 2008 года. В настоящее время мы наблюдаем применение практически всего спектра современных методов информационного воздействия в ходе кризиса на Украине и в Сирии.

В XXI веке во всем мире отмечается рост количества успешных атак на информационные ресурсы не только персональных компьютеров граждан и организаций, но и государственных ведомств и объектов критически важной инфраструктуры, которые превращаются в инструмент политического и экономического давления.

Примеры кибератак, зафиксированных во всех регионах мира, на различные информационные носители: от домашних персональных компьютеров до целевых атак на крупные информационные агентства, банковские и бизнес-структуры, разведывательные, государственные и правительственные ведомства, международные организации, и, наконец, крупные промышленные объекты критически важных инфраструктур, осуществленных с начала XXI века (см. Приложение А), доказывают глобальный уровень угрозы, демонстрируют ускоренные темпы расширения масштабов, географии и списка объектов кибернападений.

Один из первых примеров воздействия на информационно-управляющие системы критически важных инфраструктур – применение в 2010-2012 годах компьютерных вредоносных программ (ВП) *Stuxnet, Duqu, Flame* и *Wiper*, нацеленных на причинение физического ущерба иранскому заводу по обогащению урана в г. Натанз и АЭС в г. Бушер и на торможение ядерной программы Ирана. Одной из вероятных причин повреждений (о

[3] Сунь-Цзы. Искусство войны. (http://militera.lib.ru/science/sun-tszy/01.html).

котором только спустя несколько месяцев сообщили официальные представители ИРИ) является *одновременный ввод в резонансную частоту большого количества центрифуг* из-за воздействия ВП *Stuxnet*. Причем эксперты пришли к заключению, что программа создана при поддержке государственных структур командой чрезвычайно квалифицированных профессионалов, обладающих обширными ресурсами и существенной финансовой поддержкой. Поэтому имел место не случай киберпреступности, а акт кибервойны. В 2013 году генеральный директор российской компании «Лаборатория Касперского» Е. Касперский сообщил о заражении программой *Stuxnet* компьютерной сети ядерных объектов не только Ирана, но и России.[4]

Еще один подобный инцидент произошел в 2013 году в энергетической сфере и связан с вредоносной программой *Shamoon* – вирусом, который заразил почти 30 тысяч компьютеров в сети нефтяного производителя Саудовской Аравии Aramco. По мнению специалистов, нефтегазовые компании стран Персидского Залива очень уязвимы для кибератак из-за высокой вероятности проникновения вредоносных технологий в инфраструктуру критических процессов. Эксперты полагают, что *Shamoon* был разработан в Иране для поражения энергетической промышленности. Отметим, что случай с саудовской компанией Aramco – не единственный, компания RasGas Company Limited – крупнейший поставщик сжиженного газа также подвергалась кибернападению хакеров в Катаре и ОАЭ.

Один из последних примеров кибервоздействия является вредоносная троянская программа *Duqu 2.0*, зафиксированная в 2014 году и активная до настоящего времени. Это чрезвычайно сложное программное обеспечение, на целое поколение опережающее все известные угрозы. Вредоносным заражениям от него подверглись, в частности, площадки мероприятий «Группы 5+1» по решению иранской ядерной проблемы, в рамках которых проходили встречи мировых лидеров. В 2015 году киберподразделение запрещённой в России террористической группировки «Исламское государство» (ИГ) сумело получить доступ к личным данным около 1400 американских военнослужащих с дальнейшим призывом организовывать нападения на них. Среди опубликованных данных: управления и подразделения за которыми закреплены военнослужащие, адреса электронной почты, почтовые коды и телефонные номера и другие данные.

В настоящее время угрозу от вредоносного кибервоздействия можно оценивать как глобальную.

Таким образом, глобальное информационное пространство становится в XXI веке важнейшей ареной противоборства.

В связи с этим в настоящее время уже в полной мере встает проблема обеспечения информационной безопасности как важнейшего компонента национальной и международной безопасности. Разнообразные проекты национальных концепций информационной безопасности, появившиеся еще в конце прошлого века, обнаружили отсутствие на международном уровне единого понятийного аппарата и общепринятой методологии оценки угроз, а порой и несоответствие их вариантов существующим нормативно-законодательным базам на национальном и международном уровнях. Формирование соответствующей интеллектуально-политической базы является насущной задачей и непременным условием разработки международных политико-правовых норм и механизмов глобального управления и регулирования в данной области.

Теория информационной безопасности: базовые понятия и определения

Термины «информационная война», «информационное противоборство», «информационное воздействие», «информационное оружие» и т.д. часто используются в

[4] «Первое кибероружие» поразило ядерный объект в России. Касперский раскрыл информацию о заражении российской атомной станции вирусом Stuxnet. (http://nuclearno.ru/text.asp?17591).

СМИ, публицистических и научных трудах, национальных документах ряда стран, однако до настоящего времени общепринятые на международном уровне определения этих понятий не закреплены. Работа по юридическому оформлению этих и связанных с ними понятий на международном уровне идет в настоящее время, но это трудный и осложненный многими противоречиями процесс. Поэтому очень важно исследовать, когда они появились и как развивались в национальных государственных документах. Спектр понятий, связанных с проблемой обеспечения информационной безопасности, очень широк, поэтому рассмотрим только те из них, которые наиболее значимы для данной работы.

Особое место в исследованиях современных проблем информационной безопасности занимает термин ***«информационная война»***. Впервые он был употреблен в Соединенных Штатах Америки научным советником Министерства обороны Томасом Рона в отчете «Системы оружия и информационной войны», подготовленным для компании «Боинг» в 1976 году[5], где отмечалось, что информационная инфраструктура становится ключевым компонентом экономики США и в то же время уязвимой целью в военное и мирное время. Официально он появился в директиве министра обороны США «Информационное противоборство» ("Information Warfare") от 21 декабря 1992 года.[6] Таким образом, Соединенные Штаты первыми в мире официально сформулировали основы стратегии информационного противоборства сразу после завершения войны в Персидском заливе (1991 год), в которой американские вооруженные силы также первыми применили новейшие информационные технологии.

В августе 1995 году Национальный университет обороны США опубликовал статью «Что такое информационная война?» одного из крупнейших американских ученых в информационной сфере, специалиста Корпорации RAND профессора Мартина Либицки, чья научная деятельность заложила основу соответствующих концепций и стратегий ВС США, положений Министерства юстиции США и до настоящего времени связана с проблемами применения ИКТ в системе национальной безопасности.[7] Автор разработал одну из первых классификаций составных частей информационной войны XXI века и рассмотрел ее как мозаику из семи различных элементов.[8]

1. ***Война в сфере контроля и управления*** ведется на реальном поле боя, не являясь при этом чем-то новым для ВС США. Она нацелена на каналы связи между командованием и исполнителями. Перерезая эти каналы, нападающий стремится добиться нарушения систем управления войсками, линий коммуникаций и системы управления противника в целом на стратегическом, оперативном или тактическом уровнях. Таким образом, атакующая сторона изолирует командование от исполнителей.
2. ***Разведывательная война*** – сбор важной в военном отношении информации и защита собственной – благодаря развитию информационных технологий, позволяет получить дополнительные знания о противнике.
3. ***Электронная война*** предполагает действия против средств электронных коммуникаций: радиосвязи, радаров, компьютерных сетей и т.д. Ее важным элементом является криптография.
4. ***Психологическая война*** – использование информационных возможностей и ресурсов против человеческого сознания (выделяют четыре формы ее ведения: культурный конфликт, операции против национальной идеи, военного руководства и

[5] Thomas P. Rona. Weapon Systems and Information War, the Official Home of the Department of Defense. (http://www.dod.gov/pubs/foi/reading_room/09-F-0070WeaponSystems_and_Information_War.pdf).
[6] DoD Directive TS-3600.1, "Information Warfare", December 21, 1992. (http://www.dtic.mil/whs/directives/corres/pdf/300003p.pdf).
[7] Одна из последних работ М. Липицки «Кризисы и их эскалация в киберпространстве» (Crisis and Escalation in Cyberspace) вышла в Корпорации RAND в 2012 г.
[8] Martin C. Libicki. What is Information Warfare? United States Government Printing, Washington DC, 1995. (http://www.dodccrp.org/files/Libicki_What_Is.pdf).

войск противника). В качестве важного средства ее ведения М. Либицки рассматривает СМИ.

5. Основное средство поражения в «***хакерской» войне*** – компьютерные ВП (в том числе вирусы), объект воздействия – компьютерные сети (КС). Их нарушение может происходить в мирное и военное время, как в отношении военных, так и государственных и частных КС и информационных ресурсов. С военной точки зрения в зависимости от целей и объектов операции могут быть оборонительными и наступательными.

6. ***Экономическая информационная война*** направлена на коммерческую информацию и может принимать одну из двух основных форм – информационную блокаду и информационный империализм.[9] Она строится на предположении, что в будущем государства будут зависеть от информационных потоков так же, как сегодня они зависят от материального обеспечения и обмена.

7. ***Кибервойну*** М. Либицки назвал информационной войной будущего и полагал, что рассуждать о ней преждевременно. Однако, как говорилось выше, уже сегодня некоторые компьютерные атаки, например, с применением ВП на ядерных объектах Ирана в 2010-2012 годах., классифицируются специалистами именно как кибервойна.

Уже в этой работе, вышедшей 20 лет назад, отмечается: хотя информационно-психологические операции применялись в военных действиях с древних времен, однако и в войнах XXI века как технические, так и психологические информационные методы имеют равную и очень большую значимость, особенно в комплексе. Автор теории информационного противоборства указывает, что успешно вести информационную войну невозможно без точных и надежных специфических знаний о противной стороне: начиная с анализа ее СМИ и оценки их влияния на государственные решения до детального изучения бюрократической структуры руководства страны, национальной коммуникационной инфраструктуры, особенностей программного обеспечения систем и т.д. Поэтому исключительное значение приобретает особый процесс подготовки профессионалов, задействованных на разных этапах современных информационных операций. При этом их главной целью должно стать достижение своих государственных интересов, а не подавление противника.

На основе этого и других исследований разрабатывались новые доктрины Соединенных Штатов. В феврале 1996 года Объединенный комитет начальников штабов (КНШ) ввел в действие «Доктрину борьбы с системами управления»[10], а в октябре 1998 года МО США – «Объединенную доктрину информационных операций», в которой разъяснялись два базовых понятия:

информационная война *(information warfare) – комплексное воздействие (совокупность информационных операций), оказываемое во время кризиса или конфликта на определенного противника или нескольких противников для решения поставленных задач;*

информационная операция *(information operation) – действия, предпринимаемые с целью затруднения сбора, обработки, передачи и хранения информации системами противника при защите собственной информации и информационных систем*.[11]

В руководящих документах НАТО, принятых в 1999 году, ***информационная операция*** определяется как *действия, предпринимаемые с целью оказания влияния на принятие решений путем воздействия на информацию, информационные процессы и системы управления*

[9]См.: Libicki M. What is information warfare? - Washington, 1995. Информационную блокаду автор связывает с таким развитием общества, когда потоки информации будут столь же важны, как и потоки товаров. И тогда может возникать ситуация блокирования страны от такого потока. Информационный империализм автор выводит из понятия экономического империализма. Торговые войны призваны защищать своего производителя. Корпорации защищают свои умения и знания, затрудняя их получение для других стран.

[10] Command and Control Warfare, Joint Publication 3-13.1. Washington D.C.: Joint Chiefs of Staff, Feb. 1996.

[11] Joint Pub 3-13 “Information Operations”, DOD US, December 1998.

противника, при одновременной защите своей информации и информационных систем для достижения собственных политических и военных целей.

В 2010 году определение термина «информационная операция» было расширено в официальном словаре военных терминов МО США.

Информационная операция *– интегрированное использование основных возможностей электронных методов противоборства, компьютерных сетей, информационной поддержки военных операций, радиоэлектронного подавления, дезинформации, обеспечения безопасности транзакций совместно с технической поддержкой и другими возможностями для разрушения, искажения, захвата и влияния на процесс принятия решений человеком и автоматизированной системой противоборствующей стороны*.[12]

Интересно проследить дальнейшее развитие этого понятия в доктрине КНШ США 2014 года «Информационные операции» для планирования, подготовки, выполнения, а также оценку информационных операций как части военных операций. В ситуации постоянно изменяющейся стратегической обстановки и информационной среды в настоящее время под ***информационной операцией*** понимается *интегрированное использование в ходе военных операций всех связанных с информацией возможностей совместно с другими действиями для разрушения, искажения, захвата и влияния на процесс принятия решений противниками или потенциальными противниками в ходе защиты своих интересов*.[13]

По мнению Председателя КНШ, эта пересмотренная характеристика понятия информационных операций отражает современную значимость информационной сферы и способность эффективного интегрирования всех связанных с информацией возможностей в объединенные операции для создания благоприятных для достижения целей объединенного командования США условий.

Информационная поддержка военных операций, по словарю МО США, – это *планируемые операции для передачи отобранной информации и индикаторов для зарубежной аудитории с целью влияния на ее эмоции, мотивы, рассуждения, и, в конечном счете, на поведение правительств иностранных государств, организаций, групп, индивидуумов. Назначение информационной поддержки военных операций заключается в стимулировании или усилении намерений и поведения этой аудитории, исходя из цели организатора операции*.[14]

Такая трактовка этих двух понятий в современной терминологии вооруженных сил США еще раз подчеркивает взаимосвязь между техническими и психологическими информационными методами, а также указывает на важность официального закрепления соответствующей терминологии в международных правовых документах и признания использования этих методов в кризисах и конфликтах XXI века.

Достижения Соединенных Штатов в ИКТ-технологиях, разработке теории информационного противоборства и в ее практическом применении привели к необходимости или стали стимулом для других стран, в том числе, Западной Европы, Японии, Российской Федерации, государств Ближнего и Среднего Востока, Китая, Индии и др. В данной ситуации логично провести аналогию с появлением ядерного оружия: Россия оказалась в положении необходимости создания адекватного ответа на угрозы ее национальной безопасности.

Неоднозначность термина "information warfare", определенного и развитого в

[12] Dictionary of Military and Associated Terms//JP 1-02 DOD / Information operations // (JP 3-13). (http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf).
[13] Joint Publication 3-13, “Information Operations”, 27 November 2012, Incorporating Change 1, 20 November 2014, (http://www.fas.org/irp/doddir/dod/jp3_13.pdf).
[14] Dictionary of Military and Associated Terms//JP 1-02 DOD / Information operations // (JP 3-13). (http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf).

доктринах США, породила разночтение при его переводе, что обусловило появление большого количества существующих в настоящее время в российских публицистических и научных источниках определений информационной войны.

В документах, разработанных в МИД РФ, под ***информационной войной*** понимается *«противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массированной психологической обработки населения с целью дестабилизации общества и государства»,* указывая при этом на насильственный характер действий в ходе ИВ, который является необходимым обязательным признаком войны в период отсутствия открытого вооруженного конфликта.[15]

Под ***информационным оружием*** в материалах МИД России понимаются *средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства*.[16]

Представители МВД РФ считают, что ***информационная война*** – *это широкомасштабное противоборство в информационной сфере, осуществляемое путем явного или скрытного информационного воздействия на противника с целью навязывания ему требуемого для воздействующей стороны решения.*[17]

В качестве объектов воздействия выделяются властные, управленческие, информационные системы, вооруженные силы, процессы принятия решений, сознание населения, общественное мнение, критическая инфраструктура. Целями информационного воздействия авторы называют установление контроля над действиями противника и навязывание требуемого для воздействующей стороны решения; целенаправленное влияние на противника через свою и его информационную инфраструктуру; навязывание своих духовно-нравственных и культурологических ценностей в замену военных действий; гуманитарное порабощение.

По оценке российских спецслужб, ***концепция «информационной войны»*** предусматривает:

1) подавление (в военное время) элементов инфраструктуры государственного и военного управления (*поражение центров командования и управления*);
2) электромагнитное воздействие на элементы информационных и телекоммуникационных систем (*радиоэлектронная борьба*);
3) получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, и за счет специально внедренных в помещения и технические средства электронных устройств перехвата (*радиоэлектронная разведка*);
4) осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением, хищением либо нарушением нормального функционирования этих систем *(«хакерская» война*);

---

[15] Принципы, касающиеся международной информационной безопасности. Проект. Материалы МИД РФ, 2000. Крутских А., Федоров А. О международной информационной безопасности // Международная жизнь. 2000. № 2.

[16] Там же.

[17] Прокофьев В.Ф. Тайное оружие информационной войны. М.: СИНТЕГ, 1999 (Серия «Информатизация России на пороге XXI века»).

5) формирование и массовое распространение по информационным каналам противника или глобальным сетям взаимодействия дезинформации или тенденциозно поданной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения (*психологическая война*);
6) получение интересующей информации путем *перехвата и обработки открытой информации*, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в СМИ.[18]

Российские военные эксперты определяют ***информационную войну*** как *новую форму борьбы двух и более сторон, которая состоит в целенаправленном использовании специальных средств и методов влияния на информационные ресурсы противника, а также – защиты собственного информационного ресурса для достижения назначенных целей.*

В мирное время эти действия носят преимущественно скрытый характер – разведывательные и политико-психологические действия по отношению к противнику, а также осуществление мероприятий по собственной информационной безопасности.

В так называемый угрожаемый период появляются дополнительные задачи в интересах обеспечения эффективности планируемых боевых действий: предельная ограниченность в использовании сил и средств информационной войны; соблюдение существующих норм международного права (например, запрет радиоэлектронного подавления определенных частот и систем, предусмотренных Уставом Международного союза электросвязи и Регламентом радиосвязи) и т.д.

С началом военных действий решаются такие задачи, как массированное воздействие на информационный ресурс противника; предотвращение снижения боевых возможностей своих сил; проведение мероприятий по снижению уровня морально-психологической устойчивости войск противника и обеспечение нейтрализации информации, воздействующей на морально-психологическое состояние своего личного состава; ведение разведывательной деятельности и обеспечение скрытности важнейших мероприятий своих войск и т.д.[19]

В 2011 году МО России представило работу «Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве». Однако этот концептуальный документ Министерства обороны, посвященный информационной сфере, содержит только общие положения и недостаточно опирается на теоретическую основу военной и гражданской российской науки. Кроме того, опыт Соединенных Штатов в ведении эффективных информационных операций показывает, что необходимо разработать целый пакет таких документов, который должен включать теоретическое обоснование и описания практических мер, как эту концепцию реализовывать. В этой работе приводятся определения из *Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечение международной информационной безопасности от 2009 года[20]:*

информационная война – *противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;*

информационное оружие *– информационные технологии, средства и методы,*

[18] Маркоменко В. И. Невидимая затяжная война// Независимое военное обозрение. 1997. 16 августа.
[19] Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5.
[20] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. (http://docs.pravo.ru/document/view/20364925/19329178/).

предназначенные для ведения информационной войны.[21]

Некоторые другие определения понятий, связанных с обеспечением международной информационной безопасности также содержатся в Соглашении между правительствами государств – членов ШОС. (см. Приложение В).

Таким образом, решающим фактором в настоящее время становится обеспечение надежного и безопасного функционирования информационных систем, противодействие различным формам информационного воздействия. В развитых странах созданы органы власти и специальные структуры, которые отвечают за обеспечение информационно-технической и информационно-психологической безопасности, а также за проведение информационных операций.

Следовательно, *обеспечение информационной безопасности* является неотъемлемой и все более значимой частью процесса обеспечения стратегической стабильности.

Категория ***информационная безопасность (ИБ)*** возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путём воздействия на средства информационных коммуникаций.

Сегодня понятие *информационная безопасность* входит во все сферы жизнедеятельности общества. Защиту информации можно рассматривать как совокупность тесно связанных между собой задач в области международной этики, права, организации управления, разработки технических средств, программирования и математики.

Правовое обеспечение ИБ предполагает необходимость выработки юридического определения термина *информационная безопасность*.

В американском и европейском законодательстве это понятие раскрывается через определение ряда принципов:

- *доступность* – доступ к информации и функционирование системы, несмотря на возможные перебои в электроснабжении, стихийные бедствия, несчастные случаи или атаки;
- *аутентичность* – удостоверение подлинности личности пользователя (включая возможность анонимности);
- *целостность* информации – ее отправление, получение или хранение в полном и неизмененном виде;
- *конфиденциальность* – защита коммуникаций и размещенной в них информации от перехвата и ознакомления лицами, не имеющими на это права.

Такое понимание ИБ через принципы позволяет определять содержание законодательства в данной сфере и основные направления его развития. Данные понятия в дальнейшем раскрываются в целом ряде законов. В результате они дают возможность выработать единообразный подход к информационной безопасности в современном законодательстве. К примеру, конфиденциальность раскрывается в законах о персональных данных, о телекоммуникациях, об электронном документообороте, о правах потребителей в отдельных сферах (финансовой, медицинской).

В России, как и в зарубежных странах, разработке законодательства в сфере ИБ предшествует принятие политико-доктринальных документов, формулирующих основные задачи и пути их решения.

Информационная безопасность определена Доктриной информационной безопасности РФ как *состояние защищенности национальных интересов РФ в*

[21] Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве. Министерство обороны Российской Федерации, 2011 г. (https://ens.mil.ru›files/morf/Strategy.doc).

информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.[22]

Сегодня это понятие трактуется в широком и узком смыслах. В узком смысле – это безопасность самой информации и каналов ее приема (передачи), а также организация защиты от применения противником информационного оружия в ходе боевых действий. В широком – это *информационная безопасность личности, общества и государства*.

ИБ человека и общества – это состояние социума, при котором обеспечена надежная и всесторонняя защита личности, общества и государства от особого вида угроз, выступающих в форме организованных информационных потоков и направленных на деформацию общественного и индивидуального сознания.[23]

ИБ государства – это состояние сохранности информационных ресурсов государства плюс защищенность личности и общества в информационной сфере.[24]

Так как в современном социуме информационная сфера имеет две составляющие: *информационно-техническую* и *информационно-психологическую,* информационная безопасность также включает две части: ***информационно-техническую*** и ***информационно-психологическую***.[25]

Угрозы информационной безопасности в XXI веке

Под ***информационной угрозой*** понимают *потенциальную возможность нарушения информационной безопасности или потенциально возможное событие, действие, несущее определенную информацию явление, которое может привести к нанесению ущерба чьим-либо интересам*.

Угроза информационной безопасности *– это факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.*[26]

Попытка реализации информационной угрозы называется ***информационной атакой***.

В рамках вопроса об угрозах ИБ важным фактором является ***информационная уязвимость –*** *любая характеристика информационной системы, использование которой нарушителем может привести к реализации угрозы*.

Основные ***виды угроз ИБ*** направлены на нарушение:

- *доступности информационных ресурсов* (блокирование доступа);
- *конфиденциальности* (несанкционированный доступ к информации);
- *целостности* (искажение информации).

В настоящее время существуют различные классификации угроз ИБ, но в целом целесообразно выделять три основных типа.

1. *Появление и стремительное распространение «метатехнологий» (*т.е. технологий, создающих возможность контроля над потребителем и сбора информации о нем со стороны разработчика через различные гаджеты).
2. *«Электронно-цифровой разрыв»*, т.е. возникновение так называемой элиты, обладающей неограниченным доступом к ИКТ, как на внутригосударственном, так и

[22] Доктрина информационной безопасности Российской Федерации. (http://www.mid.ru/bdomp/ns-osndoc.nsf/osndd/4db2749a4b55f02f432569fb004872a4).
[23] В. П. Петров, С. В. Петров. Информационная безопасность человека и общества: учебное пособие. Москва: ЭНАС, 2005.
[24] В. Ф. Пилипенко. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник. Москва: ПЕР СЭ-Пресс, 2005.
[25] Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. Санкт-Петербург: Питер, 2008.
[26] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. (http://docs.pravo.ru/document/view/20364925/19329178/).

на международном уровнях. В результате резко возрастают возможности манипулирования мнением отдельных людей, социальных групп и государств.

3. *Компьютерная милитаризация, информационный терроризм и преступность*, т.е. использование колоссального потенциала ИКТ в интересах обеспечения военно-политического превосходства, силового противоборства и шантажа, меняющее представление о кризисах и конфликтах, тактике и стратегии ведения боевых действий и открывающее качественно новые направления гонки вооружений через сближение гражданских и военных технологий.

Основные ***цели информационных угроз –*** это ***информационные ресурсы*** – *информационная инфраструктура, а также собственно информация и ее потоки*[27] (напр., массивы документов, базы и банки данных, архивы, библиотеки, музейные фонды и пр., содержащие сведения на различных носителях информации);

Информационная инфраструктура, как совокупность информационных систем, включает в себя:

- *информационно-телекоммуникационные структуры* – государственные и корпоративные компьютерные сети, телекоммуникационные сети и системы специального и общего пользования, сети и каналы передачи данных, средства управления информационными потоками;
- *информационные, компьютерные и телекоммуникационные технологии (киберпространство*[28]*)*;
- *СМИ*;
- *организационные структуры*, обеспечивающие функционирование и развитие единого информационного пространства, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации.

Таким образом, существует принципиально новая среда ведения боевых действий – ***информационное пространство (ИП) –*** *сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию*[29].

Можно констатировать не только существование информационного пространства как части общего геостратегического ландшафта, но также наличие предпосылок для развития и распространения информационного оружия. В связи с этим вооруженные конфликты все более приобретают характер многомерных информационных войн, которые могут одновременно вестись на различных фронтах и уровнях.

---

[27] Там же.

[28] *Кибернетическое пространство – сфера деятельности в ИП, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой с их помощью человеческой активности (личности, организации, государства).* Концепция стратегии кибербезопасности РФ. Проект. (http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf).

[29] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. (http://docs.pravo.ru/document/view/20364925/19329178/).

Глава 2. Информационный фактор вооруженной борьбы: от исторических фактов к новым методам противоборства в XXI веке*

Историческая справка: психологические технологии Второй мировой войны

В 1942 году профессор Оксфорда Фредерик Линдеман, главный научный консультант и личный друг У. Черчилля, написал письмо руководителю группы военных советников Ф. Рузвельта Ванневару Бушу, в котором указывал на две проблемы. Во-первых, большие потери самолетов во время американских бомбардировок Германии, нацеленных на промышленные объекты, и их низкая эффективность. Во-вторых, неэффективность англо-американской пропаганды, нацеленной на Германию.

В письме Ф. Линдеман жаловался на Эдварда Бернейса, крупнейшего американского специалиста в области PR, которого американцы с начала войны командировали в помощь британской пропаганде. Он действовал по своим привычным рецептам, которые, как писал Ф. Линдерман, оказались в случае национал-социалистической Германии бесполезными.

Получив это письмо, В. Буш переслал его командующему американскими войсками Дж. Маршаллу, будущему автору знаменитого «Плана Маршалла» и генералу Г. Арнольду, командующему американской авиацией – самым «продвинутым» и технологичным видом Вооруженных Сил того времени, в составе которого функционировало несколько лабораторий, где работали выдающиеся американские ученые (после войны в структуре ВВС была создана первая фабрика мысли, знаменитая Корпорация RAND). Письмо попало в две такие исследовательские группы.

Первая действовала на базе самого элитного университета США – Гарварда. Эта группа занималась *анализом целей для бомбардировки на территории Германии и их отбором с точки зрения военной доктрины*. Экономическую часть группы возглавлял крупнейший американский специалист в области эконометрики, будущий лауреат Нобелевской премии, выпускник Ленинградского Университета Василий Васильевич Леонтьев.

Командующий американской авиацией исходил из того, что после завершения войны и победы над Гитлером, Германия должна стать союзником США, и поэтому ставил перед группой В.В. Леонтьева задачу нанесения максимального ущерба при сохранении системообразующих предприятий Германии. Важно было также сохранить собственность американских корпораций, которым принадлежали многие ведущие немецкие предприятия, работавшие в течение всей войны.

Получив письмо, В.В. Леонтьев обратился за советом к своему коллеге по Гарварду, декану первого в Америке факультета социологии и, как пишут в США, «отцу американской социологии», Питириму Сорокину, который сообщил генералу Г. Арнольду, что пропаганда против режимов, построенных на идеологии (П. Сорокин называл их идеократиями), которую разделяет подавляющая часть населения, бессмысленна. Более того, военные испытания и бомбардировки промышленных объектов лишь увеличивают преданность режиму. Чтобы справиться с идеократией, по мнению П. Сорокина, есть два пути. Либо революция, либо *социальный хаос на фоне резкого возрастания страданий и лишений*. В этих условиях первичные потребности в выживании становятся сильнее более высоких потребностей, связанных с самоидентификацией, культурными ценностями и т.п. Поэтому

* Статья основана на: Ковалев В.И., Ларина Е.С., Сергеев Н.А. Психологический фактор вооруженной борьбы. Работа поддержана РГНФ, грант 12-03-00387 «Междисциплинарный анализ инновационных стратегий и процессов модернизации».

целью бомбардировок, по мнению П. Сорокина, должны стать *не столько предприятия, сколько население городов*.

В результате в январе 1943 году руководство США и Великобритании приняло решение о начале «ковровых» бомбардировок городов Германии. Встал вопрос о выборе целей и повышении эффективности бомбардировок.

Для этого была задействована вторая научно-исследовательская группа ВВС, возглавляемая известным американским математиком, будущим отцом кибернетики и автором теории искусственного интеллекта Норбертом Винером. Официально группа занималась моделированием противовоздушной обороны и отработкой средств ее преодоления. Однако, Н. Винер, используя финансирование Пентагона, собрал большую группу специалистов из различных областей, заметную роль в которой играли психологи и нейрофизиологи. Интересно, что, хотя первое общедоступное издание книги «Кибернетика» датируется 1947 годом, реально эта книга с грифом «секретно» была издана в середине войны и, поскольку имела желтую обложку, была известна разведкам воющих стран, как «секретная желтая книга».

В группу Н. Винера входил молодой Ганс Селье, прославившийся вскоре после войны теорией стресса. В своих многочисленных работах он признавался, что огромное влияние на него оказали труды И.П. Павлова и В.М. Бехтерева.

Г. Селье порекомендовал Н. Винеру обратиться к знаменитому немецкому психологу и социологу Курту Левину, который после эмиграции из Германии преподавал в Университете Айовы.[30] Выполняя заказ ВВС, К. Левин написал в 1942 году работу «Перспектива времени и моральный дух». В ней он отметил: «Один из главных методов подавления морального духа посредством стратегии устрашения (террора) состоит в том, чтобы держать человека в состоянии неопределённости относительно его текущего положения и того, что его может ожидать в будущем».[31]

К. Левин предложил создать в составе сухопутных подразделений американской армии специальные группы людей, которые бы не только опрашивали пленных, но и читали письма солдат и офицеров к своим родным, захваченные в результате военных действий. Анализ писем должен был использоваться для определения морального эффекта, вызванного бомбардировками.

С использованием основных положений теорий динамической психологии и психологии поля К. Левина[32], которые разрабатывались им в течение 14 лет, была построена специальная шкала, увязывающая масштабы разрушений и жертв мирного населения с падением морального духа в тылу и на фронте. Ученый сформулировал гипотезу, устанавливающую необходимый порог разрушений и жертв, начиная с которого подавляющая часть населения в тылу и на фронте перестает верить в победу своей страны и отказывается от собственных идеологических убеждений. С 1943 года совместное командование ВВС США и Великобритании вырабатывало перечни целей с учетом «кривых Курта Левина».

Как хорошо известно, все решающие события на фронте в этот период происходили на Востоке. Судьбу войны решило противостояние Германии и Советского Союза. По мере

---

[30] Про Левина в современной литературе ходят совершенно фантастические истории. Их источником стала одна из самых известных в популярной конспирологии книг – работа Джона Колемана «Комитет трехсот». Как это бывает в большинстве популярных, а не научных конспирологических книг, факты в них грубо искажены и порождают невероятные выводы. *Прим. автора*.

[31] Левин К. Разрешение социальных конфликтов / [Пер. с англ. И. Ю. Авидон]. — СПб.: Речь, 2000. Зейгарник Б.В. Теория личности К. Левина. М.: Изд-во Моск. ун-та, 1981.

[32] Теории динамической психологии и психологии поля К. Левин разрабатывал с 1922 по 1936 гг., во взаимодействии с советскими психологами Львом Выгодским и Александром Лурия. Значительная часть студентов и аспирантов К. Левина были русскоязычными. Часть из них последовала за ним в Америку, а часть вернулась в Советский Союз. *Прим. автора*.

приближения Красной Армии к Германии, советская пропаганда разительно изменилась, в СССР были приняты достаточно суровые государственные решения, препятствующие массовому насилию, грабежам и прочим действиям против мирного населения, которые, по свидетельству советских военных, были исключительно эффективными и свели к минимуму подобные явления. Кроме того, общеизвестно, что советская авиация никогда не проводила «ковровые» бомбардировки германских городов.

Позднее, при обсуждении вопросов послевоенной Германии в военно-политическом руководстве США рассматривались две точки зрения: одна была представлена министром финансов Генри Моргентау, вторая – Джорджем Маршаллом. Г. Моргентау предлагал раздробить Германию, превратить ее в аграрную страну, демонтировать и ликвидировать промышленность. Дж. Маршалл придерживался точки зрения, что Германия в послевоенном мире должна сохраниться как промышленная держава и полноценное государство. Подобной точки зрения придерживались Ф. Рузвельт и И. Сталин. Естественно, что у каждой из союзных стран были свои резоны и свои расчеты.

Дж. Маршалл поставил перед научными группами задачу: разработать план превращения Германии, а главное, немецкого населения, в друзей США и врагов СССР. Для ее решения проводились специальные совещания у Дж. Маршалла по способам использования бомбардировок для послевоенного доминирования Америки в Германии. При этом использовалась трехступенчатая теория изменений К. Левина.

Суть теории в том, что в любых текущих условиях, допускающих желательное изменение, первый этап заключается в «размораживании» ситуации. «Размораживание» поведения или привычек оказывается особенно сложным, если они существовали в течение долгого времени и подкреплялись проявлениями одобрения или достижением успеха. Однако этот процесс облегчается в периоды кризиса или катарсиса, разрушающих ограничения, в рамках которых действуют существующие системы убеждений, ценностей и действий. Если существующие ограничения устраняются, то наступает следующий этап, называемый «движением».

На втором этапе индивид или группа побуждаются к отказу от прежних убеждений, ценностей или типов поведения ради более совершенных или более желательных с точки зрения управленца. Наконец, если переход оказался успешным, то на третьем этапе его результаты должны быть «заморожены», т.е. необходимо обеспечить равновесие сил развития и стабилизации, которое гарантирует сохранение вновь приобретенных убеждений, ценностей и т.д.

Перед ВВС была поставлена задача «вбомбить» Германию в катастрофу. Т.е. не просто лишить ее население последних иллюзий относительно гитлеровского режима, но и погрузить его в состояние подлинного ужаса. На это были направлены бомбардировки таких городов, как Берлин, Нюрнберг, Штутгарт, Фрейбург и знаменитое февральское 1945 года уничтожение Дрездена, во время бомбардировок которого, согласно официальным данным нынешних германских историков, погибло примерно 25-30 тыс. человек. Однако, согласно мнению историка бомбардировки Дрездена Дэвида Ирвинга, погибло около 130 тыс. человек, что больше, чем при бомбардировке Хиросимы. Общие потери германского населения от бомбардировок англо-американской авиацией оцениваются примерно в 600 тыс. человек.

После окончания войны наступила третья фаза реализации подхода К. Левина: Дж. Маршалл выступил инициатором разработки, а затем и реализации «Плана Маршалла» для восстановления Европы.

Теоретическая база современных средств информационного противоборства

Как социальное и общественно-политическое явление война никуда не ушла из жизни человечества и в XXI веке; она трансформируется, утрачивая прежние и приобретая новые черты. Война, по-прежнему, остаётся для общества «отцом всего» (по Гераклиту), а для государства ещё и «путём жизни и смерти» (по Сунь-Цзы).

Из века в век развитие военной техники шло в направлении создания и совершенствования боевых платформ, коими в древности являлись колесницы и боевые слоны, а сейчас – танки, бронетранспортёры, самолеты, корабли, подводные лодки и ракетные комплексы разного типа. А развитие вооружений шло в направлении от средств индивидуального поражения к средствам группового, а затем и массового поражения. Массированные бомбардировки периода Второй мировой войны, атомные бомбардировки японских городов Хиросимы и Нагасаки в августе 1945 года, а позже «ковровое» бомбометание во Вьетнаме показали, что при определённых условиях *война* может быть *дистанционной и бесконтактной*.

Дальнейшие качественные и количественные изменения вооружения и военной техники, средств разведки и наблюдения за противником, совершенствование средств автоматизации управления, связи и передачи данных, бурное развитие информационных технологий, в конце концов, привели на рубеже XX и XXI веков к осознанию необходимости изменения форм и методов управления вооружённой борьбой. Успех в сражении уже должен был решаться при слаженном взаимодействии всех видов и родов войск – флота, авиации, ракет средней и меньшей дальности, артиллерии, танков и пехоты. Тем самым от действия различных боевых платформ на поле боя достигался своеобразный синергетический эффект.

В конце 90-х годах идея объединения всех трех компонентов – средств разведки и наблюдения, боевых платформ, средств автоматизации управления и связи в единую систему для достижения поставленной цели начала обретать свои очертания в ВС США.[33] Ядром такой системы, новым «центром силы» стала телекоммуникационная сеть обмена данными, фактически образующая для потребителей единое информационное пространство, доступ к информации в котором регламентируется соответствующими полномочиями. Таким образом, необходимость максимального использования возможностей всех имеющихся средств привела к переходу от «платформоцентрической» модели управления войсками и оружием к «сетецентрической», получившей в итоге наименование *Network Centric Warfare* (NCW) – *«сетецентрический способ ведения войны»*.[34]

Термин *«сетецентризм»* впервые появился в американской компьютерной индустрии и стал результатом прорыва в информационных технологиях, которые позволили организовать взаимодействие между компьютерами, даже несмотря на использование в них разных операционных систем. Позднее идея сетецентризма была взята на вооружение армией США. Так, идеологи новой концепции – вице-адмирал ВМФ США Артур Цебровский и эксперт МО США Джон Гарстка – отмечали, что концепция «сетецентрической войны» – это не только развертывание цифровых сетей с целью обеспечения как вертикальной, так и горизонтальной интеграции всех участников боевой операции. Это еще и изменение тактики действия формирований с рассредоточенными боевыми порядками, оптимизация способов разведдеятельности, упрощение процедур согласования и координации огневого поражения, а также нивелирование разграничения средств по звеньям управления.

---

[33] Network Centric Warfare. The RMA Debate, (http://www.comw.org/rma/fulltext/netcentwar.html).
«Сетецентрическая война. Дайджест по материалам открытых изданий и СМИ». – М. ВАГШ ВС РФ, 2010.

[34] Кондратьев А. «Сетецентрический фронт. Боевые действия в едином информационном пространстве». Журнал «Национальная оборона» № 2 / 2011.

По сути ***«сетецентрическая война»*** – это *ориентированная на достижение информационного превосходства совокупность мероприятий по организации управления действиями группировок войск (сил), предусматривающая увеличение их боевой мощи за счет создания единой информационно-коммутационной сети, связывающей источники данных, принимающих решения лиц и исполнителей.* Это обеспечивает доведение до участников действий необходимой информации об обстановке, ускорение процесса управления силами и средствами, и повышение, вследствие этого, темпов операций и эффективности поражения противника.

Анализ боевых действий США в течение последних 15 лет показывает, что концепция «сетецентрической» войны хороша в военных конфликтах малой и средней интенсивности, в противоборстве сильного и слабого противников. При этом тыл сильного, в отличие от слабого, не подвергается никаким разрушающим воздействиям, а средствам разведки, системам связи и управления не оказывается серьёзного противодействия (действия США в Афганистане и Ираке). Хороша данная концепция и для блицкрига: оккупация Ирака Соединенными Штатами и Великобританией в 2003 году.

Но даже несмотря на видимые успехи, достигнутые в военной операции против Ирака в 2003 году, многие военные специалисты, и в первую очередь, из США, критически оценивают практику применения концепции «сетецентрической» войны.

Тем не менее, в когнитивную компоненту российской целевой аудитории (куда входят и базовые элементы системы принятия военно-политических решений) активно вводится положение о том, что будущие войны будут, как правило, «сетецентрическими», «дистанционными» и «бесконтактными», с использованием в основном неядерных высокоточных средств поражения. И если такой взгляд на войны будущего у нас превратится в поведенческий архетип, то мы будем готовиться к войне, в которой у нас, очевидно, на краткосрочную и среднесрочную перспективу просто нет шансов на победу (так называемое запрограммированное поражение).[35]

Но если мы зададимся вопросом: «А почему война в будущем должна быть именно такой?» и в качестве «асимметричного ответа» любому агрессору будем готовить контактную войну с применением всего арсенала средств направленного воздействия, которым мы можем обладать, то и характер такой будущей войны будет уже другой, и её финал будет заранее непредсказуем. Поэтому, как будет развиваться ситуация в том случае, если концепция «сетецентрической» войны будет применяться при столкновении сильных армий, имеющих богатый исторический опыт крупных войн и кровопролитных сражений, сказать сложно.

Что касается непосредственно российской армии, то, «примеряя» на свои вооруженные силы иноземный кафтан «сетецентрической» войны, необходимо учитывать действующие положения руководящих документов в области обороны и безопасности, в первую очередь Военную доктрину РФ, внешнеполитический курс страны, проводимый её руководством. Следует иметь в виду, что «задачи вооруженных сил США и нашей армии радикально не совпадают. США и их союзники по НАТО на протяжении десятилетий ведут, как правило, наступательные военные действия за пределами своей территории, всегда обладают инициативой в развязывании войны, воюют с более слабым противником. Поэтому их опыт нетипичен для нас. Нам, прежде всего, надо обеспечить защиту своей территории и поэтому в начале войны придется вести оборонительные действия против более сильного, принципиально разного на каждом ТВД противника»[36].

---

[35] Ковалёв В.И. «Проблема управления процессами модернизации в военной сфере в условиях неопределённости представлений о военных конфликтах будущего». Журнал «Информационные войны», № 4 (24) за 2012.

[36] Рукшин А. С. «Некоторые итоги реформы Вооруженных Сил». Газета «Военно-промышленный курьер» № 45 (462), 14 ноября 2012 г.

Исходя из этого, с целью появления возможностей, да и самих предпосылок реализации «сетецентрической» концепции в российской армии необходимо решать комплексную задачу не только в рамках ВС, но и страны в целом. Для этого должна быть разработана специальная экономическая стратегия (по типу «атомного» проекта или программы освоения космоса), в которой будут предусмотрены и поиск новых технологических решений с привлечением организаций РАН, и перевод оборонно-промышленного комплекса на инновационный путь развития, и подготовка для оборонно-промышленного комплекса квалифицированных кадров.

В рамках ВС России целесообразно активизировать работы по созданию действительно объединенных органов управления, разработке современных алгоритмов их деятельности при решении различных боевых задач, формированию перечня систем и средств, которые планируется связать в сети на разных уровнях управления с обоснованием, почему и, самое главное, для чего это нужно. Необходимо создание новых форм и способов применения группировок войск в различных условиях обстановки, уточнение боевых документов, уставов и наставлений, отработка в ходе учений и тренировок полученных навыков, а также более активное внедрение информационных технологий в повседневную деятельность российской армии.

Только в этом случае концепция «сетецентрической» войны не станет для вооружённых сил России очередной ментальной ловушкой, а действительно превратится в «множитель силы».

Концепция «сетецентрической» войны была включена в активно практикуемую Соединенными Штатами и их союзниками в XXI веке форму противоборства: *концепция нацеленности на конечный результат или эффект в объединенных операциях – «Effects-Based Approach to Joint Operations»* 2006 года.[37] Она базируется на представлении противника как многоуровневой системы, модель которой для простоты изображается в виде ряда концентрических окружностей с национальными лидерами в центре. В модели, названной авторами «враг как система», вооружённые силы страны составляют внешнее, самое последнее кольцо, предназначенное для защиты всей системы от силового воздействия армии противника. При этом каждая окружность – это своеобразный центр тяжести (силы). Прочность «врага как системы» определяется уравновешенностью всех центров соответствующей государственной политикой.

При таком подходе, по мнению стратегов США, оказывая различными способами давление не только на внешнее кольцо (армию), как это практиковалось ранее, а и на другие центры силы можно заставить противника действовать именно так, как задумано, что в итоге приведет к нужному эффекту – его поражению. При этом под эффектом понимается «физический, функциональный или психологический результат, событие или то, что является результатом конкретных военных и невоенных действий».[38] В этом случае «операция на основе эффектов» – это процесс, направленный на получение желаемых стратегических результатов или эффект, оказываемый на врага посредством синергетического, мультипликативного и кумулятивного применения полного спектра военных и невоенных возможностей на всех уровнях, от тактического до стратегического. Эффекты могут быть нескольких уровней: эффекты первого уровня наступают сразу после наступления того или иного события, эффекты же более высоких уровней могут проявиться спустя значительное время и в совершенно иной области.

Большой вклад в разработку новых концепций ведения войны с использованием информационного воздействия внесла американская Корпорация RAND. Одним из важных результатов ее исследований, проведенных в 90-х годах прошлого века, явилось глубокое

[37] Commander's Handbook for an Effects-Based Approach to Joint Operations, Joint Warfighting Center, Joint Concept Development and Experimentation Directorate, Standing Joint Force Headquarters, 24 February 2006.
[38] Сетецентрическая война. Дайджест по материалам открытых изданий и СМИ». – М. ВАГШ ВС РФ, 2010.

осознание возможностей информационного оружия, что выразилось в появлении в одном из отчетов этого аналитического центра термина *"strategic information warfare"* – ***стратегическое информационное противоборство***. Это понятие определялось как «*…использование государствами глобального информационного пространства и инфраструктуры для проведения стратегических военных операций и уменьшения воздействия на собственный информационный ресурс…*».[39]

Ключевым понятием, введенным в работах RAND, стало *«стратегическое информационное противоборство»*. ***Стратегическое информационное противоборство первого поколения*** рассматривалось наряду с традиционными средствами противоборства (ядерными, химическими, биологическими и др.) и определялось как «одна из нескольких компонент будущего стратегического противоборства, применяемая совместно с другими инструментами достижения цели…». ***Стратегическое информационное противоборство второго поколения*** определяется как «…принципиально новый тип стратегического противоборства, возникший в ходе информационной революции и включающий действия в информационном пространстве и других сферах (прежде всего, в экономике) в течение недель, месяцев и лет…»[40]. Отмечается, что развитие и совершенствование подходов к стратегическому информационному противоборству второго поколения, возможно, приведет к полному отказу от использования военной силы, поскольку скоординированные информационные акции просто не позволят применить ее.

Дальнейшее развитие понимания роли и места средств и методов информационной борьбы привело аналитиков Пентагона к осознанию необходимости трансформации существующей теоретической базы, приемов и способов ведения информационной войны. Так, развитие процессов глобализации привело к росту взаимоувязанности современного мира: сегодня практически любой региональный конфликт сказывается на биржевых котировках в любой точке земного шара. В такой ситуации, по мнению экспертов RAND, наилучший выход может быть найден путем использования в военном деле теоретического и методического задела, накопленного наукой в области теории управления сложными адаптивными системами, в области теории хаоса и теории катастроф. В наибольшей степени военных привлекает так называемый «эффект бабочки», когда даже незначительные изменения начальных условий могут привести в обозримом будущем к грандиозным последствиям в системе. Использование этого эффекта позволило бы с минимальными затратами решать сложнейшие геостратегические задачи без масштабного применения военной силы.

К действиям, обеспечивающим проведение информационных операций, относятся и мероприятия по организации связи с гражданской администрацией и населением, проводимые соответствующими службами ВС США. Подразделения этой службы непосредственно ориентированы на действия, обеспечивающие взаимную поддержку при проведении психологических операций. Декларативно задачи службы заключаются в следующем: оперативное доведение точной и своевременной информации о проводимой кампании (операции) до заинтересованных организаций и население; разъяснение задач, решаемых вооруженными силами; предоставление командованию каналов СМИ для информирования противника (потенциального противника) о намерениях и возможных действиях союзных войск. При этом утверждается, что эти действия не могут применяться для введения противника в заблуждение или для дезинформации общественности. На

[39] Molander, Roger C. Strategic information warfare: a new face of war / Roger C. Molander, Andrew S. Riddile, Peter A. Wilson. Library of Congress Cataloging in Publication Data, RAND (Firm). 1996. (http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf).

[40] Molander, Roger C. Strategic information warfare rising war / Roger C. Molander, Peter A. Wilson, B. David Mussington, Richard Mesic. Library of Congress Cataloging in Publication Data, RAND (Firm). 1998. (http://www.rand.org/content/dam/rand/pubs/monograph_reports/2009/MR964.pdf).

практике, однако, возможности этой службы широко используются для формирования мирового общественного мнения в выгодном для США отношении за счет выборочной и дозированной подачи информации.

В целом концепция информационного противоборства в том виде, в каком она реализуется в ВС США, не является новой для российского военного искусства. Теоретические основы информационного противоборства достаточно полно раскрыты в российской военной науке через понятия «борьба с системами управления противника», «радиоэлектронная война», «завоевание господства в эфире», «психологическая война», «дезинформация», «военная хитрость» и т. п. Новизна американского подхода к теории информационного противоборства заключается в комплексном использовании широкого спектра научных, военно-теоретических и технологических достижений в информационной сфере.

В настоящее время США, обладая значительным преимуществом в области разработки и использования новейших радиоэлектронных систем и компьютерных технологий и основываясь на постулатах новой концепции, стремятся закрепить за собой доминирующую роль не только в политической, экономической и военной сферах, но и в мировой информационной инфраструктуре.

Моделирование информационных процессов обеспечения информационно-технического противоборства

Война – это не столько материально-физический, сколько психологический феномен, где физическое насилие, как правило, не является самоцелью, а лишь средством для принуждения противника к выполнению своей воли.

Анализ опыта США показывает все возрастающую значимость междисциплинарных и мультидисциплинарных научных исследований информационного пространства с целью решения проблемы научного прогнозирования и планирования в сфере ИКТ. Частью такой деятельности является разработка прикладных математических методов. Поскольку материально-физические параметры информационного противоборства и войны, как крайней его формы, в значительной степени исследованы и поддаются расчёту, приведем пример применения таких методов, а именно – метода математического моделирования – к психологической (иррациональной) составляющей.

Согласно Клаузевицу, можно выделить основные психологические закономерности войны: 1) доминирование в войне враждебного чувства; 2) достижение политической цели через психологическое принуждение; 3) выбранная военная цель (психологические издержки) должна соответствовать политической цели войны (психическому доходу).

Условия, определяющие возможность поражения противника: размер накопленных сторонами средств вооруженной борьбы, включая объем финансовых ресурсов; качество военной организации – уровень «социальных трений»; воля к победе – уровень «социальной температуры».

Главное мерило войны – степень достижения политической цели.

Субъективно переживаемая и мотивирующая сила политической цели войны представляет собой разницу между следующими составляющими: «возбуждающей» составляющей (уровень психологического дохода, который сторона предполагает получить в результате победы над врагом) и «тормозящей» составляющей (психические затраты, которые население страны готово заплатить за победу).

На основе основного психофизического закона Вебера-Фехнера предлагается сформулировать математическую модель эмоции в виде:

$$\varepsilon(t) = \pi[S(t), Smax(t), Smin(t)],$$

где $\varepsilon(t)$ – побудительная сила эмоционального переживания;

$S(t)$ – текущее состояние образа-раздражителя;

$Smax(t)$ – верхнее пороговое (нормативное) значение, отождествляемое с желательным «уровнем блага» (уровень притязаний) субъекта;

$Smin(t)$ – нижнее пороговое (нормативное) значение, отождествляемое с состоянием «неприемлемого уровня наносимого ущерба;

$\pi[*]$ – логарифмическая функция.

Модель побуждения к действию базируется на следующих концептуальных положениях.

Онтологический элемент побуждает к действию две силы:

а) силу притяжения или мотива:

$$\Delta S_м(t) = [Smax(t) - S(t)]/[Smax(t) - Smin(t)];$$

б) силу отталкивания или стимула:

$$\Delta Sc(t) = [S(t) - Smin(t)]/[Smax(t) - Smin(t)].$$

Результирующая эмоциональная реакция на раздражитель в законе Вебера-Фехнера задается выражением:

$$\varepsilon(t) = \{\mu_м(t) \log \Delta S_м(t) + \mu_c(t) \log \Delta Sc(t)\},$$

где $\mu_м(t)$ и $\mu_c(t)$ ($\mu_м(t) + \mu_c(t) = 1$) – коэффициенты мотивации и стимуляции, показывающие, соответственно, значимость для субъекта переживания, связанного с желанием приблизиться к состоянию, приносящему ему радость, и переживания, связанного с желанием удалиться от состояния, приносящему ему боль.

Эмоциональная реакция по всем составляющим $Э(t)$ (психофизической, психосоциальной и духовной с коэффициентами $\rho_ф(t)+\rho_п(t)+\rho_д(t)=1$) равна:

$$Э(t) = a[\varepsilon_ф(t)]\rho_ф(t).[\varepsilon_П(t)]\rho_п(t).[\varepsilon_д(t)]\rho_д(t).$$

Исходя из изложенного, можно составить обобщённую математическую модель войны как политического инструмента психологического принуждения.

Угроза $\delta^у$ заставит отдать $\delta^{ж}$, если

$$\Delta\varepsilon_c^{ж} + \Delta\varepsilon_м^{ж} < \Delta\varepsilon_c^{у} + \Delta\varepsilon_м^{у},$$

которая используется при построении модели, отражающей изменения психосоциального состояния социума в ходе противоборства (ведения боевых действий).

Авторами предлагается использовать инвариантную модель военной организации онтологических элементов, участвующих в силовом противоборстве, и модель динамики изменения психологической ситуации в операционном пространстве. Они разработаны на базе методологии формирования операционного пространства моделей объектов информационно-технического взаимодействия (противостояния) и междисциплинарного, синтетического подхода с использованием многосторонних, многоуровневых стратегических деловых компьютерных игр, а также анализа принимаемых в сфере национальной безопасности политических государственных решений. При этом принимается во внимание

необходимость учета процессов, происходящих в области индивидуального и массового психического сознания.

Решение задачи разработки моделей информационных процессов имеет практическое применение в специальных системах поддержки принятия решения и позволяет повысить эффективность управления, обоснованность и оперативность принимаемых решений, снизить возможные риски, добиться результативности, в значительной степени сократить морально-психологические издержки.

Глава 3. Примеры информационно-технических методов противоборства XXI века

Под ***информационным противоборством*** будем понимать *совокупность таких взаимоотношений между субъектами мирового сообщества или политической системы общества, в рамках которых одни субъекты путем активного воздействия на информационную сферу других субъектов стремятся получить превосходство над противостоящей стороной в экономической, политической, военной и/или иной области*.[41]

В ***информационно-техническом противоборстве*** главными объектами нападения и защиты являются системы управления и связи, телекоммуникационные системы, различные радиоэлектронные средства, а также информационные ресурсы государства: информация на материальных носителях или существующая в любой другой форме.

Именно в этой сфере и сформировалось понятие «информационное оружие», получившее широкое распространение после завершения военной операции «Буря в пустыне» 1991 года, когда решающий вклад в поражение Ирака внесло комплексное применение средств разведки, управления, связи, навигации и радиоэлектронной борьбы, совокупность которых и была определена как информационное оружие театра военных действий.

Под специальным ***программно-математическим или кибернетическим воздействием (кибервоздействием)*** понимают *средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей и компьютерных систем*.

Кибервоздействие осуществляется в ***кибернетическом пространстве (киберпространстве)*** *– сфере деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других коммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой с их помощью человеческой активности (личности, организации, государства)*.[42]

Киберугрозы (информационно-технические угрозы) – относительно новый, ускоренно развивающийся и опасный вид информационных угроз. По данным «Лаборатории Касперского», *киберугрозы делятся на две группы по сферам воздействия*. Первая связана с *атаками на бизнес:* коммерческий шпионаж, кражи баз данных, информационные действия с целью подрыва репутации и т.д. На поле битвы встречаются хакеры, противостоящие им компьютерные специалисты из корпораций, киберспецслужбы. Целью второй группы являются *устройства, контролирующие жизнедеятельность общества, передвижение и работу большого числа служб:* кража и взлом систем, нелегальное приобретение возможности бесплатно пользоваться различными сервисами, удаление и изменение информации о себе, своей (или заказчика) активности и т.д.[43]

Согласно Европейской Конвенции по киберпреступлениям, ***киберпреступления*** – *это правонарушения, направленные против конфиденциальности, целостности и*

---

[41] Манойло А.В. Государственная информационная политика в особых условиях: Монография. М.: МИФИ, 2003.

[42] Концепция стратегии кибербезопасности РФ. Проект. (http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf).

[43] Киберпрогноз-2020 от «Лаборатории Касперского». (http://www.kaspersky.ru/about/news/virus/2011/kiberprognoz_2020_ot_laboratorii_kasperskogo).

доступности компьютерных систем, сетей и данных, а также их неправомерное использование.[44]

Некоторые виды киберпреступлений являются объектом дискуссий специалистов в информационной сфере в течение многих лет. Одни исследователи полагают, что эти преступления – не более чем противоправные деяния, совершенные с помощью современных средств – охватываются составами в национальных уголовных кодексах и не являются новыми категориями преступлений.[45] Другие считают, что киберпреступления – качественно новая категория преступлений, требующая принятия новых норм, освоения новых методов расследования, подразумевающая международное сотрудничество в борьбе с этим явлением. Действительно, компьютерные мошенничества, кражи, вымогательства и другие подобные преступления не являются новыми видами противоправных деяний. Однако средства, с помощью которых они совершаются, требуют разработки новых норм закона и освоения новых методов расследования. Это обусловлено тем, что киберпреступления зачастую выходят за рамки обычных составов, и, кроме того, их «виртуальный» характер позволяет быстро уничтожить следы, что значительно затрудняет поиск преступника.

[44] Европейская Конвенция по киберпреступлениям. (http://inter.criminology.onua.edu.ua/?p=2263).

[45] *Состав преступления* в науке уголовного права – совокупность установленных уголовным законом объективных и субъективных признаков, характеризующих общественно опасное деяние как преступление.

3.1. Кибервойна против ядерной программы Ирана

Одним из первых случаев эффективного кибервоздействия на физические объекты критически важных структур стали комплексные массированные кибератаки на ядерные предприятия Исламской Республики Иран в Бушере и Натанзе (2010-2012 годы). Кибертехнологии стали исключительно важным инструментом влияния на решение иранской ядерной проблемы, дополняющим и, возможно, не уступающим по силе воздействия политическим и экономическим санкциям и даже военным мерам. Использованный при этом компьютерный «червь» *Stuxnet* до сегодняшнего дня рассматривается в качестве уникального инструмента целевой атаки и оценивается как первый и пока единственный случай применения кибероружия, способного причинять физический ущерб, и разработанного специально для саботажа процесса по обогащению урана на определенных объектах.

В 2013 году генеральный директор российской компании «Лаборатория Касперского» («ЛК») Е. Касперский сообщил о заражении программой *Stuxnet* компьютерной сети ядерных объектов не только Ирана, но и России. Исходя из того, что Бушерская АЭС строилась российскими специалистами, такая угроза представляется небезосновательной. Однако, по заявлениям российских ядерщиков, обеспечение кибербезопасности критически важных инфраструктур РФ находится на высоком уровне, и такие риски предусмотрены соответствующими службами. В любом случае, в целях прогнозирования будущих возможных угроз необходим глубокий анализ и междисциплинарные исследования этого примера.

Вредоносные программы (ВП) Stuxnet, Duqu, Wiper и ***Flame*** были обнаружены специалистами из разных стран в период 2010-2012 годов. Их объединяет ряд общих технических параметров, высокая сложность кода и цели атаки. Программисты отмечают, что функционалы этих ВП отличаются от привычных в сфере киберпреступности, поскольку они «были созданы не для хищения денежных средств и индивидуальных данных пользователя, не для рассылки спама, а в целях вредительства на предприятиях и выведения из строя индустриальных систем».[46] В сентябре 2010 года Е. Касперский сравнил этот факт с открытием «ящика Пандоры». Подобные системы используются в нефтепроводах, электро- и атомных станциях, коммуникационных системах, портах, аэропортах и даже на военных установках.

Stuxnet — уникальный компьютерный «червь», вредоносная троянская программа, предназначенная для атаки на компьютеры под управлением системы визуализации производственных процессов Siemens WinCC с целью киберсаботажа. Атакованные платформы: промышленные системы SCADA. Способы распространения: USB-накопители, через LAN и файловое заражение. Программа получила свое название от двух драйверов (mrxnet.sys и mrxcls.sys), которые она встраивает в систему ОС Windows. Файлы драйвера в *Stuxnet* использовали действительные подписи Realtek и JMicron в качестве доказательства того, что приложение легально. Это помогло скрыть зловреда в системе и на заражённых USB-устройствах и обеспечило функционирование руткитов.[47]

ВП Stuxnet в июне 2010 года обнаружил специалист из белорусской фирмы «ВирусБлокАда» С. Уласень.[48] Сообщения, впоследствии приведшие к открытию *Stuxnet*, поступили из Ирана. В результате анализа кода *Stuxnet* выяснилось, что впервые его следы были зарегистрированы еще в 2005 году, а первые образцы поступили в базы данных

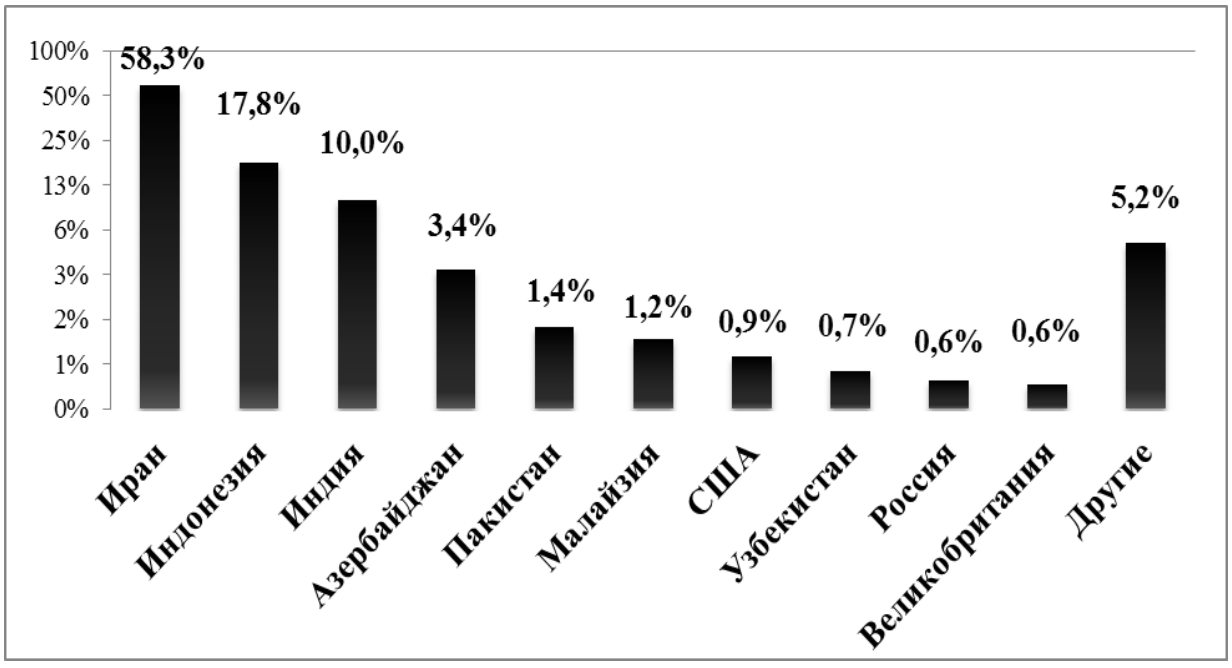
[46] Kaspersky Lab provides its insights on Stuxnet worm // Kaspersky Lab. — 2010. September 24. (http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm).
[47] Хроника целевых кибератак. Kaspersky Lab ZAO/. (https://apt.securelist.com/ru/#secondPage/attack=26).
[48] The Man Who Found Stuxnet — Sergey Ulasen in the Spotlight // Eugene Kaspersky's Blog. — 2011. November, 2. (http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight).

антивирусных компаний в 2007 году. В июле 2010 года компания *Symantec* запустила систему мониторинга трафика вируса *Stuxnet*, что позволило ей отследить число зараженных компьютеров в отдельных регионах. Программа неактивна с 2012 года.

Сразу же после его обнаружения и добавления детектирования несколько компаний зафиксировали десятки тысяч зараженных систем с эпицентром в Иране. Это дало однозначное указание на вероятную цель атаки, и последующие исследования только подтвердили эту версию. За период ее активности количество жертв оценивается от 100 тыс. до 300 тыс. заражений. Статистика показала, что больше всего зараженных вирусом компьютеров — почти 60% — расположено в Иране (см. рис. 1): более 60 тыс. компьютеров к сентябрю 2010 года. Кроме того, оказалось, что большая часть пораженных компьютеров использует в своей работе программное обеспечение Sematic Step 7, разработанное компанией Siemens AG.[49]

Эксперты Symantec выявили, что изначально ВП была направлена против пяти организаций, каждая из которых имеет представительство в Иране.[50] Широкую огласку приобрели инциденты на АЭС в Бушере, что, по их мнению, привело к сбою в работе систем управления станции, а также на заводе по обогащению урана в Натанзе, когда большое количества центрифуг были введены одновременно в резонансную частоту (в нормальном режиме центрифуги вводятся в резонансную частоту последовательно). По мнению физиков, при определенных условиях это могло привести и к серьезной аварии.

Рисунок 1.
Доля зараженных ВП Stuxnet компьютеров в разных странах мира



Источник: N. Falliere, L. O Murchu, Er. Chien. W32.Stuxnet Dossier (version 1.4) // Symantec Corporation. — 2011. February. P. 6.

[49] Chien Eric. Stuxnet: A Breakthrough. Symantec Blogs. 2010, November 12. (http://www.symantec.com/connect/blogs/stuxnet-breakthrough).
[50] N. Falliere, L. O Murchu, Er. Chien. W32.Stuxnet Dossier (version 1.4) // Symantec Corporation. — 2011. February. P. 7.

Duqu — компьютерный сетевой «червь», вредоносная троянская программа, атаковавшая платформы Windows и предназначенная для кибершпионажа. Собирала информацию о системе, снимала скриншоты, искала файлы, перехватывала пароли. Распространялась посредством электронной почты, т.е. путем социальной инженерии. Свое название получила из-за префикса «~DQ», который использовался в именах всех создаваемых им файлов.[51]

ВП Duqu зарегистрирована Лабораторией Касперского в середине апреля 2011 года.[52], однако ее первое появление специалисты относят к 2008 году. Программа неактивна с 2012 года. Анализом кода ВП занимались Лаборатория криптографии и системной безопасности (CrySyS) Будапештского университета технологии и экономики, «Лаборатория Касперского», компания Symantec и другие специалисты. Эксперты отметили связь кодов, структуры и философии построения ВП *Duqu* и *Stuxnet*. При этом программы были написаны на одной и той же платформе «Тильда» (названной так, поскольку большинство ее файлов начинаются со значка тильды ~). Сотрудник «ЛК» Райан Нарейн отметил, что *Duqu*, вероятно, был создан для шпионажа за иранской ядерной программой.[53] Среди атакованных стран были Иран, Судан, Франция, Венгрия, Австрия, Индонезия, Великобритания, однако большая часть зарегистрированных целенаправленных заражений ВП *Duqu* произошла также в Иране (см. рис. 2), а основной целью были данные о системах управления производством в различных отраслях промышленности и о торговых отношениях ряда организаций ИРИ.

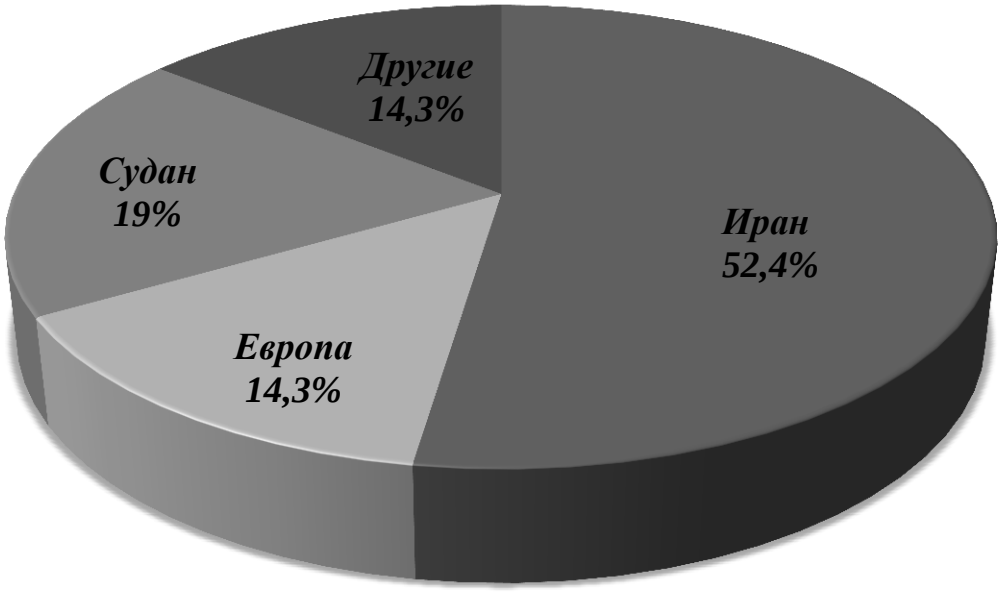
Кроме того, в отличие от *Stuxnet*, который поразил множество систем, но искал одну-единственную цель, *Duqu* поражает очень небольлшое число очень специфических объектов по всему миру, но при этом может использовать совершенно разные модули для каждой из них.

В марте 2012 года в СМИ появились сообщения о некой ВП, которая, предположительно, стерла данные с жестких дисков компьютеров в здании Министерства нефти ИРИ. ***Программа*** была названа ***Wiper***. После ее массовой атаки 22 апреля 2012 года, иранские власти приняли решение об отключении всех нефтебаз от Интернета.[54] В то же время отмечалось, что нефтедобывающая индустрия не была затронута кибератакой, т.к. она остается преимущественно механической.

Эксперты «ЛК» считают, что *Wiper* может быть связана с израильскими разработчиками. Она создавала и удаляла ключ реестра, ссылавшийся на службу модуля *Rahdaud64*, название которого, предположительно, образовано от имени великого библейского царя Давида (דָּוִד, в арабской традиции — Daud), при котором Древний Израиль присоединил наибольшее количество территорий, и прилагательного Rah (רָע), в переводе с иврита означающего «злой, плохой, вредоносный».

[51] Хроника целевых кибератак. Kaspersky Lab ZAO/. (https://apt.securelist.com/ru/#secondPage/attack=26).
[52] Гостев А. Тайна Duqu. // Все об интернет-безопасности. — 2011. Октябрь, 20. (http://www.securelist.com/ru/blog/40797/Tayna_Duqu_chast_pervaya).
[53] Ryan Naraine. Duqu First Spotted as 'Stars' Malware in Iran // Все об интернет-безопасности. — 2011. November, 5. (http://www.securelist.com/en/blog/208193211/Duqu_First_Spotted_as_Stars_Malware_in_Iran).
[54] Th. Erdbrink. Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet // The New York Times. — 2012. April, 23. (http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=2&.).

Рисунок 2.
Географическое распределение инцидентов заражения ВП Duqu в мире



Источник: Ромашкина Н. Махукова А. Компьютерная вредоносная атака на ядерную программу Ирана// Информационные войны. 2013. № 4.

В ходе анализа кода *Wiper* в «ЛК» пришли к выводу, что эта ВП ответственна за удаление конфиденциальных данных с компьютеров правительства Ирана и использует платформу «Тильда», также как *Stuxnet* и *Duqu*. В ходе расследования инцидента была найдена еще одна ВП, получившая название ***Flame***. Сообщения об ее обнаружении поступили из разных источников в апреле – мае 2012 года, первое появление специалисты относят к 2007 году. Сразу же были отмечены детали сходства между *Flame* и ранее известными *Stuxnet* и *Duqu* – это география атак и узкая целевая направленность в сочетании с использованием специфических уязвимостей в программном обеспечении.

Flame — троянская программа, бэкдор, имеющий черты, свойственные червям, созданный для кибершпионажа. Может записывать аудио с помощью микрофонов, подключенных к компьютеру, делать скриншоты, следить за клавиатурой и сетевым трафиком. Контролируется оператором и может распространяться по локальной сети или через съемные носители. Свое имя эта программа получила по названию одного из модулей, отвечающих за проведение атак и заражение новых компьютеров. Flame также известна как *Flamer*.[55] Программа неактивна с 2012 года.

Функционал *Flame* довольно разнообразен, однако сводится к хищению данных и организации массовой слежки. ВП была предназначена для автоматического сбора всевозможных данных с зараженных компьютеров, от документов до скриншотов, а также для перехвата нажатий клавиш и захвата аудио, что позволяет получить доступ к электронным письмам, документам, сообщениям и разговорам, в том числе на территории

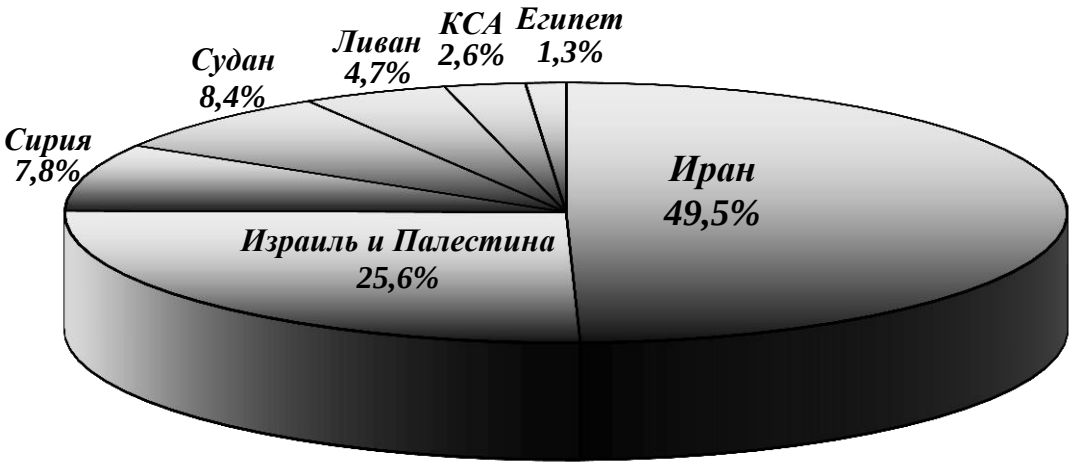
[55] См. подробнее на сайте «Все об интернет-безопасности». (http://www.securelist.com/ru/).

секретных объектов. Специалисты классифицируют *Flame* в качестве комплексной платформой для кибератак.

Flame – одна из первых вредоносных программ, в которой был реализован механизм заражения не подключенных к Интернету компьютеров через USB-накопители («флешки»). При подключении «флешки» к зараженному компьютеру, не подключенному к Интернету, ВП сохраняла украденную информацию на «флешке» в скрытом файле. Он был невидим для большинства файловых менеджеров и содержал до 16 Мб украденных документов и других данных с компьютера жертвы. Когда такая «флешка» подключалась к компьютеру, зараженному Flame и имеющему Интернет-доступ, данные с нее пересылались на командные серверы зловреда.

Распространение *Flame* происходило в странах Ближнего Востока: ИРИ, Израиле, Палестине, Судане, Сирии, Ливане, Саудовской Аравии и Египте, однако наиболее активной атаке подвергся Иран (см. рис. 3). Активность Flame также замечена в Европе и Северной Америке.

Рисунок 3.
Географическое распределение инцидентов заражения ВП Flame в мире



Источник: Ромашкина Н. Махукова А. Компьютерная вредоносная атака на ядерную программу Ирана// Информационные войны. 2013. № 4.

Специалисты «ЛК» считают, что и спустя 3 года *Flame* оценивается в качестве особенной угрозы – одной из самых сложных, неожиданных и продвинутых среди известных вредоносных кампаний.[56]

После обнаружения *Flame* Лаборатория Касперского обнаружила на Ближнем Востоке в 2012 году ещё две сложные вредоносные программы из того же семейства – ***Gauss*** и ***MiniFlame***. Сходства прослеживаются в архитектуре, модульной структуре, а также способах связи с серверами управления. Это еще раз доказывает, что есть ещё много неизвестного пока вредоносного программного обеспечения (ПО), на обнаружение которого уйдут многие годы.

[56] Мари-Бет Самех. Уроки Flame: три года спустя. Июнь 8, 2015. (https://securelist.ru/blog/mneniya/25876/uroki-flame-tri-goda-spustya/).

Троянская программа *Gauss* была обнаружена в ходе масштабной кампании, инициированной Международным союзом электросвязи (International Telecommunication Union, ITU) после выявления *Flame*. Эксперты отнесли ее к классу кибероружия. Особенность новой ВП, названной по имени немецкого математика Иоганна Карла Фридриха Гаусса, состоит в том, что она, помимо шпионского функционала, направлена на кражу финансовой информации пользователей зараженных компьютеров. ВП скрытно пересылает на сервера управления пароли, введенные или сохраненные в браузере, файлы cookie, а также подробности конфигурации инфицированной системы. Наличие функционала банковского троянца является уникальным случаем, ранее никогда не встречавшимся среди вредоносных программ. Проведенное исследование показало, что первые случаи заражения Gauss относятся к сентябрю 2011 года. Однако командные сервера вредоносной программы прекратили свою работу только в июле 2012 года. Gauss похищала конфиденциальную информацию у клиентов ряда ливанских банков, таких как Bank of Beirut, EBLF, BlomBank, ByblosBank, FransaBank и Credit Libanais. Кроме того, его целью являлись клиенты Citibank и пользователи электронной платежной системы PayPal.

В ходе исследования кода и версий ВП Flame эксперты «ЛК» обнаружили программу, которую изначально они сочли модулем Flame. Анализ показал, что это отдельная ВП - бэктор, которая получила название miniFlame.[57] Программа базировалась на платформе Flame и была предназначена для хищения данных, однако, по выражению исследователей «ЛК», является «инструментом для хирургически-точных атак», т.к. развертывалась лишь на очень небольшом числе компьютеров жертв «высокого ранга».[58] MiniFlame была обнаружена в Иране, Кувейте, Катаре, Ливане и Палестине, однако четкой географической привязки он не имеет.[59]

В «ЛК» сравнивают *Stuxnet* с ракетой. При этом ее разгонный модуль — тело компьютерного «червя» — было использовано в *Duqu*, а «боеголовка» могла быть оборудована дополнительно для воздействия на определенную цель (в случае *Stuxnet* – это блок, одновременно вводящий в резонансную частоту большое количество центрифуг). В Symantec также считают, что *Duqu* была заготовкой для осуществления атаки типа *Stuxnet*. Исходя из этого, был сделан вывод, что *Duqu* и *Stuxnet* были параллельными проектами, за созданием которых стоит одна группа либо сотрудничающие команды чрезвычайно квалифицированных профессионалов, обладающих обширными ресурсами и существенной финансовой поддержкой. В «ЛК» пришли к мнению, что программа создана при поддержке госструктур.[60]

Кроме того, все применяемые в Иране ВП связаны, причем их можно разбить на две группы: *Stuxnet, Duqu* и *Wiper* работают на платформе «Тильда», а *Flame, Gauss, miniFlame* и *Narilam* – на платформе Flame, причем разработчики двух платформ сотрудничали друг с другом. В то же время, эти ВП делятся по функционалу – часть из них шпионят за зараженным пользователем, часть стирает информацию с зараженного компьютера, а *Stuxnet* выводит из строя промышленное оборудование. При этом атаки *Stuxnet, Gauss* и *Flame* были обширными, а *Duqu* и *miniFlame* – тонко настроенными на определенную жертву. Об этом свидетельствуют и данные об общем количестве зарегистрированных инцидентов указанными ВП, представленные в таблице 1 (речь идет о приблизительном числе, т.к. мнения специалистов по этому вопросу неоднозначны). Все это позволило говорить о

[57] Полный анализ командных серверов Flame / Все об интернет-безопасности. — 2012. Сентябрь, 17. (http://www.securelist.com/ru/blog/207764193/Polnyy_analiz_komandnykh_serverov_Flame).
[58] miniFlame, он же SPE: «Элвис и его друзья» / Все об интернет-безопасности. — 2012. Октябрь, 15. (http://www.securelist.com/ru/blog/207764257/miniFlame_on_zhe_SPE_Elvis_i_ego_druzya).
[59] Там же.
[60] Kaspersky Lab provides its insights on Stuxnet worm // Kaspersky Lab. — 2010. September, 24. (http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm).

комплексном применении этих ВП не просто как о примере киберпреступности, а как о кибероружии и кибервойне.

Таблица 1.
Приблизительное общее число случаев заражения вредоносными программами Stuxnet, Gauss, Flame, Duqu и miniFlame в мире

Название ВП	Число инцидентов
Stuxnet	*100001- 300000*
Gauss	*Около 10000*
Flame	*500-1000*
Duqu	*11-100*
miniFlame	*50-60*

Источники: Хроника целевых кибератак. Kaspersky Lab ZAO/ (https://apt.securelist.com/ru/#secondPage/attack=26).
MiniFlame, он же SPE: «Элвис и его друзья» / Все об интернет-безопасности. — 2012. Октябрь, 15.
(http://www.securelist.com/ru/blog/207764257/miniFlame_on_zhe_SPE_Elvis_i_ego_druzya).

В 2011 году в СМИ были названы и конкретные государства-заказчики: Израиль и США. *The New York Times* опубликовала данные о том, что в израильской пустыне Негев, где, предположительно, находится исследовательский ядерный центр, была построена точная копия обогатительного завода в Натанзе, чтобы испытывать на ней кибероружие *Stuxnet*.[61] При этом указывалось, что в работе принимали участие не только израильские, но и американские специалисты. Примечательно, что одним из авторов статьи выступил шеф Вашингтонского бюро газеты Дэвид Сангер – автор книги «Конфронтация и сокрытие: тайные войны Обамы и удивительное использование американской мощи», вышедшей в свет в июне 2012 года. В ней раскрывается существование плана, включающего кибератаки на иранские промышленные системы, разработанного в США еще во время президентства Дж. Буша-младшего.[62]

Подозрения в том, что Израиль может начать кибервойну против Ирана, появились еще в 2009 году, когда эксперт из исследовательского института США *Cyber Consequences Unit* С. Борг заявил, что на чувствительных к вмешательству иранских предприятиях – таких как завод по обогащению урана – может быть применена какая-либо ВП.[63] После раскрытия существования *Stuxnet* С. Борг подтвердил, что Израиль обладает возможностями для создания таких программ.[64] Кроме того, на церемонии проводов уходящего с поста главы Армии обороны Израиля Габи Ашкенази в феврале 2011 года был показан видеосюжет, в

[61] Broad, W. J., Markoff, J. and Sanger, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. — 2011. January 15. (http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html).
[62] Sanger, D. E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power // Crown Publishers. — New York. — 2012.
[63] Williams, D. Wary of naked force, Israelis eye cyberwar on Iran // Reuters Analisys. — 2009. July 7. (http://www.reuters.com/article/2009/07/07/idUSLV83872).
[64] A worm in the centrifuge: An unusually sophisticated cyber-weapon is mysterious but important // The Economist. — 2010. September 30. (http://www.economist.com/node/17147818).

котором среди оперативных успехов генерала указывался и *Stuxnet*.[65]А в декабре 2011 года в интервью журналу «*IEEE Spectrum»* известный программист Ларри Константин подтвердил, что основным подозреваемым в разработке вируса по-прежнему считается Израиль.[66] В июле 2013 года бывший сотрудник Агентства национальной безопасности США Эдвард Сноуден заявил, что *Stuxnet* является совместной разработкой США и Израиля.[67]

Официальный Иран не сразу подтвердил заражение компьютеров внутри страны. Только в сентябре 2010 года глава Совета по информационной технологии министерства промышленности Ирана Махмуд Лиайи заявил, что заражению в ИРИ подверглись около 30 тыс. компьютеров. Официальное новостное агентство IRNA процитировало слова руководителя проекта Бушерской АЭС Махмуда Джафари о том, что *Stuxnet* поразил некоторые персональные компьютеры сотрудников станции. Однако арабоязычный телеканал Al-Alam показал его интервью с противоположной информацией: «Вирус не причинил никакого вреда главным системам Бушерской АЭС. Все компьютерные программы на станции работают в штатном режиме».[68] Информацию об этом подтвердил замглавы ОАИЭ по вопросам защиты и обеспечения безопасности Ашгар Зареан: «Мы предприняли собственное расследование и не нашли следов проникновения вируса в наши системы»[69]. В конце сентября 2010 года глава ОАИЭ Али Акбар Салехи заявил, что персональные компьютеры сотрудников станции были очищены от ВП *Stuxnet*.[70] В начале октября того же года министр разведки и национальной безопасности ИРИ Хейдар Мослехи объявил об аресте «нескольких» шпионов, следивших за ядерными объектами. Он также заявил, что «враги разработали и запустили через Интернет компьютерных «червей», которые могли бы подорвать ядерную программу Ирана»[71]. При этом сами эти объекты не назывались. А в конце ноября 2010 года президент Ирана Махмуд Ахмадинежад признал, что предприятие по обогащению урана подверглись кибератаке[72], не уточняя ни само предприятие, ни орудие нападения.

Летом 2012 года власти Ирана сообщили о планах создания собственного национального интернета.[73] От обычного интернета начали отключать компьютеры в министерствах и на госпредприятиях. По словам министра информационных технологий и коммуникаций ИРИ Резы Тагипура, такая сеть поможет решить проблемы безопасности. По мнению представителей неправительственной организации Freedom House, такие меры являются следствием иранской политики ужесточения в отношении глобальной сети[74], однако можно предположить, что пойти на такой шаг власти ИРИ заставили именно кибератаки, таких ВП как *Wiper*, которая стерла данные с компьютеров иранского правительства.

---

[65] Williams, Ch. Israel video shows Stuxnet as one of its successes // The Daily Telegraph. — 2011. February 15. (http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes).

[66] St. Cherry, with L. Constantine. Sons of Stuxnet // IEEE Spectrum “Techwise Conversations”. — 2011. December 14. (http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet).

[67] «Первое кибероружие» поразило ядерный объект. 11 ноября 2013. (http://internetua.com/pervoe-kiberorujie--porazilo-yadernii-ob-ekt).

[68] Бушерская АЭС в Иране подверглась кибератаке / Русская служба BBC. (http://www.bbc.co.uk/russian/international/2010/09/100926_iran_virus.shtml).

[69] L. Maillard. Iran denies nuclear plant computers hit by worm / AFP. — 2010. September, 26. (http://www.google.com/hostednews/afp/article/ALeqM5izMHSVD4tEUYpQJa7iGAp5vJyTUw).

[70] Сотрудники АЭС в Бушере очистили систему от компьютерного вируса / РИА «Новости». — 2010. Сентябрь, 29. (http://ria.ru/science/20100929/280467410.html).

[71] Iran nabs several 'nuclear spies' / Press TV. — 2010. October 2. (http://www.presstv.ir/detail/144871.html).

[72] Iran says cyber foes caused centrifuge problems / Reuters. — 2010. November, 29. (http://www.reuters.com/article/2010/11/29/iran-ahmadinejad-computers-idAFLDE6AS1L120101129).

[73] Iran to launch national data network / Press TV. — 2011. August 10. (http://www.presstv.ir/detail/193306.html).

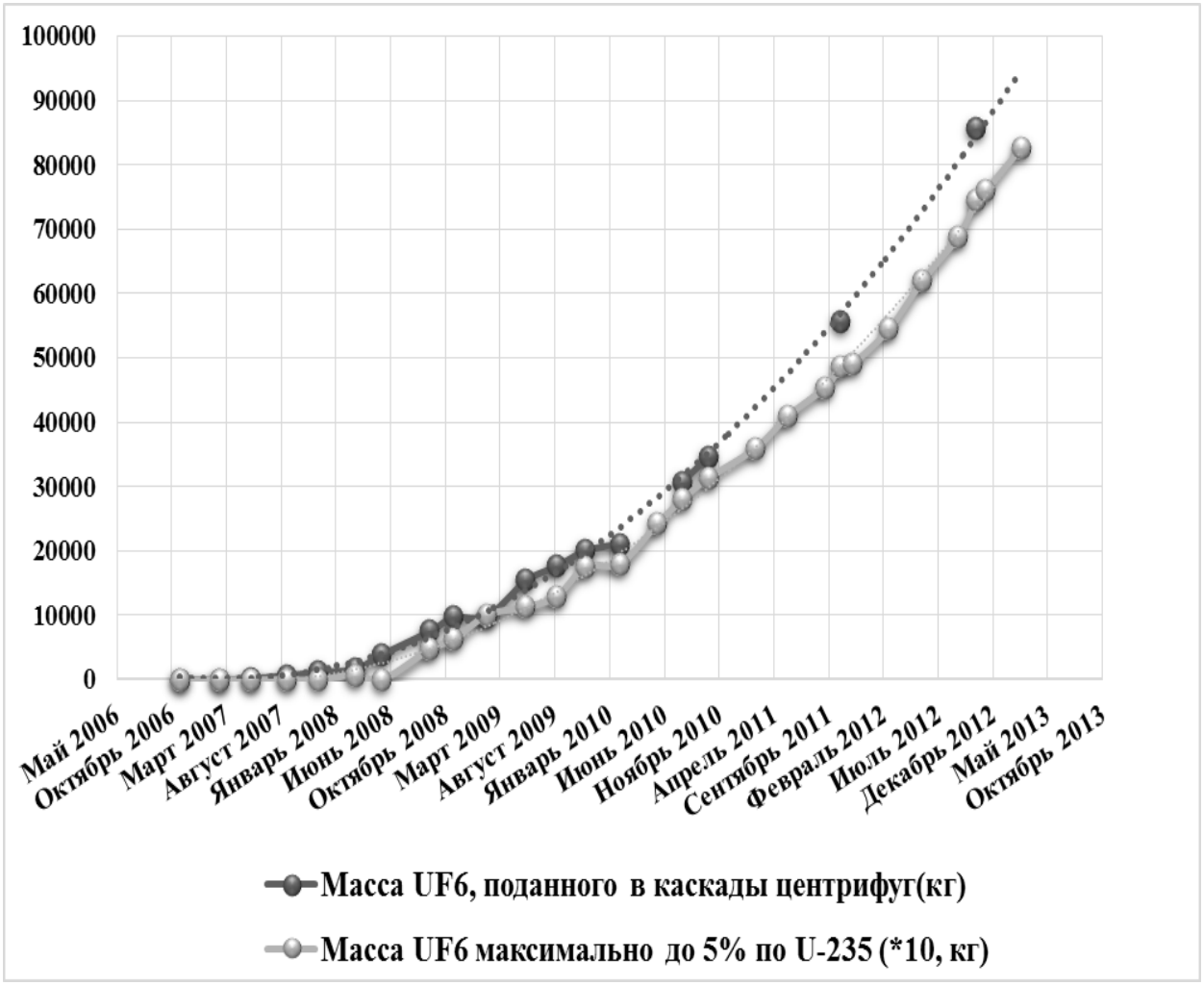
[74] Kelly, S., Cook S., Truong, M. Freedom On the Net 2012. A Global Assessment of Internet and Digital Media // Freedom House. — 2012. — September 24. P. 269.

По словам немецкого IT-специалиста Ральфа Лангера, применение ВП оказалось по эффективности сравнимо с полноценной военной операцией, но при отсутствии человеческих жертв. В частности, все зараженные *Stuxnet* иранские компьютеры подлежали уничтожению, т.к. избавиться от вируса крайне сложно, необходимо починить центрифуги на предприятии в Натанзе и, возможно, купить новую турбину для бушерской АЭС.

Однако точной информации о физическом вреде, нанесенном ядерным объектам ИРИ вредоносными программами, до сих пор нет.

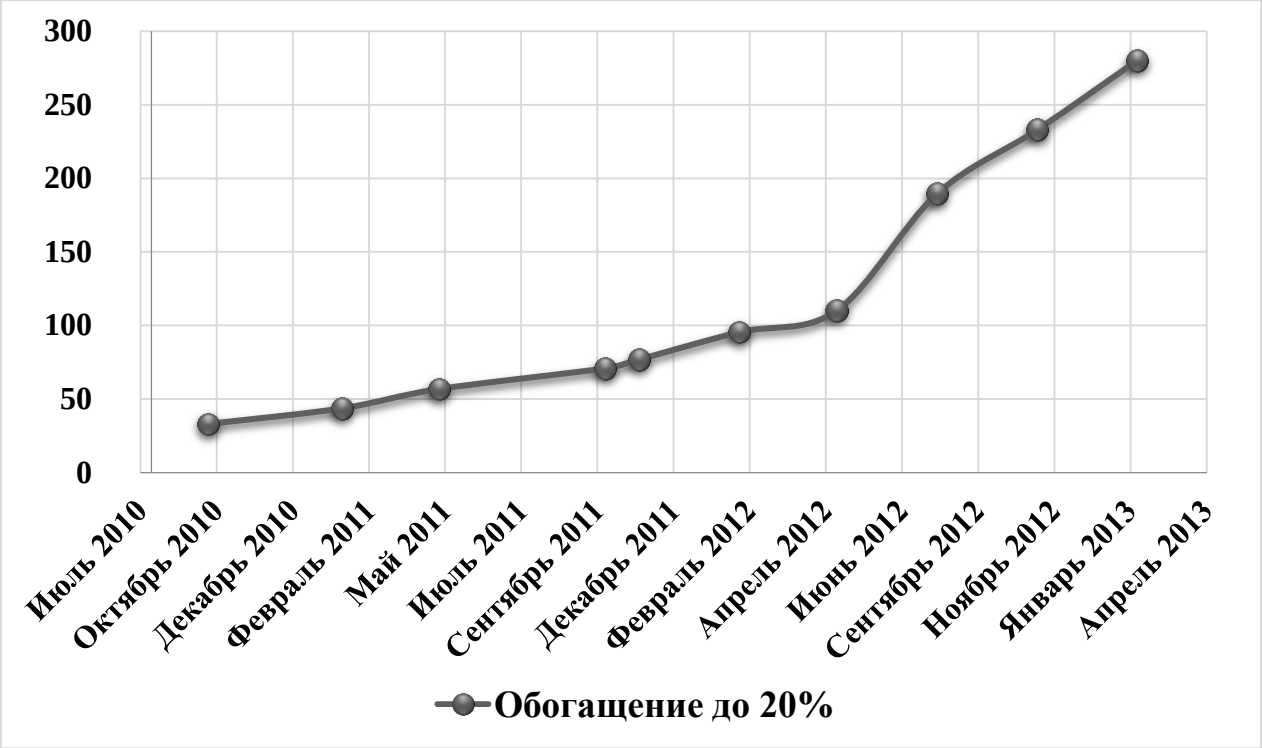
Анализ данных МАГАТЭ показывает, что количество урана, обогащенного на заводе в Натанзе в период 2007-2013 годов, стабильно росло. Более того, обогащение урана до 20% началось сразу после кибератаки – в июле 2010 года (см. рис. 3 и 4). Поэтому вполне возможно, реальный физический ущерб был не столь значительным. Тогда нельзя исключать, что заявление властей Ирана о том, что некий вирус повредил предприятие по обогащению урана, было сделано лишь для отвода глаз: так они могли бы добиться смягчения позиции западных стран на переговорах «шестерки» по ядерной программе ИРИ.

Рисунок 3.
Масса урана UF6, обогащенного на заводе в Натанзе (2006 – 2013 годы)



Источник: IAEA Reports // Сайт МАГАТЭ. (http://www.iaea.org/newscenter/focus/iaeairan/iaea_reports.shtml).

Рисунок 4.
Масса урана, обогащенного до 20% на заводе в Натанзе (в кг) (2010 – 2013 годы)



Источник: IAEA Reports // Сайт МАГАТЭ. (http://www.iaea.org/newscenter/focus/iaeairan/iaea_reports.shtml).

С другой стороны, Иран мог скрыть реальный ущерб и затаиться, чтобы создать собственную киберармию – в настоящее время уже достаточно информации в пользу этой версии. Подтвердили ее и в Иране: еще в декабре 2011 года замглавы Генштаба ВС ИРИ по вопросам культуры и связей с общественностью Массуд Джазайери заявил о создании штаба по ведению «мягкой войны».[75] А в феврале 2012 года глава Организации пассивной обороны Ирана генерал Голамреза Джалали сообщил о формировании штаба по противодействию кибернетическим угрозам и о намерении основать первую в истории Ирана киберармию[76], на что планировалось потратить около $1 млрд.[77]

Отметим, что неофициальная «иранская киберармия», состоящая, по всей видимости, из т.н. хактивистов[78] существовала еще в 2009 году, когда хакерам удалось взломать сервис микроблогов Twitter[79]: в течение нескольких часов на главной странице сайта висело изображение зеленого флага с надписью на фарси и заявлением о вмешательстве США в

[75] Jazayeri: Soft war headquarters established by Iranian Armed Forces / IRNA. — 2011, December 1. (http://www.irna.ir/en/News/80437009/Politic/Jazayeri__Soft_war_headquarters_established_by__Iranian_Armed_Forces).
[76] Iran set to build first cyber army / Press TV. — 2012. February 20. (http://www.presstv.ir/detail/227739.html).
[77] Katz, Y. Iran embarks on $1b. cyber-warfare program / The Jerusalem Post. — 2011. December, 18. (http://www.jpost.com/Defense/Article.aspx?id=249864).
[78] Хактивизм — сетевая активность хакеров, выражающаяся в форме акций прямого действия. Фр. Паже «Хактивизм. Киберпространство стало новой средой для выражения политических взглядов». (http://www.mcafee.com/ru/resources/white-papers/wp-hacktivism.pdf.).
[79] Arrington, M. Twitter Hacked, Defaced By "Iranian Cyber Army" / TechCrunch. — 2009. — December 17. (http://techcrunch.com/2009/12/17/twitter-reportedly-hacked-by-iranian-cyber-army/).

дела ИРИ с электронным почтовым адресом Iranian.Cyber.Army@gmail.com. В январе 2010 года та же группировка атаковала китайскую поисковую систему Baidu – на этот раз на главной странице сайта появился иранский флаг на черном фоне, надпись на фарси и на английском о том, что сайт атакован «иранской кибермией».[80]

В любом случае иранский инцидент является показательным примером кибервойны, в ходе которой было применено полноценное кибероружие. Опыт его применения, безусловно, учтен и нападающей стороной для проведения других подобных операций, и Ираном, о чем свидетельствуют изменения в развитии иранской ядерной проблемы, начиная с 2013 года.

В настоящее время источники ВП существуют практически в каждой стране, однако более 80% всех площадок, используемых для распространения «зловредов», не протяжении длительного периода расположены всего в нескольких государствах: США, РФ, Нидерланды, Германия, Великобритания, Украина, Франция, Китай, Испания, Швейцария, Латвия, Швеция.[81]

Сегодня уже существует целый класс программного обеспечения, которое специалисты оценивают как «кибероружие». К нему относят ВП, созданные и профинансированные государственными структурами, которые могут применяться против граждан, важных стратегических объектов, организаций и государственных ведомств и способны привести к настоящей реальной войне. Можно выделить три основные группы угроз в этой категории.

«Разрушители» **–** программы, предназначенные для уничтожения баз данных и информации в целом, могут быть реализованы в виде «логических бомб», либо заранее внедренных в системы и срабатывающих в определенный момент времени, либо в ходе целенаправленной атаки с моментальным исполнением. Наиболее показательным примером подобной ВП является *Wiper*.

Шпионские программы – ВП (*Flame, Gauss, Duqu, miniFlame)*, целью которых является сбор информации (например, данные проектов Autocad, SCADA-систем и т.д.), которая затем может быть использована для создания других групп угроз.

Инструменты кибердиверсии – высшая форма кибероружия, в результате действий которых объекту наносится физический ущерб. В эту категорию попадает «червь» *Stuxnet*. Этот вид угроз является уникальным, и его применение видится достаточно редким явлением, однако с каждым годом все больше и больше усилий разных государств направлены как на разработку именно такого вида оружия, так и создание защиты от них.

[80] Baidu hacked by “Iranian cyber army” / BBC News. — 2010. — January 12. (http://news.bbc.co.uk/2/hi/8453718.stm).

[81] См. (https://securelist.ru/analysis/malware-quarterly/25544/razvitie-informacionnyx-ugroz-v-pervom-kvartale-2015-goda/).

3.2. Индийская политика противодействия угрозам в кибернетическом пространстве

Хотя Индия сталкивается с угрозами в кибернетическом пространстве (КП) с конца прошлого века, долгое время она уделяла им недостаточное внимание. Лишь в 2012 году, когда серия широкомасштабных кибератак были предприняты против гражданских и военных объектов Индии, власти страны предприняли серьезные шаги по обеспечению кибербезопасности.

Основные направления политики Индии в КП были определены в документе «Национальная политика в области кибернетической безопасности» (National Cyber Security Policy), принятом в 2013 году. Однако реализация этой политики все еще не соответствует тому уровню угроз, с которыми сталкивается Индия. Это является причиной острой озабоченности как в Индии, так и в государствах-партнерах этой страны, прежде всего, в России.

Индия пытается разработать политику информационной безопасности в соответствии с угрозами, с которыми она все чаще сталкивается в настоящее время. Эти угрозы можно разделить на кибератаки и враждебные акции в информационной среде. В первом случае основным орудием злоумышленников становятся вредоносные программы, во втором – информация, нацеленная на получение той или иной реакции в обществе. За этими атаками в обоих случаях стоят зарубежные хакерские группы, которые, как правило, ассоциированы с государственными специальными службами. Индийский ответ на рост опасностей в киберпространстве не носит комплексный характер. Он не адекватен масштабу угроз. Очевидно в ближайшее время Индия будет вынуждена уделить значительно большее внимание информационной безопасности.

Основные угрозы в кибернетическом пространстве

В последние годы в Индии все большее внимание уделяется угрозам преступлений, терроризма и шпионажа в КП, т.е. всему тому, что может быть объединено понятием «угрозы в кибернетическом пространстве». Они могут наносить ущерб национальной безопасности Индии, подрывать политическую и финансово-экономическую систему, воздействовать на общественно-политическую ситуацию в стране. Вероятный противник может предпринимать комплекс мер в КП, которые могут восприниматься как акт агрессии.

Даже на официальном уровне в Индии признается неразвитость наступательных и оборонительных средств страны в КП.[82] Это подтверждается рядом фактов.

Так, летом 2012 года стало известно о том, что хакерам удалось получить доступ к данным компьютеров на объектах Военно-морских сил (ВМС) в Висакхапатнаме, где располагается штаб Восточного командования ВМС, отвечающий за направление, на котором интересы Индии наиболее явно пересекаются с интересами Китая. Кроме того, Восточное командование проводит испытания первой индийской атомной подводной лодки (АПЛ) «Арихант». В Висакхапатнаме находятся судоверфи, на которых строятся вторая («Аридхаман»), третья (S-4) и четвертая (S-5) АПЛ.[83] Там же планируется строительство подземной базы для АПЛ.

[82] National Cyber Security Policy – 2013 // Department Of Electronics & Information Technology, Government Of India. (http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf).

[83] Pandit R. Post-accident, lens on nuclear submarine projects // Times of India. – Mar. 10, 2014. (http://timesofindia.indiatimes.com/india/Post-accident-lens-on-nuclear-submarine-projects/articleshow/31758017.cms);

В результате заражения вирусами собирались секретные данные и отправлялись на китайские IP адреса. Расследование показало, что утечка секретных данных стала возможной из-за нарушений, допущенных рядом офицеров. Они использовали зараженные вирусом «флэшки» для переноса файлов *на* и *с* компьютеров с секретной информацией, которые, в соответствии с правилами безопасности, не имели выхода в интернет. После присоединения «флэшки», вирус находил необходимые файлы по заданным ключевым словам и копировал их в скрытую папку на носителе, с которого эти файлы отправлялись на адреса в другой стране после его подключения к компьютеру, имевшему выход в интернет.[84]

В середине июля 2012 года, примерно через две недели после утечки данных из Висакхапатнама, стало известно, что взломана электронная почта нескольких высокопоставленных членов индийского правительства. Дальнейшее расследование показало, что были взломаны около 12 тыс. аккаунтов электронной почты. Эта атака коснулась министерств иностранных дел, внутренних дел, обороны, Организации оборонных исследований и разработок (Defense Research and Development Organization), Индо-тибетской пограничной полиции и была направлена на серверы Национального центра информатики (National Informatics Centre), который обслуживает все государственные ведомства. По оценкам Национальной организации технических исследований (National Technical Research Organization, далее НОТИ) при индийском Совете национальной безопасности, данная масштабная атака была направлена против государственной инфраструктуры с целью получения секретной информации.[85] Кстати, НОТИ является индийской службой научно-технической разведки, к сфере деятельности которой относятся кибернетические вопросы.

Уязвимость Индии в киберпространстве может быть обусловлена не только несоблюдением правил безопасности, неразвитостью системы мониторинга и оборонительных средств, но и проблемами, связанными с импортом и использованием программного обеспечения и телекоммуникационного оборудования зарубежного производства.

В 2011 году стало известно, что НОТИ закупила у индийской корпорации «Бхарат электроникс лимитед» (Bharat Electronics Ltd., БЭЛ) системы шифрования, не представив их на предварительное рассмотрение в Комитет шифровальной политики, утверждающий приобретение всего аппаратного и программного обеспечения, связанного с обеспечением коммуникаций в правительственных учреждениях. При этом в 2009 году НОТИ и БЭЛ уже пытались поставить те же самые системы шифрования в военно-воздушные силы (ВВС). Но ВВС направили их в профильный Комитет, который обнаружил, что в основе данных систем лежит китайское программное обеспечение, содержащее к тому же серьезные недостатки.

Комитет шифровальной политики известил о происшествии секретариат Совета национальной безопасности, который, в свою очередь, установил, что НОТИ успел поставить шифровальные системы, произведенные компанией БЭЛ, на сумму 400 млн. рупий. Впоследствии Комитет запретил использование этих систем.[86] Насколько известно, ни в НОТИ, ни в БЭЛ никто не понес ответственности за неоднократные попытки поставить продукт, использование которого могло вызвать проблемы для национальной безопасности.

INS-Aridhaman mishap: Submarine safe; DRDO orders immediate inquiry // Daily Bhaskar. – Mar. 9, 2014 (http://daily.bhaskar.com/news/NAT-TOP-shocking-one-civilian-worker-two-others-injured-in-nuclear-submarine-mishap-in-v-4544815-NOR.html).

[84] Pubby M. China hackers enter Navy computers, plant bug to extract sensitive data // The Indian Express. – Jul. 1, 2012. (http://archive.indianexpress.com/news/china-hackers-enter-navy-computers-plant-bug-to-extract-sensitive-data/968897/0).

[85] Saksena A.R. India Scrambles on Cyber Security // The Diplomat. - Jun. 18, 2014. (http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/).

[86] Indian Commentary Discusses Security Agencies 'Failure' To Counter Terror Attacks // The Pioneer. - Nov., 26, 2011.

Атаки на компьютеры Восточного командования ВМС и массовый взлом почтовых аккаунтов государственных служащих связывается с деятельностью китайских спецслужб. В индийском случае для них характерен интерес к военным разработкам, развитию стратегических сил, состоянию индийских сил, используемых на китайском направлении и другим связанным вопросам.

Без сомнения, все перечисленные вопросы представляют интерес и для специальных служб другого вероятного противника Индии – Пакистана. Но, во-первых, Пакистан может не иметь тех технических возможностей в КП, которыми располагает Китай. Во-вторых, специальные службы Пакистана могут ставить иные акценты в своей деятельности против Индии. Помимо добычи секретной информации, Пакистан может быть заинтересован в подрыве политической и финансово-экономической системы Индии и в воздействии на ее общественно-политическую ситуацию.

Одним из наиболее распространенных способов подрыва различных систем Индии являются взломы правительственных сайтов. Наиболее дерзким стал взлом сайта индийского Центрального бюро расследований (ЦБР), предпринятый в декабре 2010 года хакерской группой «Пакистанская киберармия» (Pakistan Cyber Army, далее ПКА). Таким образом, эта группа отомстила за взлом 36 пакистанских сайтов, осуществленный «Индийской киберармией» (India Cyber Army) в память о террористическом нападении на Мумбаи в ноябре 2008 года, которое было организовано с территории Пакистана.[87]

Очевидно, между индийскими и пакистанскими хакерскими группами идет своеобразная дуэль. Однако, по индийским данным, активность индийских хакеров в разы уступает активности пакистанских.[88] Последним масштабным нападением пакистанских хакеров стал массовый взлом индийских сайтов 26 января 2014 года, когда Индия отмечает День Республики. По данным индийской прессы, были взломаны 2118 сайтов, по словам хакеров – 2618.[89] Атаке подверглись сайты Центрального банка Индии, Министерства железнодорожного сообщения, военизированного формирования «Ассамские стрелки» и др. Ответственность за взломы взяли на себя три хакерские группы: «MaXiMiZerS», «Пакистанские киберэксперты» (Pak Cyber Experts) и «Кашмирская киберармия» (Kashmir Cyber Army). Операция носила название «#OP26jan», цель которой заключалась в поддержке кашмирских сепаратистов.

В конце ноября 2014 года Рави Шанкар Прасад, министр коммуникаций и информационных технологий, привел официальные данные о десятках тысяч нарушений информационной безопасности (ИБ) в последние годы (см. рис. 1). Эти нарушения включают сетевое мошенничество («фишинг»), сканирование сайтов злоумышленниками, рассылка спама, применение вредоносных кодов, различные проникновения в сети и на сайты. Отдельно дана статистика по взломам сайтов.[90]

Цифры, приведенные министром Р.Ш. Прасадом, вызывают много вопросов. Например, почему до 2012 года взломов сайтов было больше, чем всех нарушений ИБ, включая незаконные проникновения на сайты? С чем связано падение количества взломов сайтов после 2013 года при стремительно растущем количестве всех нарушений ИБ?

---

[87] 36 government sites hacked by 'Indian Cyber Army' // The Express Tribune. - Nov. 30, 2010. (http://tribune.com.pk/story/83967/36-government-websites-hacked-by-indian-cyber-army/).

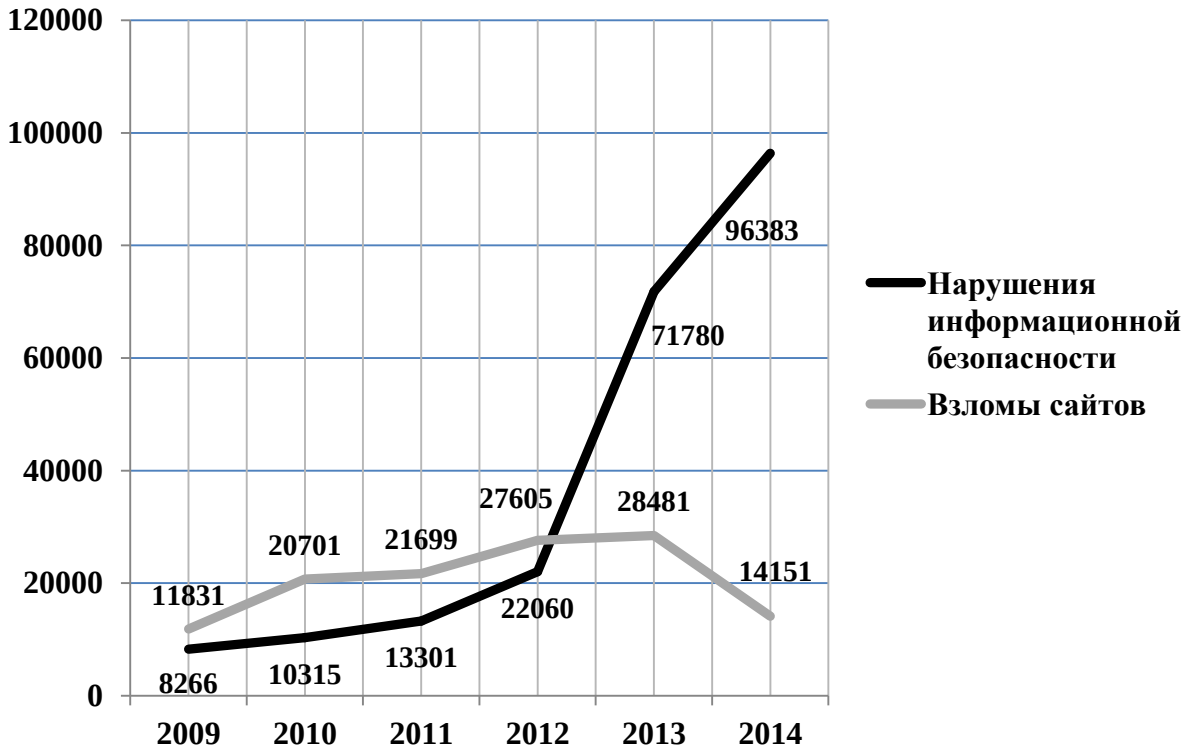
[88] Nanjappa V. Cyber war with Pak! Why India is the weaker side // Rediff News. - Aug. 21 – 2012. (http://www.rediff.com/news/report/cyber-war-with-pak-why-india-is-the-weaker-side/20120821.htm).

[89] Baloch F. Cyber warfare: Pakistani hackers claim defacing over 2,000 Indian websites // The Express Tribune. - Feb. 2, 2014. (http://tribune.com.pk/story/666537/cyber-warfare-pakistani-hackers-claim-defacing-over-2000-indian-websites/).

[90] Indian Cyber Security Violations Similar to Global Trends, Says Ravi Shankar Prasad // NDTV. - Nov. 28, 2014. (http://www.ndtv.com/article/india/indian-cyber-security-violations-similar-to-global-trends-says-ravi-shankar-prasad-627242?ndtv_alsoread).

Несмотря на явные противоречия в официальных данных, значительные масштабы угроз Индии в КП не вызывают сомнений, как и общая тенденция роста случаев кибератак на индийские объекты. При этом в отличие от атак, предпринимаемых с территории Китая, нападения с территории Пакистана нацелены не только на государственные организации. Существуют угрозы и для сфер телекоммуникационных и банковских услуг. Жертвами нападений часто становятся рядовые пользователи интернета и мобильной связи.

Рисунок 1.
Нарушения информационной безопасности Индии, 2009-2014 годы.



Среди других способов подрыва политической, финансово-экономической и общественно-политической системы Индии может быть распространение паники, радикальной или террористической идеологии среди населения. Во всех этих случаях наиболее эффективным средством для злоумышленников могут быть социальные сети. Так, во время индусско-мусульманских столкновений 2012 года в штате Ассам, были предприняты попытки вызвать панику у членов мусульманской общины в других штатах Индии. К примеру, среди жителей городов Мумбаи (штат Махараштра) и Бангалор (штат Андхра-Прадеш) распространялись сообщения о якобы массовых убийствах мусульман в Ассаме, сопровождавшиеся фальшивыми фотографиями. Для этого использовались службы коротких сообщений (СМС) и соцсети.[91] Эти попытки предпринимались с территории Индии и Пакистана.

Среди стран, с территории которых наиболее часто предпринимались атаки против Индии, лидирующие места занимают Алжир, Бангладеш, Бразилия, государства Европейского Союза, КНР, ОАЭ, Пакистан, США, Турция (даны в алфавитном порядке).

[91] Tiwary D. Indian Mujahideen stoked Assam violence in 2012, NIA says // The Times of India. – Mar. 10, 2014. (http://timesofindia.indiatimes.com/india/Indian-Mujahideen-stoked-Assam-violence-in-2012-NIA-says/articleshow/31759301.cms).

Среди групп – инициаторов атак, выделяются хакеры, связанные с правительствами и/или радикальными и террористическими организациями, а также с организованной преступностью.

Политика безопасности Индии в кибернетическом пространстве

Первоначально в Индии доминировал подход к обеспечению ИБ с акцентом на экономических аспектах, который был характерен для Закона об информационных технологиях (Information Technology Act), принятого в 2000 году.[92] Главная цель этого правового документа заключалась в упорядочивании и облегчении предпринимательской деятельности в КП. Поэтому в этом законе рассматривались преступления преимущественно экономического характера, а в парламентских дискуссиях о поправках к закону главное место занимали экономические вопросы.

Ситуация изменилась после террористического нападения на Мумбаи в ноябре 2008 года. 23 декабря того же года в закон были внесены поправки, которые сместили его акценты с экономических вопросов на обеспечение национальной безопасности. Вместе с тем, внесенные поправки вызвали серьезную критику в Индии, поскольку в новой версии закон создал основу для нарушения прав и ограничения свобод индийцев. После принятия поправок следственные органы активизировали деятельность в области кибепреступлений. Так, в 2011 году было заведено 1791 дел по обвинению в нарушении Закона об информационных технологиях, в 2012 году – 2876 дел, а в 2013 году – 4356. Часть из них классифицировалась в качестве уголовных преступлений в области КП: 422 в 2011 году (23,6% от всех дел), 601 в 2012 году (20,9%) и 1337 в 2013 году (30,7%).[93] Однако в 2010-2012 годах отношение количества обвинительных приговоров к общему числу рассмотренных дел составило всего 1%.[94] Это свидетельствует о несовершенстве индийского законодательства и недостаточных возможностях следственных органов в борьбе с киберпреступлениями.

Рост кибератак на Индию повлиял на изменение роли государственных организаций, в чью сферу ответственности входит киберпространство. Согласно проекту «Национальной политики в области кибернетической безопасности» 2011 году, в Индии существует около дюжины таких организаций.[95] В их число входят Национальный информационный совет во главе с советником премьер-министра по безопасности (National Information Board), Национальный комитет управления кризисными ситуациями (National Crisis Management Committee), Совет национальной безопасности, министерство внутренних дел, министерство обороны, включая Группу реагирования на компьютерные происшествия Армии (A-CERT) и Агентство исследований и обеспечения целостности оборонной информации (DIARA), Министерство коммуникаций и информационных технологий и созданная при нем Группа реагирования на компьютерные происшествия (CERT-In, ГРКП), Национальная организация технических исследований и сформированный при нем Национальный центр защиты ключевой информационной инфраструктуры (National Critical Information Infrastructure Protection Centre, НЦЗКИИ) и другие.

---

[92] The Information Technology (Amendment) Act, 2008 // Department Of Electronics & Information Technology, Government Of India. (http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf).

[93] CERT-In reports over 62,000 cyber attacks till May 2014 // Live Mint. - Jul. 14, 2014. (http://www.livemint.com/Politics/NNuFBA3F2iX4kxIXqKaX2K/CERTIn-reports-over-62000-cyber-attacks-till-May-2014.html?utm_source=copy).

[94] Nanjappa V. Cyber war with Pak! Why India is the weaker side // Rediff News. - Aug. 21 – 2012. (http://www.rediff.com/news/report/cyber-war-with-pak-why-india-is-the-weaker-side/20120821.htm).

[95] Discussion draft on National Cyber Security Policy // Department of Information Technology, Ministry of Communications and Information Technology. (http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf).

Среди названных организаций круглосуточный мониторинг угроз в КП ведется силами НЦЗКИИ и ГРКП. Причем, первый из них отвечает за угрозы в сфере безопасности, водоснабжения, государственных организаций, здравоохранения, космоса, обороны, приоритетных секторов промышленности, разведки, телекоммуникации, транспорта, финансов, электронного правительства, энергетики. Вторая несет ответственность за остальные направления, а также проводит общий мониторинг и делает ежедневные оповещения. В области надзора за деятельностью в КП главную роль играют Совет национальной безопасности и министерства коммуникаций и информационных технологий, внутренних дел и обороны.[96]

Недостатки индийской политики в области кибербезопасности

Принятая в 2013 году «Национальная политика в области кибернетической безопасности» предлагает рамки для обеспечения ИБ, снижая количество уязвимостей.[97] Для решения этой задачи предлагаются следующие шаги.

Во-первых, «Национальная политика в области кибернетической безопасности» делает акцент на научно-исследовательских работах, тестировании и развертывании систем безопасности.

Во-вторых, в документе содержится призыв развивать партнерские отношения между государственными и частными организациями и поощрять последних брать на вооружение лучшие практики в области кибербезопасности.

В-третьих, приоритетным направлением политики является развитие человеческих ресурсов (документ предусматривает в течение ближайших пяти лет подготовку около 500 тыс. специалистов).

В-четвертых, упоминается необходимость защиты передачи и хранения частной информации.

В-пятых, обращается внимание на необходимость создание законодательной базы для борьбы с преступлениями в КП.

В-шестых, документ призывает к индивидуальной ответственности в обеспечении безопасности в КП.

Принятие «Национальной политики» стало позитивным шагом на пути к обеспечению ИБ, однако явно недостаточным, что связано с отсутствием детального описания путей достижения поставленных целей. В «Национальной политике» не предложена общенациональная стратегия. В целом, этот документ носит рекомендательный, а не обязательный характер.

В отсутствие «дорожной карты» обеспечения безопасности в КП различные ведомства Индии действуют зачастую не согласованно, что при ограниченных ресурсах на борьбу с киберугрозами (7,8 млн. долл. в 2013 году[98]) снижает эффективность предпринимаемых шагов.

Недостатком стратегии Индии в КП является отсутствие в «Национальной политике» упоминания такого аспекта, как безопасность телекоммуникаций, который приобрел особую важность в связи с ростом мобильных устройств, имеющих доступ к интернету. По данным

[96] Samuel Ch. Prospects for India–US Cyber Security Cooperation // Strategic Analysis. – Sept., 2011. – Vol. 35, No. 5. – P. 773.
[97] National Cyber Security Policy – 2013 // Department Of Electronics & Information Technology, Government Of India. (http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf).
[98] Saksena A.R. India Scrambles on Cyber Security // The Diplomat. - Jun. 18, 2014. (http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/).

«Лаборатории Касперского», в 2013 году Индия заняла второе место в мире после России по количеству атак на мобильные устройства (7,9% атак, предпринятых всего в мире).[99]

Обойден молчанием также вопрос о создании Киберкомандования (Cyber Command) ВС Индии, которое будет располагать основными наступательными и оборонительными средствами в данной области. В «Национальной политике» об этом и вообще о военной составляющей не сказано ни слова[100], хотя эти темы являются предметом острых дискуссий как в Индии, так и в других странах.

Является ли это ошибкой авторов текста или же свидетельством наличия глухой стены между гражданскими и военными организациями Индии, работающими в области КБ? Первый вариант ответа представляется более правдоподобным. Представители Вооруженных Сил Индии понимают невозможность разделить КП на гражданскую и военную составляющие. Так, по словам бригадного генерала (в отставке) Абхиманью Гхоша, «для защиты киберпространства в интересах национальной безопасности и международной стабильности необходимы сотрудничество между гражданскими и военными организациями, включая партнерство между государственными и частными организациями, а также международный консенсус».[101]

[99] India 2nd in list of countries facing cyber attack on mobiles: Kaspersky // Business Line. – Mar. 2, 2014. (http://www.thehindubusinessline.com/news/india-2nd-in-list-of-countries-facing-cyber-attack-on-mobiles-kaspersky/article5742910.ece?ref=relatedNews).

[100] Pandit R. Tri-service commands for space, cyber warfare // The Times of India. – May 18, 2013. (http://timesofindia.indiatimes.com/india/Tri-service-commands-for-space-cyber-warfare/articleshow/20115462.cms).

[101] Ghosh A. Cyber Threat and Military Challenge // Challenges of International Strategic Environment and Multilateral Security Cooperation. – Seoul: Korea National Defense University, 2011. – P. 91.

Глава 4. Примеры информационно-психологических методов противоборства XXI века

Информационно-психологическое противоборство *как определенная методология изменения картины мира в заданном направлении,* в настоящее время стало одной из наиболее быстро развивающихся форм борьбы передовых государств. При этом объектом воздействия могут быть как отдельные лица (или группа лиц), принимающие решения на различном уровне, так и массовое сознание народа в целом.

Информационно-психологическое противоборство в политической сфере *– использование информационных, дипломатических, военно-демонстрационных, экономических и других приемов для воздействия на мнение, настроения и, в итоге, на поведение противоположной стороны*.

Принципиальные особенности информационно-психологического воздействия:

- ведется, как правило, на любой территории, без ограничений пересекая границы, проникая, в том числе, и в сознание противника;
- ведется, не оставляя видимых следов; объекту воздействия кажется, что это он сам принимает решение, на самом же деле он оказывается ведомым другими;
- относительная экономичность для ее инициаторов, поскольку небольшой объем входной информации может привести к максимально значимому результату, например, к формированию нужного общественного мнения;
- один и тот же факт в условиях информационно-психологической операции может получать разные интерпретации, вплоть до диаметрально противоположных.
- даже при условии наличия самых современных ИКТ невозможно блокировать действия противника в информационной борьбе подобно тому, как это делается традиционными видами оружия.

Информационно-психологическая война *– наиболее острая форма противоборства в информационно-психологической сфере, осуществляемого путем воздействия на информационно-психологическую сферу противника с целью решения стратегических задач. В том числе, это включает целенаправленное и планомерное использование инструментов информационно-психологического воздействия и других средств (дипломатических, военных, экономических и т.д.) для влияния на мнения, настроения и, в итоге, – на поведение противника с целью заставить его действовать в заданном направлении.*

Информационно-психологическое воздействие (ИПВ) *– это применение информационно-психологических средств влияния на психику человека с целью ее модификации в нужном для воздействующей стороны направлении и внесения изменений в его поведение и (или) мировоззрение*.

Основной формой ведения и главным элементом содержания информационно-психологической войны является ***информационно-психологическая операция*** *– совокупность согласованных, скоординированных и взаимоувязанных по целям, задачам, месту и времени, объектам и процедурам видов, форм и способов информационного воздействия.*[102]

Информационно-психологические операции различаются масштабами, целями и задачами, объектами воздействия, используемыми технологиями и условиями проведения.

По срокам осуществления информационно-психологические операции делятся на *стратегические* (долгосрочные), *оперативные* (среднесрочные) и *тактические* (краткосрочные).

[102]См. Матвиенко Ю. А. Информационно-психологическая война как одна из форм разрешения социально-политических противоречий в современном обществе// Информационные войны. 2008. № 4.

По времени осуществления – на операции, проводимые до перехода конфликта в активно-силовую фазу и проводимые в условиях разгоревшегося конфликта.

По направленности – на операции, проводимые непосредственно против реципиента, либо в интересах коммуникатора, либо против третьих лиц с целью склонить их на свою сторону.

Информационно-психологические методы и средства психотехнологий подразделяются на ***открытые*** и ***скрытые (тайные)***, ***положительные*** и ***негативные***, ***преследующие явные и скрытые цели***.

Тайные информационно-психологические операции одного государства (группы государств) против другого осуществляются путем оказания управляющего информационного воздействия на индивидуальное, групповое и массовое сознание, чувства, волю граждан, дезинформирования субъектов принятия политических, экономических и иных решений, а также путем подрыва информационной инфраструктуры стороны-противника. Такие операции ориентированы на формирование условий для принятия выгодных для применяющих эти действия государств решений в военной, политической, экономической и других областях в странах, являющихся объектами информационно-психологического воздействия. Для создания таких условий специально подготовленная информация доводится до объектов воздействия через электронные, печатные и иные средства массовых коммуникаций, средства электронной и почтовой связи, аудио-, видео- и кинопродукцию, открытые телекоммуникационные сети, наглядно-демонстрационные средства.

В целом можно прогнозировать усовершенствование методов и расширение сфер применения информационно-психологической войны, что может не только повлиять на сложившийся в мире стратегический баланс сил, но и изменить сами ныне существующие критерии оценки такого баланса на основе соотношения геополитических, экономических и военных факторов.

4.1. Грузино-южноосетинский конфликт 2008 года: уроки информационной войны

Одна из причин негативного восприятия внешней политики РФ на Западе в последние годы заключается в том, что со стороны западных стран на мировое общественное мнение оказывалось медиадавление[103] в рамках проводимой информационной войны. Это стало возможным на основе бурного развития информационных технологий и глобального распространения англоязычных СМИ, что привело к неравенству коммуникационных возможностей России и Запада в доведении политической позиции и отстаивании внешнеполитических интересов. При этом соотношение удельного веса сторон по военному и экономическому потенциалам перестало быть определяющим фактором. Так, в рамках грузино-южноосетинского конфликта 2008 года перевес в информационном противоборстве оказался на стороне Тбилиси, благодаря созданному общественному мнению и осуждению действий России западными государствами.

Подготовка Тбилиси к информационной операции 2008 года

Трагические события августа 2008 года в Южной Осетии нельзя рассматривать только как войну в классическом понимании этого термина. Вооруженное противостояние между Тбилиси и Цхинвалом можно объяснить вековыми политическими, межэтническими, историческими и другими причинами. Существовала латентная конфликтность, обусловленная, в том числе, рассеченностью территории на Северную и Южную Осетию. После распада Советского Союза это усугубилось в процессе реализации грузинским руководством недальновидной внутренней политики, основанной на подавлении национальных меньшинств. Имели место и факты геноцида, когда граждане уничтожались по этническому признаку в ходе массовых убийств. При этом грузинские лидеры заявляли о необходимости «очистить территорию Грузии от осетин».[104] Это подтолкнуло граждан Южной Осетии к реализации своего права на самоопределение.

Обстрел Цхинвала в августе 2008 года, по свидетельствам множества очевидцев, был неожиданным, но прогнозируемым. В частности, существуют факты, свидетельствующие о заблаговременной подготовке Грузии к военным действиям (так, в апреле 2006 года Тбилиси потребовал вывода миротворческих войск с территории Южной Осетии и Абхазии, грузинские и западные СМИ стали утверждать, что какая-либо потребность в нахождении там миротворцев отсутствует). Но это не помешало Западу развернуть против РФ крупную информационную операцию с целью дискредитации России в глазах международного сообщества и формированию имиджа государства-агрессора. В то время российское руководство не предвидело этого. Как следствие, оно не смогло донести до внутренней и внешней аудитории два тезиса:

1) Грузия не единожды проявила геноцид в отношении национальных меньшинств, следовательно, нахождение на ее территории миротворцев является жизненно необходимым;

---

[103]Под медиадавлением предлагается понимать целенаправленное воздействие СМИ на актора мировой политики, имеющее целью изменение его позиции в решении какого-либо вопроса, в том числе в процессе урегулирования политического конфликта (например, на Украине). Прим. авт.

[104]Кочиева И., Маргиев А. Грузия. Этнические чистки в отношении осетин. М., 2005.
Блиев М. М. Южная Осетия в коллизиях российско-грузинских отношений. М., 2006.
Грузия-Осетия: история геноцида. (http://www.osetia-news.ru/analytics/91.html).
Идаятов А.К. Медиакратия и ее роль в урегулировании политических конфликтов. МГУ им. М.В. Ломоносова, факультет политологии, кафедра российской политики.
(http://istina.msu.ru/media/dissertations/dissertation/858/120/7517857/Idayatov_A.K._Dissertatsiya_soisk._uch._st._k.p.n..pdf).

2) согласно Дагомысскому соглашению о принципах мирного урегулирования грузино-осетинского конфликта от 24 июня 1992 года и Московскому соглашению о прекращении огня и разделении сил между грузинской и абхазской стороной от 14 мая 1994 года, Россия является гарантом мира на этих территориях и сдерживающим фактором в противостоянии между Грузией и Южной Осетией и Абхазией.

На фоне важных политических событий в регионе в 2006 году разразился шпионский скандал, когда Грузия задержала двух российских военнослужащих по подозрению в шпионаже и подготовке провокаций. В качестве ответной меры грузинским туристам перестали выдавать визы для въезда в Россию. Одновременно Москва отозвала семьи своих дипломатических сотрудников из Тбилиси и повысила уровень боеготовности контингентов, размещенных на грузинской территории. Такие действия при правильном информационном освещении могли служить предупреждением Грузии на случай подготовки агрессии и создать недоверие к ней со стороны международного сообщества. Однако медийное освещение этих событий в РФ в тот период носило, в основном, констатационный характер.

В качестве еще одного факта подготовки Грузии к военным действиям можно рассматривать широкое применение ею с начала 2008 года беспилотных летательных аппаратов (БПЛА) с целью проведения разведки на территориях Абхазии и Южной Осетии. Это совершалось вопреки обязательствам Грузии не совершать полеты в зоне конфликта. Весной 2008 года, после потери пяти БПЛА, Грузия обвинила Россию в агрессии и бомбардировке ее территории. Во второй половине апреля этот вопрос был рассмотрен на заседании Совета Безопасности ООН. И вновь Москва уклонилась от публичного обсуждения этой темы в СМИ, что позволило Тбилиси усилить негативное восприятие РФ в Европе и США.

Информационная война в период вооруженного конфликта 2008 года

Психологическая составляющая информационной войны, которую можно определить как *противоборство двух и более государств относительно доминирующей трактовки происходящих событий с параллельной дискредитацией образа противника*, имела в период вооруженного конфликта августа 2008 года первостепенное значение.

Последующие события поставили под сомнение представление о том, что в современном мире действуют подлинно независимые СМИ, которые совершенно объективно освещают политически важные события. Даже главное преимущество телевидения – «эффект присутствия» – нивелируется подменой используемых понятий и кадров, искажением сведений о происходящих на экране событиях, а также целенаправленным видоизменением слов выступающего лица.

Изучая характер информационного противостояния в период грузино-южноосетинского конфликта, эксперты отмечают широкое использование западными и грузинскими СМИ олимпийской тематики (в это время в Пекине проходили Олимпийские игры) с целью привлечения максимально широкой аудитории к обсуждению рассматриваемой проблемы.[105] Так, вначале грузинские представители заявили об отзыве всех своих спортсменов из Пекина. Потом это опроверг президент М. Саакашвили, который аргументировал это необходимостью выступления спортсменов за честь страны в тяжелое для нее время. При закрытии олимпийских игр США предоставили возможность нести американский государственный флаг спортсменке грузинского происхождения, которая не выиграла ни одной медали. Это стало привлекательным информационным поводом и позволило мировому сообществу сделать вывод, на чьей стороне

[105]Забурдаева Е.В. Управление общественным мнением в условиях современной России//Дис. канд. соц. наук. М., 2009.

предпочтение американцев.[106] Подобные информационные сигналы, обращенные к максимально широкой аудитории, были услышаны.

Россия избрала иной путь. В частности, российские СМИ транслировали тезис о том, что в связи с войной в Южной Осетии премьер-министр В. Путин был вынужден покинуть Пекин для урегулирования конфликта и поддержки населения этой республики. Выход на международную аудиторию в рамках олимпийской темы Россией не был осуществлен вовремя, а проводился постфактум с помощью внедрения термина «олимпийская война». Такое позднее реагирование и оправдательная (объяснительная) позиция снизила эффективность линии России в ходе проводившейся информационной войны.

Следует отметить, что оправдательная позиция губительна для субъекта, который стремится донести свои аргументы. Это объясняется следующими причинами:

- изначально подготовленная позиция содержит наиболее выгодные и удобные для освещения аргументы, тогда как оправдание заставляет переходить к ответу на чужие тезисы, которые не всегда позволяют сохранить и улучшить собственный имидж;
- диалог по заготовленному противником сценарию заставляет государство играть по чужим правилам, т.е. снижает саму возможность контролировать ситуацию, и в повестке дня начинают доминировать аргументы другой стороны, что существенно влияет на восприятие аудиторией ситуации в целом, а также на оценку аргументов сторон.

Помимо этого, в рамках информационной войны 2008 года неоднократно использовался ***метод «наклеивания ярлыков»*** путем проведения исторических параллелей, невыгодных для образа РФ. При этом западные журналисты заявляли об имперских амбициях России как наследницы Советского Союза, ее настойчивом стремлении к возврату утраченных позиций на мировой арене. Так, 18 сентября 2008 года в Фонде Маршалла в Вашингтоне государственный секретарь США К. Райс провозгласила, что «ставшие анахронизмом демонстрации Россией своей военной мощи не смогут повернуть историю вспять».[107] Аналогичным образом высказался журналист британской газеты Observer: «Во время войны меня удивили российские военные. Я не ожидал, что они окажутся такими жестокими. Они грабили и убивали мирных грузинских жителей».[108]

Президент М. Саакашвили постоянно сравнивал действия России в Южной Осетии с вторжением в Афганистан и введением войск в Чехословакию. Он напомнил о том, что именно «советские танки, вошедшие в Прагу, растоптали надежды Чехословакии на свободу и либерализацию». Авторитетное британское издание Independent отметило, что действия США и Великобритании создали «впечатление, что виновна во всем Россия, а Грузия – это маленькая, но храбрая демократия, которую большая и плохая Россия решила подавить. Такая версия практически мгновенно получила всеобщее признание. А Москве оказалось почти невозможно ее опровергнуть, поскольку она подтверждала все существующие негативные стереотипы».[109]

Россия также пыталась использовать этот метод, сравнивая события в Южной Осетии с терактом 11 сентября 2001 года в США. Однако данное сравнение, несмотря на чувствительность к этой тематике американцев, не нашло отклика ни у российской, ни у зарубежной аудитории, т.к. в России события 11 сентября уже мало кого интересовали, а американская аудитория не сумела понять логическую связь между фактами. Таким образом, метод «наклеивания ярлыков» не использовался Россией результативно.

---

[106]Пекин 2008: американский флаг на закрытии олимпиады несла грузинка. Интернет-портал Sportbox.ru. М., 25 августа 2008 г. (http://news.sportbox.ru/Vidy_sporta/Events/Pekin-2008-Amerikanskiy-flag-na-zakritii-Olimpiadi-nesla-gruzinka).

[107] Информационная война против России: как это было. Информационно-аналитическое сетевое издание «Сегодня.Ру». М., 17 апреля 2009. (http://www.segodnia.ru/content/18043).

[108]Georgia marches into South Ossetia, 8 August//The Observer. London. December 28. 2008.

[109]Почему Запад игнорировал правду о войне в Грузии? Интернет-проект «ИноСМИ.RU». М., 12 ноября 2008. (http://www.inosmi.ru/world/20081112/245289.html#ixzz2ij3cEPM4).

Важную роль в информационном противостоянии сыграл ***метод определения характера событий и способа их публичной интерпретации***, т.е. *описания событий на основе собственных интересов*. Россия определяла происходившее как грузино-южноосетинский конфликт, а вторжение Грузии в Южную Осетию как геноцид осетин. В Вашингтоне и Тбилиси рассматривали это как противостояние Грузии и России и вторжение российских войск на грузинскую территорию. Причем на Западе Южная Осетия не признавалась ни участником конфликта, ни пострадавшей стороной вплоть до конца 2008 года.

Параллельно западными СМИ *создавались соответствующие образы обеих сторон конфликта*. Это позволяло конструировать образ врага в лице Кремля, который преподносился как серьезная угроза западным ценностям. Для этого Западом применялся ***метод гиперболизации***, т.е. преувеличение опасности от РФ, и создавались разного рода панические настроения.

При этом призыв Москвы к публичному признанию геноцида осетин не воспринимался западной аудиторией. И для этого было много причин. Во-первых, малочисленность осетин на фоне массовой гибели мирного населения в Ираке и Афганистане. Во-вторых, данное понятие классифицируется как международное преступление, признаваемое только по решению Совета Безопасности ООН или Международного уголовного суда. Очевидно, что в этих институтах получить такое признание было бы невозможно. В-третьих, российские политические деятели и СМИ слишком свободно употребляли этот термин, что негативно воспринималось на общественном уровне за рубежом, не говоря уже об экспертном подходе.

Одной из попыток России по восстановлению собственного имиджа стало оглашение информации о военной операции Грузии в Южной Осетии под названием «Чистое поле». Однако западные источники массово распространили в электронных СМИ и сети Интернет информацию о том, что такое название носила операция вооруженных сил РФ против Грузии. Это не соответствовало действительности, но в политических условиях того момента в это достаточно легко поверили многие.

Следует отметить, что все указанные аргументы России о событиях в Южной Осетии внутри страны воспринимались позитивно и вызывали полную поддержку. Следовательно, формирование внутреннего общественного мнения велось достаточно грамотно, что не наблюдалось на международной информационной арене. С целью подтверждения этого вывода можно привести слова представителя русской службы ВВС о том, что «когда на телеэкранах мира замелькали первые кадры разрушенных домов в Цхинвали, российские политики, начиная с В. Лукина и кончая С. Лавровым, вдруг стали произносить название города Цхинвали на осетинский манер – Цхинвал. Это сразу указало, на чьей они стороне».[110]

Принципиально разное восприятие одной и той же информации российской и западной аудиторией обусловлено наличием *когнитивных стереотипов*. Примером этого служит трансляция кадров, на которых в зоне военных действий президент М. Саакашвили показан крайне испуганным, а позднее – «жующим галстук». Этот материал был адекватно воспринят внутренней российской аудиторией, поскольку соответствовал стереотипу о трусости и несерьезности грузинского президента. Однако внешняя аудитория отреагировала на этот материал отрицательно, ввиду соответствия состояния М. Саакашвили на картинке стереотипу об агрессии России. Дифференцированное воздействие одних и тех же фактов на разные аудитории объясняется также отсутствием каналов коммуникации, позволяющих Москве доносить свою точку зрения до мировой общественности.

Другими словами, наличие широких возможностей по разъяснению ситуации внутри страны не могло компенсировать их ограниченность в представлении аналогичных аргументов международной общественности. Российские СМИ, вещающие на английском языке, не имели реального выхода на широкую аудиторию. В первую очередь это касалось телевизионного канала «Russia Today», который за рубежом смотрели преимущественно выходцы из России и СССР.

[110]Цыганок А.Д. Война 08.08.08. Принуждение Грузии к миру. М.: Вече, 2011.

Кроме того, в качестве проблемного и сдерживающего фактора следует выделить *наличие различных систем восприятия* у российской и западной аудитории. Грузия находилась в одном семантическом поле с западными СМИ и использовала привычные для потребителей понятия англоязычной информации.[111] Например, понятие «демократические ценности» в отечественных СМИ используется редко и в основном в отрицательном контексте. Зато широкое распространение в РФ получили термины «национальные интересы» и «государственная мощь», использование которых на Западе часто воспринимается как проявление империализма и милитаризма. Отметим, что термины «национальная безопасность» и «национальные интересы» в 90 годы XX века были заимствованы Россией у Запада, где в университетах преподают учебные курсы с такими названиями.

Значение фактора наличия различных систем восприятия аргументов подтверждается американским журналистом У. Липманом. По его мнению, сформированная западными СМИ картина мира фактически поддерживает американские и европейские ценности. Поэтому в ходе грузино-южноосетинского конфликта Россия столкнулась с проблемой донесения своей позиции, когда ей оказалось чрезвычайно трудно не только «прорваться» сквозь информационную блокаду, но и за короткий срок развенчать систему стереотипов, играющих против ее интересов.

Отметим, что в период конфликта действия России в информационном пространстве далеко не всегда велись в нужном направлении.

Во-первых, отечественные СМИ проводили множество разовых акций по дискредитации властей Грузии, но деятельность этих властей уже и до того имела негативную оценку в России. Следовательно, основные усилия СМИ направлялись на те проблемы, которые уже были решены.

Во-вторых, действия российского руководство не были подчинены единой цели, в первые дни конфликта у России не было официальной точки зрения, а также собственных информационных репортажей. Для донесения своей позиции тогда использовались кадры, снятые грузинами и американцами. В комментариях российских очевидцев событий присутствовала путаница с датами ввода российских войск через Рокский тоннель.

В-третьих, не учитывалась необходимость работы с оппозиционно настроенной частью аудитории. По ряду причин, включая воздействие западных СМИ, она имела негативное отношение к действиям собственной власти, тиражируя их в сети Интернет. Кроме того, большинство российских граждан осознавало проигрыш Москвы в информационной войне, что не могло не сказываться на общих настроениях.

Однако главной проблемой России в период информационной операции 2008 года была не столько некорректная работа с информацией, сколько запаздывание в предоставлении необходимых аргументов. Так, российские масс-медиа включились в публичное обсуждение грузино-южноосетинского конфликта лишь на второй день. Такое отставание от противников на шаг-два стало одним из критических факторов, которые повлияли на исход информационного противостояния. Как следствие, трансляция аргументов на первом этапе осуществлялась фрагментарно, что не позволило сформировать устойчивое отношение к происходящему даже нейтральным зрителям. В то же время, предложенная BBC и CNN хронология событий попала на благодатную почву.

К числу причин, которые позволили западным СМИ сформировать нужное им видение ситуации, относится также отсутствие российских журналистов в местах боевых действий.

Следует отметить, что в конце 2008 года, когда в силу различных обстоятельств информационное давление на Россию со стороны Запада ослабло, европейские журналисты совершили поездку в Южную Осетию. Это позволило им сделать более объективные выводы и впоследствии привело к изменению отношения к действиям России. Однако в большей степени это было обусловлено активизацией лидеров Евросоюза в качестве посредников в мирном урегулировании конфликта.

---

[111]Забурдаева Е.В. Управление общественным мнением в условиях современной России//Дис. канд. соц. наук. М., 2009.

Как было отмечено ранее, в условиях информационной войны лидирующую позицию занимает более подготовленный участник. В такой позиции оказались зарубежные СМИ, которые, возможно, были заранее проинформированы о начале вооруженного конфликта. Это выразилось в наличии единой точки зрения, совпадающей с заявлениями лидеров США и их союзников, и были быстро растиражированы с помощью многочисленных каналов коммуникации.

Несомненно, что *возможность вещания и передачи аудиовизуальных аргументов на широкую мировую аудиторию в период политического конфликта* играет огромную роль. Именно поэтому в первые дни конфликта Россия транслировала кадры, предоставляемые BBC, поскольку у нее отсутствовали собственные материалы.[112]

Информация зарубежных медиа, направленная на граждан Грузии, говорит о том, что имела место целенаправленная информационная кампания, в ходе которой организация и освещение событий было подчинено единой цели. Об этом свидетельствует и предоставление медиаплощадок для зарубежных журналистов в г. Гори, которые создавали для западной аудитории «эффект присутствия» и позволяли осуществлять подмену видеоряда: «Грузия Online», телекомпания «Рустави-2», информагентство ИнтерпрессНьюс и радио «Имеди». Особенно мощный информационный эффект имели телерепортажи о бомбардировках г. Гори российскими самолетами и о колоннах бронетехники на дорогах за пределами Южной Осетии с лозунгами «На Тифлис». Не меньшее воздействие имели передачи об операции в Абхазии, на которую Грузия в 2008 году не нападала, что создавало картину не ответных действий России, а ее шагов по захвату новых территорий, якобы «под предлогом» спасения мирных жителей двух автономий.

Необходимо также обратить внимание на *особенности риторики* России и Грузии. Как уже отмечалось, Москва не имела единой тактики подачи информации и выстраивала оправдательные речи, используя образы, не основанные на когнитивных стереотипах целевой аудитории (геноцид осетин, террористические атаки 11 сентября, агрессивная геополитика США и т.д.). Это сталкивалось с простотой грузинских обращений, которые сводились к трем фразам: «Россия – агрессор», «Мы – маленькая демократическая страна», «Пожалуйста, помогите нам». Такой подход, не требующий от аудитории логических рассуждений, работал быстрее, масштабнее и эффективнее.

Дезинформация и клевета в рамках информационной операции 2008 года активно использовались даже весьма авторитетными на Западе СМИ. Так, психологические приемы – на одной странице газеты был расположен портрет В. Путина и кадры убитых мирных жителей в Цхинвале – позволяли установить ассоциативную взаимосвязь. Наиболее известным и распространенным подлогом стала трансляция видеоряда из разрушенной столицы Южной Осетии с подписью «г. Гори, Грузия» одновременно с интервью вице-премьера РФ С. Иванова по телеканалу CNN. Таким образом, слова российской стороны об отсутствии агрессии со стороны РФ и о необходимости ответа на действия Грузии в отношении Южной Осетии «опровергались» в прямом эфире. Кроме того, такая подмена видеоряда позволила западным медиа закрепить два ключевых образа: «жертвы» – Грузии и « агрессора и врага» – России.

В качестве подлога можно также расценить интервью грузинской газете «гражданина России», которое было призвано продемонстрировать негативное отношение русских к действиям Кремля в Южной Осетии. В этой статье проводилось сравнение военных действий России (Советского Союза), начиная с Афганистана и заканчивая войной в Чечне. На передний план выводилось обсуждение внутренних российских проблем, которые должны были продемонстрировать аудитории слабость страны ввиду существенной внутренней нестабильности: «любая война отвлекает людей от реальных проблем – бедности и бесправия…, как и во всех недемократических государствах, власть в нашей стране принадлежит не гражданам (пусть опосредованно, через партии и другие политические институты), а исключительно правящей верхушке. А поскольку в ней всегда в большой мере представлены военные и спецслужбы, они

[112]Цыганок А.Д. Война 08.08.08. Принуждение Грузии к миру. М.: Вече, 2011.

беззастенчиво тянут одеяло на себя. Пытаясь оправдать свое существование и получить из бюджета кусок покрупнее, они не останавливаются ни перед чем, даже перед разжиганием войны».[113]

Отметим, что в мировой практике существует формат допустимых реакций на информационный подлог. Как правило, он выражается в предоставлении претензий опубликовавшему недостоверные сведения СМИ, после чего поступает опровержение и извинение со стороны редакции. В 2008 году это также имело место. Так, испанский канал TVE включил в один из репортажей видеоролик «победного въезда» грузинских солдат в Цхинвал, но он представлялся как въезд российских войск в Гори. После предъявления Москвой претензии поступили официальные извинения. Однако в условиях интенсивного противостояния и массовой дезинформации значение опровержения существенно снижается. Причина в том, что высокая скорость обновления информации и параллельное использование ряда манипулятивных технологий быстро закрепляют нужную мысль. Как следствие, использование такой технологии в момент массовой информационно-психологической атаки даже при ее дальнейшем опровержении успевает выполнить свою задачу.

Таким образом, в ходе информационной войны 2008 года западные СМИ задействовали в своем арсенале практически все имевшиеся у них средства с целью формирования нужного Западу общественного мнения: от ***лексико-грамматических*** *(повторы, метафоры, эпитеты, лингвистические аномалии и т.д.)*[114] до ***политико-психологических*** *(конструирование мифов*[115]*, формирование образа врага*[116]*, привлечение экспертов*[117]*, апелляция к статистическим данным*[118] *и проч.)*. При этом популярность американских и британских телеканалов у населения всей планеты и широкое распространение англоязычной прессы не требовало от США и ЕС разделения усилий в отношении внутренней и внешней аудитории. Формирование единого информационного потока, который достигает различных субъектов и максимально широкой аудитории, является их однозначным преимуществом. В отличие от этого, Россия была вынуждена проводить обособленные информационные кампании внутри и вне страны. В результате Москва смогла формировать общественное мнение внутри страны, основанное на своем видении событий, но этого не удалось сделать в рамках глобального медиапространства, где позиция России целенаправленно заглушалась и не получала должного распространения.[119]

Приоритетным способом аргументации России в то время была апелляция к фактам без учета когнитивных стереотипов аудитории, что заранее было обречено на провал. В условиях заранее подготовленной критически настроенной аудитории, получающей освещение тех же фактов под другим углом из более привычных источников, это неизбежно вело к отторжению информации из России.

Особенности использования киберпространства в грузино-южноосетинском конфликте 2008 года

В рамках конфликта 2008 года хорошо проявились также возможности воздействия на общественное мнение в киберпространстве в ходе так называемой ***«войны блоггеров»***. В этом противостоянии русскоязычные представители блоггосферы поддерживали точку зрения федеральных радио- и телеканалов и подтверждали правдивость их сведений. Зарубежные

[113]Последний рубеж//Интернет-проект «ИноСМИ.RU». М., 19 августа 2008. (http://www.inosmi.ru/world/20080819/243374).
[114]Данилова А.А. Манипулирование словом в средствах массовой информации. М., 2011. С. 207.
[115]Russia and Georgia. A scripted war. The Economist. London. August 14. 2008; Europe view. Leave no stone turned. The Economist London. April 19. 2009.
[116]After the War//The Economist. London. October 18. 2008.
[117]Russia and the West. Confrontational Russia//The Economist. London. August 26. 2008.
[118] NATO responds, spin on the ground//The Economist. London. August 19. 2008.
[119]Забурдаева Е.В. Политическая кампания. Стратегии и технологии. М., 2012.

блоггеры, напротив, высказывались в пользу грузинской версии. Недостатком деятельности российских блоггеров было отсутствие выхода на англоязычную аудиторию.

Популярность блоггеров и их способность воздействовать на широкую аудиторию объясняется возможностью установления тесного общения между тем, кто потребляет информацию, и тем, кто ее предоставляет, т.е. ведет блог. При этом устанавливается персональная связь, а коммуникация обретает черты межличностной, что делает ее наиболее эффективной и убедительной.

В ходе грузино-южноосетинского конфликта имели место и ***хакерские атаки,*** которые были начаты со стороны Тбилиси в день обстрела Цхинвала. Началом хакерского противостояния стал взлом югоосетинских сайтов. На это ответили представители России, взломав сайты президента и правительства Грузии и других оплотов «Саакашвили в киберпространстве».[120]

Тогда войну России объявил сайт youtube.com. Размещение на этом ресурсе видеоматериалов, которые позволяли бы правдиво отразить происходящие в Цхинвале события, всячески блокировалось модераторами: от традиционных удалений роликов до отключения счетчиков просмотров, которые выводят ролик в число наиболее популярных и, как следствие, более доступных. Второй способ использовался, например, против фильма «Искусство предательства 08.08.08», переведенного на большинство европейских языков, который показал разрушенный Цхинвал, многочисленные жертвы среди мирного населения, а также агрессивные действия грузинских военных. За довольно короткий срок его посмотрели многие, но сведения об этом обнулялись, что приводило к падению рейтинга видео и затрудняло его поиск. Кроме того, были установлены возрастной ценз для зрителей и обязательная регистрация на сайте. В конечном итоге свободное распространение фильма стало возможным только на сайтах с доменом .ru, т.е. позиция России ограниченно транслировалась на внешнюю аудиторию. Тем не менее, был получен опыт освоения формата выражения своей позиции с помощью художественных произведений. При этом наличие художественной ценности и высокое качество работы обеспечивают более широкое распространение и более длительное существование.

Таким образом, в рамках информационной деятельности 2008 года Москва использовала методы, позволяющие косвенно выразить собственную позицию, минуя коммуникационную «блокаду» в традиционных СМИ, путем отказа от прямолинейных способов предоставления информации. Таким примером стал концерт Мариинского театра под управлением В. Гергиева в Цхинвале 21 августа 2008 года. Зарубежные медиа в целом негативно отнеслись к данному событию, но позднее стали появляться первые единичные одобрительные отклики с Запада о действиях и мотивации России. Появление в Южной Осетии В. Гергиева как знаковой фигуры в мировой культуре стимулировало более сбалансированное обсуждение событий в Грузии, Абхазии и Южной Осетии. Поэтому ответ Западу с помощью культурных акций можно считать вполне адекватным и эффективными.

Уроки информационной войны 2008 года

Несомненно, что в августе 2008 года против России была проведена не просто информационная кампания, а полноценная информационная война, которая соответствовала всем признакам этого явления. Такие операции представляют собой не только способ формирования картины мира с выявлением «своих» и «чужих», но также служат формой межгосударственного взаимодействия. В данном случае речь шла о подавлении российской информационной линии по обоснованию ее национальных интересов с целью формирования негативного имиджа России на Западе. Это обеспечило поддержку общественным мнением

[120]Defenders of cyberspace//The Guardian. London. October 10. 2008.

политики стран НАТО, направленной на достижение более благоприятных для Запада итогов грузино-южноосетинского вооруженного конфликта, чем было бы в ином случае.

Последние события на Украине полностью подтвердили необходимость изменения Россией стратегии поведения в рамках глобальной медиа-политической среды. Нынешние методы борьбы Запада с РФ во многом идентичны тем, которые имели место в 2008 году, поэтому опыт прошлой информационной войны дает возможность Москве скорректировать свое позиционирование в медиапространстве. При этом следует учитывать, что информационная война обеспечивает давление, которое стремительнее любых иных форм разрешения конфликтов влияет на соотношение сил конфликтующих сторон. И это оказывает воздействие на переговорный процесс, направленный на урегулирование конфликта.

Отметим, что в процессе информационного противостояния Грузии и России возросло число сторонников вооруженного разрешения южноосетинского конфликта среди грузинского населения. Если первоначально только 20% националистически настроенных граждан выступало за продолжение вооруженных действий, то ощущение безнаказанности и обиды на Россию, которое укрепилось с помощью внутренних и внешних СМИ, привело к повышению данного показателя до 80%.[121]

В мире, где медиасредства позволяют существенно видоизменять реальность, Россия недостаточно использует свои возможности. В результате, когда против нее проводят информационную кампанию, Москва порой бездействует. Необходимо развивать методы профилактики и предотвращения информационного воздействия и формировать зарубежное общественное мнение, исходя из национальных интересов России. Осуществление соответствующих информационных кампаний способно повлиять на продуктивность и исход официальных переговоров в период кризисов и конфликтов. Под последними нужно понимать подчиненный единой цели и выстроенный в соответствии с заданной стратегией процесс: анализ когнитивных особенностей аудитории, создание базы информационных поводов и материалов, реализация плана, подведение итогов и корректировка общественного мнения при наличии пробелов в реализации плана.[122]

Необходимо учитывать, что Интернет в России является источником информации, влияющим на умы людей не меньше традиционных СМИ. Однако властные структуры до сих пор недостаточно адаптированы к этой среде и не повышают уровень собственного позитивного восприятия со стороны пользователей всемирной сети. При этом достаточно часто здесь применяются методы сухой констатации и логического объяснения, которые еще в 2008 году не оправдали себя.

Одним из ведущих способов формирования общественного мнения со стороны Запада в 2008 году являлось создание информационной повестки дня. Отсутствие такой практики в России стало причиной ее слабости в информационной сфере, что сказалось не только на дипломатическом взаимодействии с другими странами, но и на разрешении внутренних проблем, подрывавших авторитет российской власти. Анализ методов стран Запада, основанных на теоретической базе, разработанной лучшими научно-исследовательскими организациями и институтами, показывает, что в рамках проведения информационной кампании достаточно эффективным средством является отвлечение внимания зрителя от проблемы с параллельной дискредитацией соперника.

Существует разные точки зрения на пути обеспечения информационной безопасности России в рамках разрешения политических конфликтов. Рассмотрим некоторые из них.

1. Целесообразно развивать более тесное сотрудничество российского руководства не только с отечественными, но и с зарубежными журналистами, а также предварительно проводить

[121]Цыганок А.Д. Война 08.08.08. Принуждение Грузии к миру. М.: Вече, 2011.
[122]Почепцов Г.Г. Теория коммуникации. М., 2008.

информационные мероприятия, соответствующие национальным интересам государства.[123] Подобная стратегия позволит планомерно создавать позитивный имидж России и поддерживать ее присутствие в медиапространстве. Однако трансляция определенной идеологической позиции в нынешней международной системе возможна только в двух случаях: когда СМИ достаточно независимы и могут свободно выбирать, чью точку зрения транслировать или же когда они зависят от воли другого, солидарного в отдельных сферах, государства. Первая ситуация не является в полной мере реальной, а вторая невозможна для Российской Федерации. Поэтому только сотрудничества с зарубежными СМИ недостаточно для России. Это серьезно осложняет реализацию эффективной информационной стратегии за рубежом, а также позволяет противникам достаточно успешно дискредитировать политику России. В таких условиях необходимо создавать (развивать) СМИ, которые, с одной стороны, были бы интегрированы в современную глобальную медиа-политическую систему, а с другой – отвечали бы интересам РФ и могли доносить до массовой аудитории аргументы, которые высказывают официальные представители страны. Существующий ныне телеканал «Russia Today», хотя и подвергся гонениям в ряде стран Запада за свою активность в показе нежелательной информации, не может считаться полноценной платформой для создания подобного медиаресурса. Он воспринимается западной аудиторией как ангажированный источник информации, который не может оцениваться как объективный (в отличие от более сбалансированных программ канала «Евроньюс» в России). Именно поэтому требуется создание новых СМИ с широким диапазоном подходов. Напористая демонстрация только одной точки зрения рано или поздно уступит первенство трансляции разных позиций с тонким и умелым перевесом нужного государству подхода. Впоследствии новые СМИ могут быть использованы для улучшения информационного фона в разрешении политических конфликтов.

2. Первоначальным этапом подготовки информационной платформы для повышения эффективности разрешения политических конфликтов является планомерное изменение стереотипов восприятия России в сознании мирового сообщества. Для этого целесообразно развивать концепцию национальной идеи для поддержки национального имиджа. Так, в США концепция национального брендинга активно развивается и является частью дипломатии, начиная с 2006-2007 годах.[124] Ее автором стал британский эксперт С. Анхольт, который указал, что формирование национального бренда является неотъемлемой частью всей межгосударственной деятельности. При этом политика государства воспринимается через конкретную призму, которая сложилась под воздействием медиа и публичных заявлений других государств. Однако, по мнению С. Анхольта, бренд не формируется самостоятельно. Он целенаправленно создается, исходя из интерпретации поведения государства на международной арене другими субъектами. Однако существующие в общественном мнении стереотипы не могут быть разрушены одномоментно. Для противодействия разрушению нужны многие предпосылки, главная из которых – отсутствие противостояния и действий, которые этот стереотип поддерживают. В связи с этим проведение информационных кампаний, направленных на создание более благоприятного имиджа объекта воздействия представляется еще более сложным. Однако если таким образом удается донести свою позицию еще до проведения переговоров, направленных на разрешение политических конфликтов, то их эффективность серьезно повышается. Необходимо учитывать, что в такой ситуации со стороны Запада в отношении России, которая проводит самостоятельную внешнюю политику, будут прилагаться все возможные усилия, препятствующие созданию благоприятного имиджа. Немалым активом в улучшении имиджа России остается распространение русской культуры и искусства, исторических знаний.

3. Для повышения продуктивности мер, направленных на разрешение политических конфликтов, от России требуется создание специальных органов государственной власти, в

[123]Забурдаева Е.В. Управление общественным мнением в условиях современной России//Дис. канд. соц. наук. М., 2009.
[124]Кубышкин А.И., Цветкова Н.А. Публичная дипломатия США. М.: Аспект Пресс, 2013.

том числе на базе МИДа и Администрации Президента РФ, которые могли бы достойно сопровождать международную информационную деятельность страны.[125] Сейчас в российской практике трудно найти пример целенаправленной информационной кампании, тогда как США и страны ЕС большую часть переговоров предваряют именно информационным воздействием на широкую аудиторию. Следовательно, поддержка российских переговорщиков должна рождаться внутри таких структур исполнительной власти. При этом информационные подразделения могут сотрудничать с единым центром медиаподдержки России.

4. Отсутствие у России места в рамках глобальной медиа-политической системы привело в 2008 году не только к искажению ее позиции, но и к своеобразной информационной блокаде, которая препятствовала выходу российских журналистов в мировое информационное пространство. Поэтому особое внимание целесообразно уделять важному принципу антикризисного менеджмента – предотвращению, а не разрешению политических кризисов, а также подготовке антикризисной программы еще до возникновения серьезных проблем. Превентивные меры должны охватывать период, как минимум, в полгода и быть направлены на освещение вопросов, которые могут стать проблемными в ходе переговорного процесса. Следует отметить, что данная тактика используется зарубежными странами, что позволяет им готовить мировое сообщество, как к собственной риторике, так и к неприятию аргументов противоположной стороны.

5. На данном этапе России потребуется реализация кардинальных мер в связи с негативным имиджем страны и отечественной журналистики за рубежом, а также доминированием англоязычных медиа, которые транслируют точку зрения США. В связи с этим целесообразно сформировать перечень авторитетных российских журналистов, ученых и общественных деятелей, которые своей деятельностью заслужили признание на Западе, но не относятся к жесткой оппозиции Кремлю.

6. Развитие российского англоязычного Интернета и привлечение блоггеров способно решить проблему присутствия России в киберпространстве. Реализация этой задачи должна быть подчинена тем же принципам, что и развитие отечественной журналистики в целом. Важнейшее внимание целесообразно уделять работе с официальными представителями России за рубежом на предмет их переориентации на использование методов современной дипломатии и передовых информационных технологий.

Таким образом, события в Южной Осетии в 2008 году продемонстрировали, что проведение политических переговоров в условиях острого конфликта сталкивается не только с традиционными проблемами, такими как неприятие позиции участников, желание использовать преимущественно жесткую модель, но и такие, как ловушка медиа-мировоззрения, которая формируется англоязычной прессой еще до начала переговорного процесса и заранее предопределяет соотношение сил сторон.

Анализ освещения грузино-южноосетинского конфликта в СМИ наглядно показывает необходимость для России интеграции в глобальную медиа-политическую систему для донесения собственной позиции до широкой аудитории. Для этого нужно, в том числе, создать независимые англоязычные СМИ, удовлетворяющие запросам разных возрастных, культурных и иных аудиторий, развивать внутреннюю медиасистему, а также поощрять развитие объективной отечественной журналистики, которая могла бы за счет собственного авторитета выводить аргументы России в ведущие СМИ.

[125]Забурдаева Е.В. Управление общественным мнением в условиях современной России//Дис. канд. соц. наук. М., 2009.

4.3. Методы информационного воздействия в кризисе на Украине в период с 2013 по 2015 годы

Методы информационно-психологического воздействия

Информационно-психологическое воздействие (ИПВ) *– комплекс специальных психологических операций, мероприятий и акций, проводимых с помощью информации, пропаганды и агитации, подготовленной соответствующим образом и доводимой до объекта (групп объектов) воздействия с помощью различных форм психологического воздействия (печатными средствами, радио- и телевещанием, изобразительными средствами, через непосредственное общение, материальными акциями, через информационные компьютерные сети).*[126]

Основным критерием ИПВ выступает результат этого процесса – *изменение установок, поведения, намерений и оценок конкретного индивида или группы лиц.*

Методы ИПВ представлены в таблице 1.

По объекту воздействия выделяют два типа ИПВ: *прямое (открытое)*, которое обращено непосредственно на объект при полном осознании субъектом цели воздействия и *косвенное*, которое обращено на окружение объекта.

По степени открытости для объекта выделяют *открытое ИПВ*, при котором объект осознает цели субъекта и средства их достижения и *скрытое или тайное ИПВ (манипуляция)*, при котором цели субъекта и средства их достижения не осознаются объектом.

По отношению к потребностям объекта выделяют *конструктивное*, которое способствует удовлетворению потребностей и достижению целей объекта и *деструктивное ИПВ*, которое препятствует решению задач объекта и достижению его целей.[127]

Организация и проведение «цветных революций» как результат информационного воздействия

На смену методам, применявшимся прежде для проведения государственных переворотов, в последние десятилетия приходят более тонкие технологии «цветных революций». В XXI веке в целом ряде стран, как с нестабильными, так и с достаточно устойчивыми политическими режимами, произошли события, которые привели к полной или частичной смене власти. Одним из основных инструментом их осуществления является информационно-психологическое воздействие. Отсутствие достаточной нормативно-правовой базы, препятствующей использованию таких методов воздействия, позволяет государствам применять их как в военное, так и в мирное время.

[126]EdwART. Словарь терминов МЧС, 2010. (http://dic.academic.ru/dic.nsf/emergency/944/Информационно-психологическое).

[127]Потеряхин А.Л. Понятие и виды информационно-психологического воздействия // Лаборатория информационно психологических технологий. – 2014. (http://labipt.com/Понятие-и-виды-информационно-психоло/).

Таблица 1.
Методы информационно-психологического воздействия

Группа методов	Метод	Описание метода
Трансляция деформированных образов	***Искажение объемов***	Отвлечение внимания объекта за счет снижения объема и/или интенсивности определенной части информации (образа).
	Упрощение темы	Отвлечение внимания объекта от информации посредством пренебрежения фактами и упрощения интерпретации.
	Внедрение деформированной информации	Скрытие искаженной информации в массиве «маскировочной» информации.
	Изменение причинно-следственных/ временных/ пространственных связей	Нарушение связи между различными компонентами при деформации информации.
	Имитационная дезинформация	Изменение большей части фактов, за исключением той, которая идентифицирует информацию как исходящую от какого-то конкретного источника.
	Заострение или концентрация внимания и уменьшение значимости темы	Видоизменение (деформация) информации (образов) о тех или иных объектах в интересах субъекта воздействия. Существенная часть информации при этом остается неизменной. Объекты: персоны, организации, события, темы, товары и т.д. После видоизменения информации она транслируются тем или иным образом на целевую аудиторию. Такая деформация может затрагивать различные компоненты информации (образа).
	Привлечение внимания внутри темы	
	Псевдологические выводы	
Использование референтных групп	***Идентификация с референтной группой***	Объект сравнивает себя с референтной группой и переносит ее поведение, реакцию и взгляды на себя.

	Метод ссылки на авторитет	Увеличение доверия к информации за счет апеллирования к авторитетному лицу.
Сравнение и контраст	***Сравнение***	Сопоставление предметов с уже известными ранее для акцентирования внимания на положительных/отрицательных чертах предмета с целью создания соответствия подчеркнутых отличий интересам субъекта воздействия и создание у целевой аудитории необходимого отношения объекту.
	Контраст	Применение цветовых решений и особенностей визуального восприятия.
Рефрейминг информации	***Перенос выводов и умозаключений***	Изменение контекста, умозаключения, идеи, обстоятельств и т.д. для придания ситуации другого значения и смысла, который соответствует целям воздействующей стороны. Перенос логических выводов без изменений в новый контекст.
	Перенос игровой ситуации на реальную	Создание ситуации в определенном контексте и ее дальнейший перенос в реальные условия.
	Формирование предопределений	Описание ситуации, относящейся к будущему, и утверждение ее предопределенности.
Ненасильственное убеждение	***Официальные заявления***	Использование различных видов официальных заявлений (таких как публичные выступления, декларации организаций, публичные заявления, групповые петиции и т.д.) для убеждения субъекта.
	Общение с широкой аудиторией	Применение лозунгов, символов, листовок, книг, периодических печатных изданий, теле- и радиопередач и т.д. в целях убеждения.
	Давление на отдельных людей	Давление на лиц различными методами (напр., насмешки над официальными лицами).
	Общественные собрания	Воздействие на субъект посредством проведения собраний протеста и поддержки, митингов, семинаров и т.д.

Связывание	***Использование эмоциональных слов***	Связывание двух объектов (старого и нового), при котором часть свойств, характеристик, оценка, прошлые и будущие действия или поведение и прочее переходит от старого объекта к новому (проектируется со старого объекта на новый). Основным фактором, влияющим на эффективность данной группы методов, является наличие у существенной части целевой аудитории устойчивого отношения к старому объекту. В качестве объектов могут выступать персоны, организации, идеологии, моральные ценности, основные потребности человека, ценности общества, товары, программы и т.д.
	Связывание с помощью объединяющих слов	
	Связывание через схожесть по параметру	
	Связывание через частный случай или обобщение	
	Связывание через средство реализации, совместную сферу применения	
	Причинно-следственное связывание	
	Связывание через третий объект	
	Связывание через совместную демонстрацию	Совместная трансляция информации об обоих объектах (старого и нового) с использованием различных каналов коммуникации
	Связывание через отношение и поддержку	Выражение поддержки одного объекта другому для создания у аудитории ощущения связи объектов и для переноса свойств и отношения с одного объекта на другой.
	Связывание через использование многозначных слов, понятий, образов	Использование слов/образов с несколькими значениями (омонимы), а также слов/образов, приобретающих различные значения в зависимости от контекста, которые могут иметь различную интерпретацию/ различное значение с целью достижения запланированных субъектом воздействия результатов без высказывания конкретных обвинений, предположений, оценки объектов.
«Проблема-решение» («угроза – спасение»)	***Связывание объекта с проблемой (угрозой) с прямым обращением к целевой аудитории***	Выявление существующей угрозы (проблемы): угроза жизни, здоровью, потеря статуса, семьи, друзей, комфорта, процветания; некачественная работа того или иного прибора и т.д. Связывание того или иного объекта с угрозой (проблемой) или избавлением от нее. Если целью воздействия является создание негативного отношения к одному из объектов, этот объект связывают с угрозой. Если целью является создание позитивного отношения - этот

		объект связывают с избавлением от данной угрозы. В качестве действующих лиц сообщений выступает целевая аудитория, которой непосредственно и направлено сообщение.
	Связывание объекта с проблемой (угрозой) с косвенным обращением к целевой аудитории	В качестве действующих лиц сообщений выступает некая абстрактная аудитория, как правило, похожая по характеристикам на аудиторию, подвергающуюся воздействию.
Превентивные ответы и пропаганда («вакцинация»)	***Превентивные ответы и пропаганда в явном виде***	Нейтрализация восприятия особенностей объектов и пропагандистских тем, которые являются потенциальной угрозой для осуществления целей воздействующей стороны и могут присутствовать в общественном сознании. Заблаговременная подготовка эффективной реакции объекта воздействия на основе анализа возможных «угрожающих» для воздействующей стороны тем и вопросов. «Угрожающие» темы или вопросы описываются в явном виде, за чем непосредственно следует «ответ» на них, что не дает аудитории времени сформировать свое мнение после описания темы.
	Превентивные ответы и пропаганда в неявном виде	«Угрожающие» темы или вопросы описываются в неявном виде или опускаются вовсе. Заблаговременно формируется оценка, которая будет резко противоречить возможной «угрожающей» теме.

Под ***«цветными революциями»*** понимается *технология осуществления государственного переворота путем внешнего управления политической ситуацией в стране в условиях искусственно обостренной политической нестабильности, в которой давление на власть осуществляется с использованием в качестве инструмента массового протестного движения.*[128] *При этом зачастую применяется какой-либо яркий запоминающийся символ.*

Разносторонний анализ подобных событий приводит к выводу о том, что организация «цветных революций» потребовала выработки четкого сценария, специальной подготовки и последовательных действий, которые под силу только высокоразвитым государствам. Системный и статистический анализ позволяют сделать вывод о том, что они чаще всего проводились в интересах США с целью удаления от власти и/или прихода к власти других лидеров. Для реализации привлекались финансовые, научные, технические, дипломатические и информационные ресурсы, с помощью которых формировались движущие силы, непосредственно осуществлявшие смену власти.

Современные методы развития политических информационно-психологических технологий базируются на разработках психологов середины прошлого века (см. главу 2 данной публикации), с тех пор постоянно развиваются и совершенствуются. В целом логика организации и проведения подобных «цветным революциям» операций может быть описана следующим образом.

После этапа предварительной информационной подготовки объекта воздействия, который может иметь разные временные рамки, в зависимости от цели воздействующего субъекта, «запускается боевой механизм» объекта. Чтобы инициализировать этот механизм информационно-психологического воздействия на сознание (или подсознание), используется мощный толчок, или стресс, способный вывести психику человека из равновесного состояния и активизировать в ней поиск новых защитных механизмов, адекватных стрессовой ситуации. Такая защита в виде идеологии, мировоззрения, системы ценностей, замещающей прежние психологические механизмы защиты человека, разрабатывается в интересах субъекта воздействия профессиональными психотехнологами. В конечном итоге обеспечивается достижение главной цели любой современной психологической операции — добровольное подчинение личности и группы.

В современном мире информационно-психологическая операция не всегда начинается собственно с насильственных действий, но они по-прежнему остаются необходимым фактором любой боевой психологической операции — в качестве средства инициирования цепных психологических реакций, предусмотренных сценарием субъекта воздействия. В планах информационно-психологической операции традиционная война играет ограниченную роль, но это не делает ее менее опасной, не снижает ее масштабов и не вытесняет ее из сферы политических отношений. Глобальные военные конфликты ушли из политической жизни (при наличии ядерного оружия они слишком опасны для всех сторон), количество же локальных вооруженных конфликтов и частота их возникновения растут.

Совет Безопасности РФ отмечает: «Все более широкое распространение для устранения неугодных США политических режимов приобретут усовершенствованные технологии «цветных революций» с высокой вероятностью применения их в отношении России».[129] Это обуславливает необходимость дальнейшего разностороннего исследования

[128]Тезисы выступления д.п.н., проф. кафедры российской политики факультета политологии МГУ имени М.В. Ломоносова Манойло А.В., круглый стол «Информационная безопасность государства в современных международных отношениях», 23 июля 2014. (http://eurasian-defence.ru/node/31263).

[129]О Стратегии национальной безопасности США. 25.03.2015. Сайт Совет Безопасности Российской Федерации. (http://www.scrf.gov.ru/news/865.html).

проблем защиты индивидуального, группового и массового сознания российского общества от подобных деструктивных информационно-психологических воздействий.

Анализ развития кризисов по сценарию «цветных революций» XXI века выявляет определенные закономерности. Применение методов обобщения, типологии, сравнения и классификации позволяют сделать вывод, что события, произошедшие в Грузии (2003 год) и на Украине (2004 год), демонстрируют идентичную последовательность, а также набор механизмов, с помощью которых реализовался политический переворот (см. таблицу 2). Выделим пять основных этапов активной фазы «цветных революций».

Таблица 2.
Сравнительная характеристика «Революции роз» в Грузии (2003 год) и «Оранжевой» революции на Украине (2004 год)

Параметр сравнения	«Революция роз» Грузия, 2003 г.	«Оранжевая» революция Украина, 2004 г.
Причины начала революции	Победа проправительственного блока «За новую Грузию» в парламентских выборах в Грузии 2 ноября 2003 г. (результаты объявлены сфальсифицированными)	Победа В. Ф. Януковича во втором туре президентских выборов 21 ноября 2004 г. (результаты объявлены сфальсифицированными)
Основные участники выборов	Блок «За новую Грузию» и «Национальное движение»	В.Ф. Янукович и В.А. Ющенко
Глава государства	Э.А. Шеварднадзе	Л.Д. Кучма
Лидеры протестного движения	М.Н. Саакашвили, З.В. Жвания	В.А. Ющенко, Ю.В. Тимошенко
Требования оппозиции	Уход Э.А. Шеварднадзе в отставку	Признание недействительными результатов президентских выборов и назначение переголосования
Организации – будущее ядро протестного движения	Молодежное движение «Кхмара» (создано в апреле 2003 г.)	Молодежное движение «Пора!» (создана в марте 2004 г.), украинская военизированная организация «Патриот Украины» (начало деятельности в 2004 г.)
Символика	Розы	Оранжевый цвет
Результат	Уход в отставку Э.А. Шеварднадзе и победа М.Н. Саакашвили на выборах в январе 2004 г.	Победа В.А. Ющенко в ходе повторного голосования 26 декабря 2004 г.

Источники: Кара-Мурза, С.Г. Оранжевая мина / С.Г. Кара-Мурза, М.Н. Мурашкин, С.А. Телегин. – М.: Изд-во Алгоритм, 2008;
Бочанов, М.А. «Цветные революции» как фактор трансформации внешнеполитических стратегий государств на постсоветском пространстве / М.А. Бочанов. – Орел, 2011 и др.

Первый этап. *Формирование в стране организованного протестного движения*, которое впоследствии становится базой будущей революции. Чаще всего такие движения формируются на базе молодежных организаций, т.к. именно в этом возрасте психика человека наиболее восприимчива к информационно-психологическому воздействию.

Второй этап. *Активизация протестного движения посредством инцидента*, получившего мощный резонанс в стране. Инцидентом может быть любое событие, которое привлекло общественное внимание, стало предметом широкого обсуждения и спровоцировало стихийные формы массового поведения. Такое событие, как правило, инициируется специально.

Третий этап. *Вовлечение в массовые движения все больших слоев населения* путем ИПВ через социальные сети и СМИ, основной целью которых является создание тревожных настроений у граждан страны, что делает их более подверженными массовым паническим реакциям.

Четвертый этап. *Формирование «политической толпы»*. Для этого выбирается достаточно большая территория (площадь), на которой могло бы разместиться значительное количество людей. В ходе многочасовых митингов происходит полное эмоциональное слияние отдельных личностей в единую коллективную «толпу» для облегчения манипуляции ее поведением. Для усиления этого эффекта внедряется яркая опознавательная символика. В этих условиях ИПВ на население применяется для внедрения новых ценностей. Поддержание устойчивого существования и функционирования толпы создается за счет ее материального обеспечения.

Пятый этап. *Выдвижение требований к власти от имени толпы*. Чаще всего они являются ультимативными. В случае отказа властей «цветная революция» может перерасти в массовые беспорядки или даже гражданскую войну.

Очевидно, что начало кризиса на Украине можно рассматривать как очередную «цветную революцию». При этом, безусловно, нужно иметь в виду, что на Украине, как и в других странах, где произошли подобные события, для революции сложились серьезные социально-политические предпосылки. Однако ИПВ придало протестным настроениям массовый характер, организованность, агрессивность и особую политическую направленность. В таблице 3 представлены примеры развития каждого из названных выше этапов этих событий.

Сценарий «цветных революций» на Украине угрожает российской национальной безопасности, поскольку при определенных условиях может возникнуть возможность аналогичного развития событий и в России. Кроме того, нельзя исключать, что подобные методы информационного воздействия уже запланированы в отношении Китая, Казахстана и других стран. Именно этим обуславливается исключительная своевременность, важность и актуальность исследований методов, результатов и последствий применения информационно-психологического воздействия на Украине.

С середины 80-х годов и по сей день с целью обеспечения антироссийских настроений на Украине действуют западные высокопрофессиональные специалисты в сфере ИКТ. Соответствующие задачи однозначно ставились не только в трудах З. Бжезинского, отчетах Корпорации RAND, но и в официальных документах США (см. главу 1). Поэтому необходимо отдавать себе отчет в том, что на Украине выросло уже не одно поколение людей, ставших жертвами информационной кампании, даже не подозревая об этом. В частности, для этого использовались учебники по истории для средней школы, которые являются результатом серьезно спланированной и хорошо финансируемой работы, что вряд ли было бы осуществимо только за счет возможностей Украины (см., например, учебник истории для 11 класса: О.К. Струкевич, І.М. Романюк, С.І. Дровозюк. ІсторіяУкраїни. 11 клас. – К.: Грамота, 2011).

Таблица 3.
Этапы «цветной революции» на Украине 2013-2014 годов

Этап «цветной революции»	**Пример**
1. Формирование организованного протестного движения в стране	Радикально-националистическая политическая партия Всеукраинское объединение «Свобода»; Всеукраинская организация «Тризуб им. Степана Бандеры»; украинская националистическая военизированная организация «Братство»; украинская военизированная неонацистская праворадикальная организация «Патриот Украины»; неформальная правоэкстремистская националистическая праворадикальная организация «Правый сектор»; студенческая организация «Батькивщина молода»; добровольная общественная организация (группа) «Самооборона Майдана» и др.
2. Инцидент, получивший мощный общественный резонанс	Принятие Кабинетом министров Украины распоряжения о приостановки процесса подготовки к подписанию Соглашения об ассоциации между Украиной и ЕС.
3. Вовлечение больших слоев населения	Широкое освещение инцидента в СМИ, критика в социальных сетях.
4. Формирование политической толпы	Призывы лидеров оппозиции к массовым протестам на Майдане, в т.ч. с использованием всех СМИ; использование бандеровской символики (ОУН и УПА) в качестве опознавательной; создание условий для поддержания существования и функционирования толпы (материальное обеспечение, горячие напитки, питание и т.д.).
5. Требования, выдвигаемые от имени толпы	Скорейшее подписание Соглашения с Евросоюзом; смена власти и политической системы в стране «для проведения эффективных реформ в рамках Соглашения с ЕС и на основе европейских ценностей».

Украина подвергалась и подвергается информационному воздействию по нескольким общим направлениям: военно-политическому, культурно-психологическому, криминальному и террористическому. Речь идет и о скрытном вмешательстве США и некоторых стран Европы во внутренние дела государства и об ущемлении национального суверенитета Украины с помощью информационных средств.

При этом важнейшее глобальное направление информационного воздействия со стороны США – безусловно, Россия. Но в ходе подготовки и организации украинского кризиса огромные средства тратились и тратятся также на ИКТ-воздействие на другие страны, и в том числе – на союзников и партнеров Соединенных Штатов.

Напомним, что «Объединенная доктрина информационных операций» Министерства обороны США 1998 года определяет *информационную войну* как *«комплексное воздействие (совокупность информационных операций), оказываемое во время кризиса или конфликта на определенного противника/противников с целью решения определенных задач или содействия их решению»*.[130] Эта формула в полной мере соответствует действиям Соединенных Штатов в ходе кризиса на Украине. При этом применяется концепция информационной войны, предусматривающая: перехват и дешифрование информационных потоков (радиоэлектронная разведка); осуществление несанкционированного доступа к информационным ресурсам («хакерская» война); формирование и массовое распространение по информационным каналам противника или глобальным сетям информационного взаимодействия дезинформации для воздействия на население и руководство (информационно-психологическая война); экономическое информационное воздействие. Различные методы используются в зависимости от цели и ситуации.

Несмотря на то, что вопросы использования ИКТ в конфликтах и применение международного права к дестабилизирующим действиям государств в информационном пространстве уже выведены на международный уровень в рамках инициированной Россией Резолюции ГА ООН («Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»), в настоящее время ответственность за подобные действия не предусмотрена.

В то же время и Украина применяет методы информационного воздействия на Россию: попытки радиоэлектронного воздействия и разведки, «хакерские» и информационно-психологические методы (классическая пропаганда, отключение вещания российских СМИ, запрет к показу советских и российских художественных фильмов, отказ в аккредитации российским журналистам и другие имеющиеся у Украины средства). Так, в материалах украинского Центра исследований России (Центр Дослідження Росії) в качестве одного из «методов войны с РФ» предлагается усиление средств информационной борьбы. Причем список целевой аудитории, выбранной в качестве объекта таких средств, удивляет масштабами: «Украина (зона АТО, Крым); Украина (остальная часть Украины); Россия (Москва, СПб, различные регионы); Мир (Европа, США, страны СНГ, другие страны)»[131]. Для ведения этой войны в феврале 2015 года объявлен набор добровольцев в так называемые информационные войска Украины.

Безусловно, Россия должна отвечать на эти информационные угрозы. Москва ведет большую информационно-психологическую кампанию, нацеленную на отечественную аудиторию, Украину и другие страны. Эта деятельность весьма успешна, прежде всего, в ее влиянии на российскую общественность и население юго-востока Украины. Но одновременно здесь обнаружились серьезные недоработки, рассмотрение которых – тема отдельного исследования.

В связи с тем, что «цветные революции» носят подчеркнуто коммуникативный характер, важнейшими их инструментами являются средства массовой коммуникации. Поэтому целесообразно исследовать результаты применения методов информационно-психологического воздействия в период кризиса на Украине на основе контент-анализа СМИ различных заинтересованных стран.

---

[130] Joint Pub 3-13 “Information Operations”, DOD US, December 1998. (http://www.fas.org/irp/doddir/dod/jp3_13.pdf).

[131] Центр исследований России. (http://www.slideshare.net/DenisBohush/infowar-russia-against-ukraine-2014?next_slideshow=2).

Содержательный контент-анализ СМИ Украины, России США, Великобритании и Казахстана в период кризиса на Украине

Контент-анализ *– методика выявления частоты появления в тексте определенных, интересующих исследователя характеристик, которая позволяет ему делать выводы относительно намерений создателя этого текста и/или возможных реакций адресата.*[132]

Содержательный контент-анализ – *анализ, основой которого является исследование сообщений, тем, слов и т.д., сосредотачивающий внимание исследователя на сущности (содержании) текста.*[133]

Этот метод позволяет сделать важные выводы, а также научно подтвердить предположения и гипотезы относительно эффективности применения методов ИПВ.

Для проведения контент-анализа освещения начальных этапов кризиса на Украине были выбраны СМИ:

- *Украины* как основного субъекта кризиса (СМИ: «УКРИНФОРМ»: 388 статей и «Украинская правда»: 550 статей);
- *России* как государства, для которого кризис является угрозой национальной безопасности («Российская газета»: 483 статьи и «Коммерсантъ»: 446 статей);
- *Соединенных Штатов Америки* как государства, заинтересованного в своем влиянии на постсоветском пространстве (“CNN”: 229 статей и “The New York Times”: 139 статей);
- *Великобритании* как главного союзника Соединенных Штатов в Европе и одного из лидеров Евросоюза, ассоциация с которым явилась лозунгом протестного движения на Майдане в ходе эскалации кризиса на Украине (“BBC”: 248 статей и “The Times”: 130 статей);
- *Казахстана* – союзника России и государства, для которого подобные методы информационного воздействия также могут представлять угрозу в будущем («Казахстанская правда»: 47 статей и “Tengri news”: 89 статей).

Всего анализу было подвержено содержание 2749 статей.

Список заинтересованных стран и их СМИ, безусловно, может быть расширен. Данный пример применения этого научного метода для оценки эффективности информационно-психологического воздействия на граждан разных стран может стать основой для дальнейших исследований.

Для проведения контент-анализа был выбран временной период с августа 2013 года по сентябрь 2014 года, охватывающий события на Украине, начиная с подготовки революции до перехода кризиса в критическую фазу, и характеризующийся наиболее интенсивным потоком публикаций мировых СМИ.[134]

---

[132]На основе: Федотова, Л.Н. Анализ содержания – социологический метод изучения средств массовой коммуникации / Л.Н. Федорова. – М.: Институт социологии РАН, 2001.

[133] На основе: Мангейм, Дж. Б. Политология. Методы исследования: пер. с англ. / Дж. Мангейм, Р.К. Рич. – М.: Изд-во Весь Мир, 1997. – С. 276.

[134]Содержательный контент-анализ СМИ Украины, России, США, Великобритании и Казахстана проводился в рамках образовательного процесса в Институте международных отношений (ИМО) НИЯУ МИФИ, специальность «Международные отношения» (ВКР Пересыпкиной О.В.) под руководством к.п.н. Ромашкиной Н.П. с сентября 2014 г. по январь 2015 г.

Единица анализа – это элемент текста, который подлежит подсчету (понятия, темы, ситуации, события). В нашем случае единицей анализа является тема кризиса на Украине и роли России в нем.

Единица счета – количественная характеристика отношения категорий анализа друг к другу или единиц анализа к категориям. Единица счета в данном случае совпадает с единицей анализа.

Выбор источников информации определен периодичностью издания, географией распространения и объемом аудитории. В каждой стране анализировались по два издания – государственное и негосударственное – для обеспечения более объективной оценки. В процессе анализа статьи, касающиеся *кризиса на Украине и роли РФ в нем*, были проранжированы по модальности на нейтральные, отрицательные и положительные[135]. Категории и элементы содержательного контент-анализа представлены в таблицах 4 и 5.

В ходе *пилотажа подлежащей анализу совокупности сообщений*[136] были выявлены типы ключевых упоминаний на темы: *двусторонние отношения РФ и Украины*; *роль РФ в ассоциации Украины с ЕС*; *роль РФ в эскалации кризиса на Украине*; *переговоры РФ и Украины по проблеме поставок газа*; *присоединение Республики Крым к РФ*; *санкции в отношении РФ*; *роль РФ в вооруженных действиях на Юго-Востоке Украины*; *крушение Боинга 777 компании «Малазийские авиалинии» в районе вооружённого противостояния на Востоке Украины 17 июля 2014 г*.

Максимальное количество публикаций (в рамках заданного в исследовании объема статей в выбранных источниках) по проблеме *кризиса на Украине* были обранужены в украинских СМИ – 938 статей, что вполне логично. На втором месте по количеству публикаций на эту тему находится Россия – 929 статей. На третьем месте – США – 378 статей по украинской проблематике, немного меньше публикаций в СМИ Великобритании – 368 статей. И на последнем месте находится Казахстан – всего 136 статей в выбранных для анализа СМИ.

Исходя из того, что Казахстан является одним из ключевых партнеров РФ, логично было ожидать от СМИ Республики (как и от других российских союзников) более активной поддержки внешней политики России. Ее недостаточный уровень должен быть предметом пристального политического анализа государственных органов и экспертных кругов РФ.

---

[135] ***Модальность*** – категория, обозначающая отношение говорящего к содержанию высказывания (к деятельности).

Ранжирование – способ оценки переменной, когда ее значению приписывается место в последовательности величин (ранг), определяемое при помощи порядковой шкалы.

[136] ***Пилотаж подлежащей анализу совокупности сообщений*** – пробный анализ, предназначенный для проверки надежности методик основного исследования.

Таблица 4.
Категории контент-анализа СМИ Украины, России, США, Великобритании и Казахстана

Страна / Категория	Украина		Россия		США		Великобритания		Казахстан	
Тип сообщений	**Статья**									
Объем сообщений	**1000 – 2000 знаков**									
Частота появления сообщений	**Ежедневные газеты**									
Место распространения	**Территория Украины**		**Территория РФ**		**Территория США, Канады, Австралии, Азии, Европы**				**Территория Казахстана**	
Временной период	**Август 2013 года – сентябрь 2014 года**									
Тип продуцента сообщений	УКРИНФОРМ	Украинская правда	Российская газета	Коммерсантъ	CNN	The New York Times	BBC	The Times	Казах-станская правда	Tengri news
Количество анализируемых статей	**550**	**388**	**483**	**446**	**229**	**139**	**248**	**130**	**47**	**89**

Источник: Ромашкина Н.П., Пересыпкина О.В. Информационно-психологическое воздействие в период кризиса на Украине: уроки для России. Информационные войны, № 1, 2016.

Таблица 5.

Модальность статей по проблеме кризиса на Украине

Страна	Название СМИ	Контекст упоминания, событие, тематика / Модальность упоминания	*Двусторонние отношения РФ и Украины*	*Роль РФ в ассоциации Украины с ЕС*	*Роль РФ в эскалации кризиса на Украине*	*Переговоры РФ с Украиной по проблеме поставок газа*	*Санкции в отношении РФ*	*Присоединение Республики Крым к РФ*	*Роль РФ в вооруженных действиях на Юго-Востоке Украины*	*Непричастность РФ к крушению малазийского Boeing-777*
Украина	*Украинская правда*	**Положительная**	7	7	0	2	**43**	0	0	0
		Нейтральная	25	11	23	5	7	11	32	16
		Отрицательная	**110**[137]	**19**	**27**	**11**	1	**35**	**136**	**22**
		Суммарное кол-во статей [138]	142 (5,2;41,8)	37 (1,3;25,2)	50 (1,8; 6,1)	18 (0,7; 8,9)	51 (1,8; 22,4)	46 (1,7; 17.2)	**168** (6,1; 33,0)	38 (1,4; 15,8)
	УКРИНФОРМ	**Положительная**	6	10	0	4	16	0	0	**0**
		Нейтральная	20	10	12	10	**17**	7	15	13
		Отрицательная	**69**	**15**	**20**	**15**	1	**26**	**81**	**21**
		Суммарное кол-во статей	95 (3,5; 27,9)	35 (1,3; 23,9)	32 (1,2; 3,9)	29 (1.0; 14,4)	34 (12,3; 15,0)	33 (1,2; 12,3)	**96** (3,5; 18,9)	34 (1,2; 14,2)
РФ	*Российская газета*	**Положительная**	12	6	5	4	0	10	1	0
		Нейтральная	**31**	**7**	**160**	**35**	**33**	**12**	**48**	**20**
		Отрицательная	11	0	54	4	2	3	25	0
		Суммарное кол-во статей	54 (2,0; 15,9)	13 (0,5; 8,9)	**219** (8,0; 26,8)	43 (1,6; 21,4)	35 (1,3; 15,4)	25 (0,9; 9,3)	74 (2,7; 14,5)	20 (0,7; 8,3)
	Коммерсантъ	**Положительная**	10	5	8	9	3	9	1	1
		Нейтральная	**23**	**9**	**113**	**39**	**19**	**26**	**39**	**12**
		Отрицательная	8	0	71	7	4	7	23	0
		Суммарное кол-во статей	41 (1,5; 12,0)	14 (0,5; 9,5)	**192** (7,0; 23,5)	55 (2,0; 27,4)	26 (1,0; 11,4)	42 (1,5; 15,7)	63 (2,3; 12,4)	13 (0,5; 5,4)

[137]Жирным шрифтом выделены максимальные значения количества статей по модальности. *Прим. автора*.

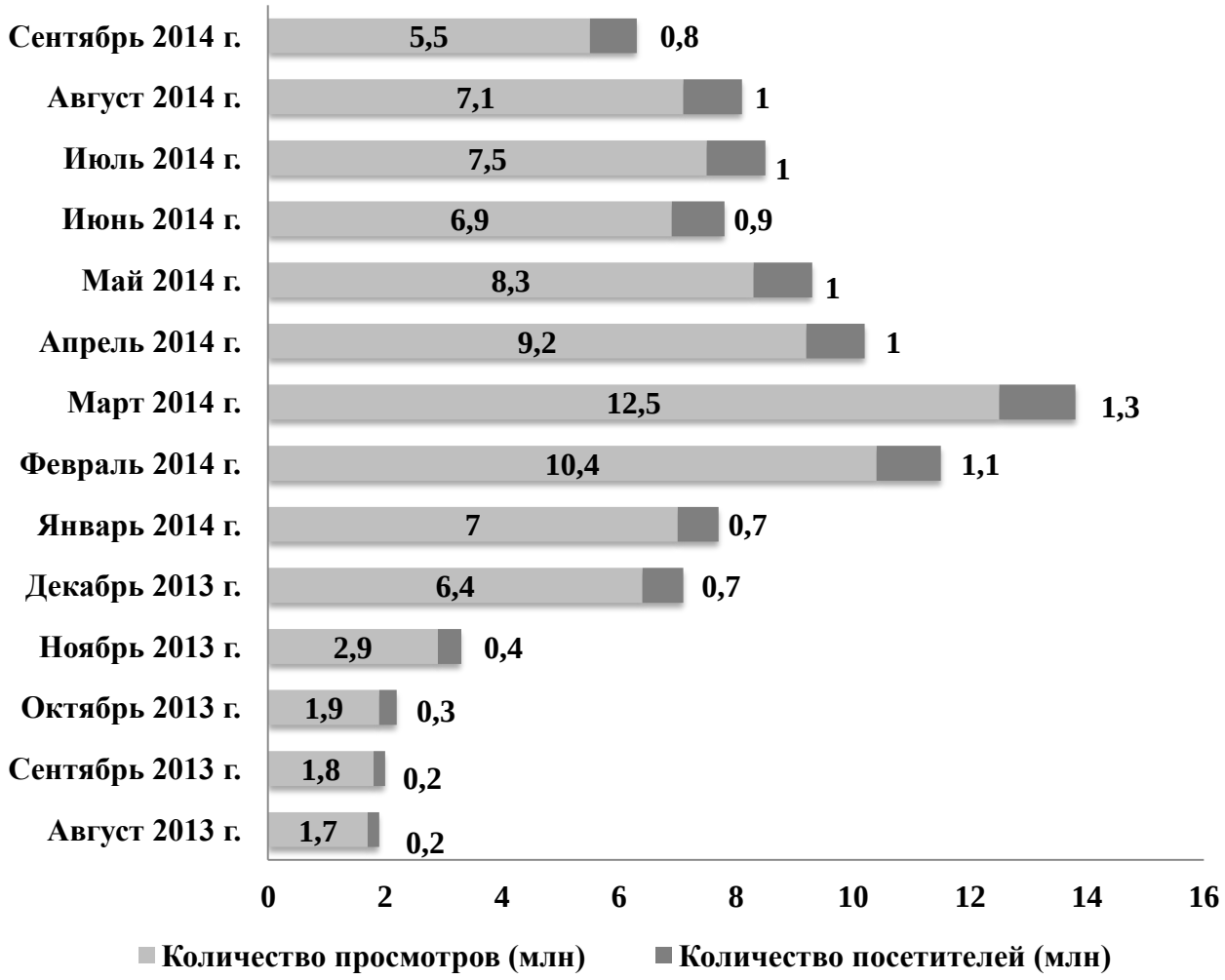
[138]Суммарное количество статей по теме равняется доле от общего числа статей; доля от общего числа статей по теме выражается в %. *Прим. автора*.

США	***CNN***	**Положительная**	0	0	3	1	6	0	0	6
		Нейтральная	0	**2**	**54**	**2**	**16**	16	**16**	8
		Отрицательная	0	0	52	1	0	**19**	12	**15**
		Суммарное кол-во статей	0 (0; 0)	2 (0,1; 1,4)	**109** (4,0; 13,4)	4 (0,1; 2,0)	22 (0,8; 9,6)	35 (1,3; 13,0)	28 (1,0; 5,5)	29 (1,0; 12.1)
	The New York Times	**Положительная**	0	0	0	1	**8**	0	0	0
		Нейтральная	0	**2**	**26**	**5**	5	9	8	**18**
		Отрицательная	0	0	18	0	0	**11**	**14**	14
		Суммарное кол-во статей	0 (0; 0)	2 (0,1; 1,4)	**44** (1,6; 5,4)	6 (0,2; 3,0)	13 (0,5; 5,7)	20 (0,7; 7,5)	22 (0,8; 4,3)	32 (1,2; 13,3)
Великобритания	***BBC***	**Положительная**	0	2	0	0	3	0	0	0
		Нейтральная	0	**17**	**39**	**22**	**29**	7	12	**22**
		Отрицательная	0	2	28	5	0	**32**	**18**	10
		Суммарное кол-во статей	0 (0; 0)	21 (0,8; 14,3)	**67** (2,4; 8,2)	27 (1,0; 13,4)	32 (1,2; 14,0)	39 (1,4; 14,5)	30 (10.,9; 5,9)	32 (1,2; 13,3)
	The Times	**Положительная**	0	**2**	1	0	2	0	0	0
		Нейтральная	0	1	17	**7**	**9**	8	**11**	**17**
		Отрицательная	0	**2**	**23**	6	0	**14**	5	5
		Суммарное кол-во статей	0 (0; 0)	5 (0,2; 3,4)	**41** (1,5; 5,0)	13 (0,5; 6,5)	11 (0,4; 4,8)	22 (0,8; 8,2)	16 (0,6; 3.1)	22 (0,8; 9,2)
Казахстан	***Казах. правда***	**Положительная**	**2**	0	5	0	0	0	0	0
		Нейтральная	1	**3**	**20**	0	0	**1**	**1**	**8**
		Отрицательная	**2**	0	4	0	0	0	0	0
		Суммарное кол-во статей	5 (0,2; 1,5)	3 (0,1; 2,0)	**29** (1,0; 3,6)	0 (0; 0)	0 (0; 0)	1 (0,04; 0,4)	1 (0,04; 0,2)	8 (0,3; 3,3)
	Tengri news	**Положительная**	0	0	0	0	0	0	0	0
		Нейтральная	**2**	**15**	**18**	**6**	**4**	**5**	**11**	**12**
		Отрицательная	1	0	15	0	0	0	0	0
		Суммарное кол-во статей	3 (0,1; 0,9)	15 (0,5; 10,2)	**33** (1,2; 4,0)	6 (0,2; 3,0)	4 (0,1; 1,7)	5 (0,2; 1,9)	11 (0,4; 2,2)	12 (0,4; 5,0)

Содержательный контент-анализ СМИ Украины включает инернет-статьи государственного информационного агентства «УКРИНФОРМ» (основано в 1918 году), среднесуточная аудитория которого составляет 149 тысяч человек[139], и украинского ежедневного аналитического журнала «Украинская правда» (основан в 2000 году) со среднесуточной аудиторией 591 тысяча человек.

Статистика посещения этих интернет-изданий показана на рисунках 1 и 2, откуда видно, что количество просмотров и посетителей растет с ноября 2013 года (21 ноября 2013 года в центре Киева началась массовая акция протеста – Евромайдан).

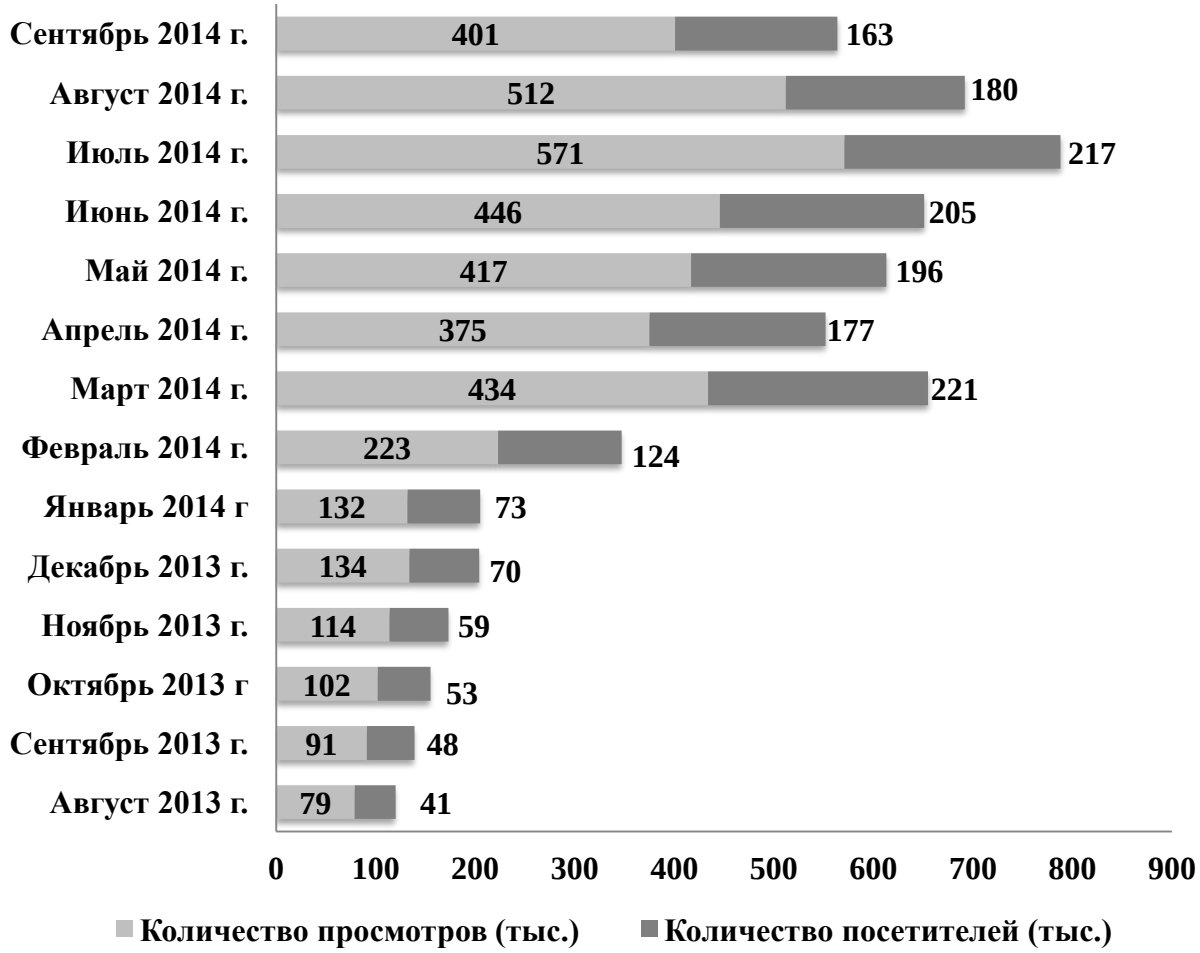
Рисунок 1.
Статистика посещения Интернет-издания «Украинская правда»



Источники: официальный сайт издания «Украинская правда».
(http://www.pravda.com.ua/rus/);
интернет-портал Liveinternet.
(http://www.liveinternet.ru/stat/ukrpravda/index.html?period=month;graph=table).

[139] Официальный сайт «УКРИНФОРМ»: об агентстве.(http://www.ukrinform.ua/rus/page/about_agency). Официальный сайт Liveinternet: статистика посещения Интернет-ресурсов (http://www.liveinternet.ru/stat/ukrinform.ua/index.html?avgraph=yes).

Рисунок 2.
Статистика посещения интернет-издания «УКРИНФОРМ»



Источники: официальный сайт «УКРИНФОРМ»: (http://www.ukrinform.ua/); интернет-портал Liveinternet. (http://www.liveinternet.ru/stat/ukrinform.ua/index.html?period=month;graph=table).

Анализ количества статей о роли РФ в кризисе на Украине в украинских СМИ, представленного на рисунке 3, позволяет сделать вывод, что изменение количества посетителей Интернет-ресурсов пропорционально изменению количества статей. Однако вид графиков изменения количества информации в этих двух СМИ различный, что говорит об отсутствии у них единого плана предоставления информации. При этом тенденции изменения количества статей в обоих источниках связаны с несколькими ключевыми событиями: решение Совета Федераций ФС РФ об использование ВС РФ на территории Украины; референдум о статусе Крыма, Постановление Государственного Совета Республики Крым «О независимости Крыма» и решение РФ об образовании в составе России новых субъектов. Однако экстремумы графика «Украинской правды» как одного из самых читаемых СМИ Украины намного значительнее, чем в «УКРИНФОРМ», что позволяет сделать выводы о том, на чем власти Украины делали акцент, а о чем старались умолчать.

Рисунок 3.
Количество статей о роли РФ в кризисе на Украине в «Украинской правде» и «УКРИНФОРМ»



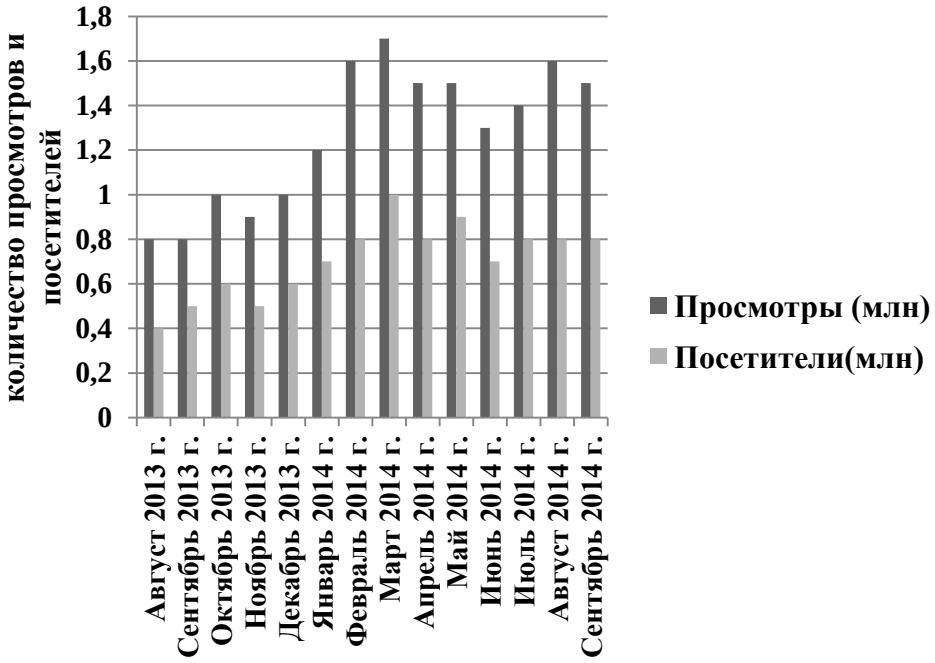
Источники: официальный сайт Интернет-издания «Украинская правда». (http://www.pravda.com.ua/rus/);
официальный сайт государственного информационного агентства «УКРИНФОРМ». (http://www.ukrinform.ua/rus/).

Контент-анализ СМИ Российской Федерации проводился по интернет-статьям *«Российской газеты»,* которая является ежедневным государственным изданием и официальным печатным органом Правительства РФ[140] (выходит с 1990 года), а среднесуточная аудитория составляет 490 тысяч человек и ежедневного общественно-политического издания *«Коммерсантъ»* (основано в 1991 году), среднесуточная аудитория которого – 213 тысяч челоаек.

На диаграммах статистики посещения издания «Российская газета» и новостного портала «Коммерсантъ» с августа 2013 года по сентябрь 2014 года (см. рис. 4 и 5) можно выделить два экстремума – март 2014 года и август 2014 года.

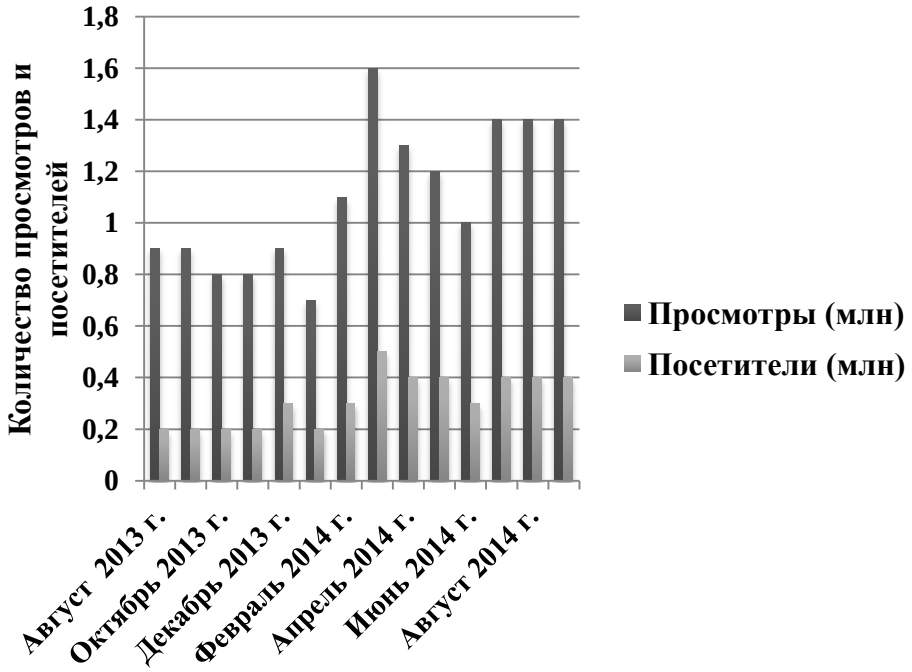
[140] Официальный сайт издания «Российская газета»: о газете. (http://rg.ru/about/index.html).

Рисунок 4.
Статистика посещения Интернет-издания «Российская газета»



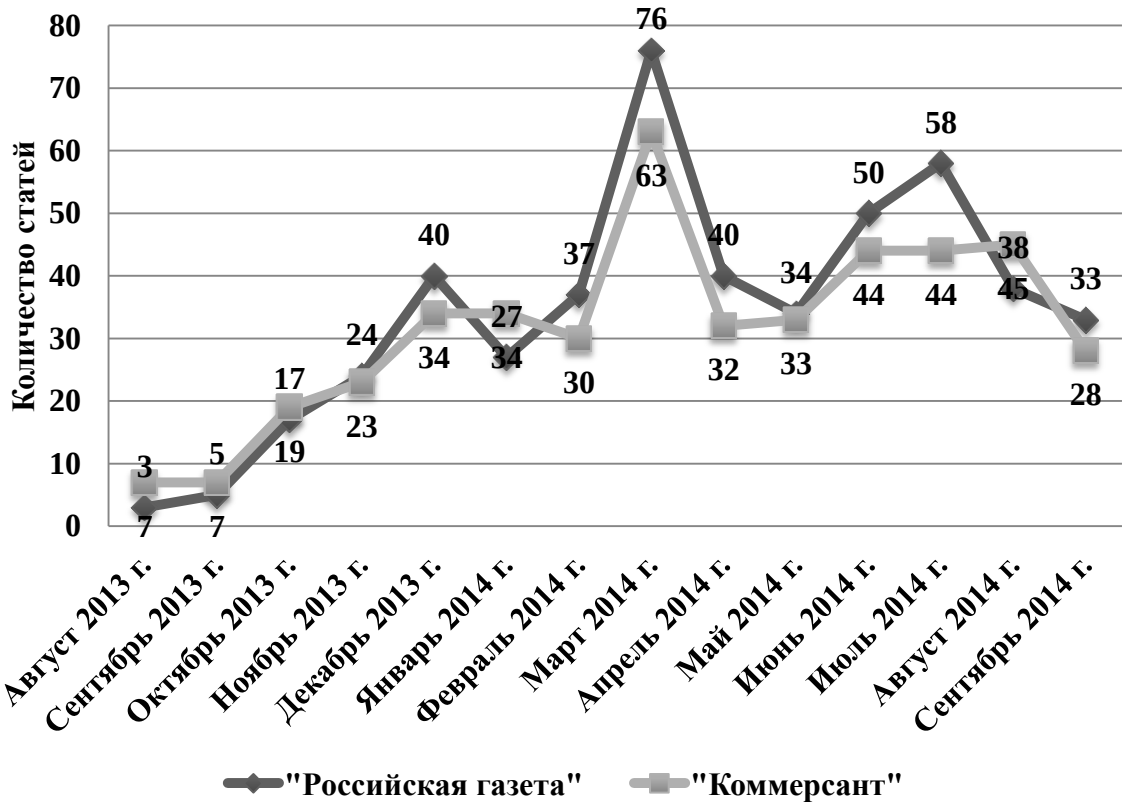
Источники: официальный сайт издания «Российская газета».(http://rg.ru/about/index.html);
интернет-портал Liveinternet.
(http://www.liveinternet.ru/stat/rg.ru/index.html?period=month;graph=table).

Рисунок 5.
Статистика посещения Интернет-издания «Коммерсантъ»



Источники: официальный сайт издания «Коммерсантъ». (http://www.kommersant.ru);
интернет-портал Liveinternet.
(http://www.liveinternet.ru/stat/kommersant.ru/index.html?period=month;graph=table).

Рисунок 6.
Количество статей, касающихся кризиса на Украине, в издании «Российская газета» и «Коммерсантъ»



Источники: официальный сайт издания «Российская газета». (http://www.rg.ru); официальный сайт издания «Коммерсантъ». (http://www.kommersant.ru).

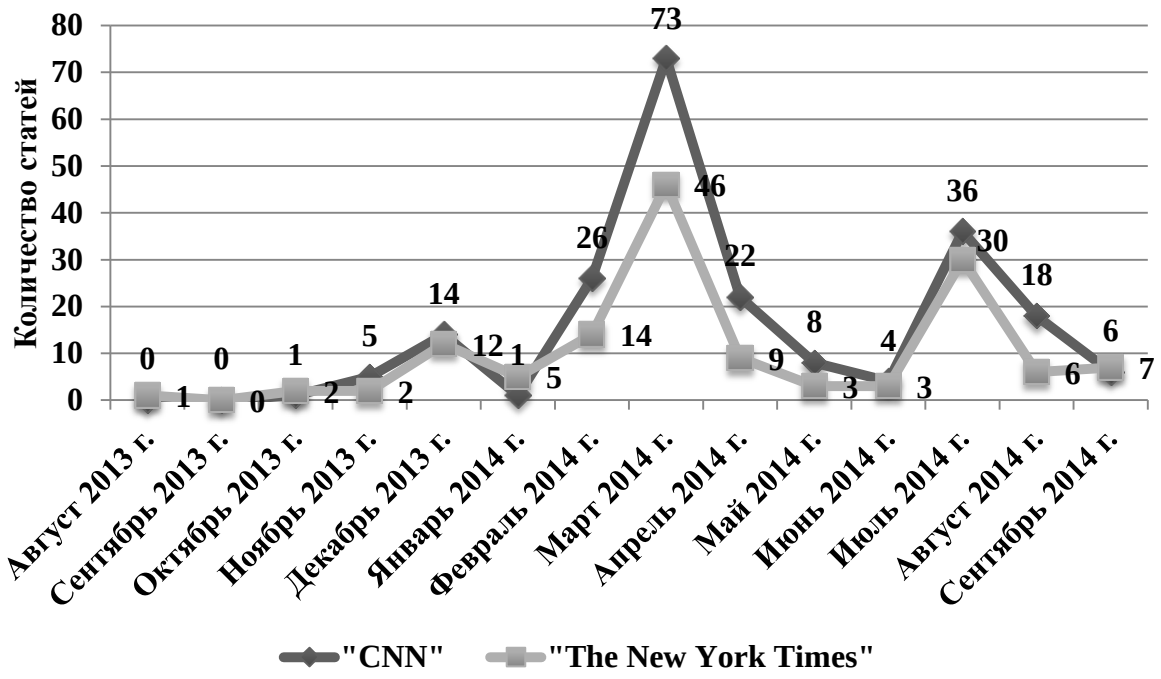
В ходе ***контент-анализа СМИ США*** исследовались интернет-статьи ежедневной международной службы новостей "CNN" (Cable News Network) (основана в 1980 году), большая часть информации которой формируется на основе государственных пресс-релизов и отчетов, а среднесуточная аудитория составляет 1,6 млн. человек и ежедневной американской газеты "The New York Times" (выходит с 1851 года), среднесуточная читательская аудитория которой 24 млн. человек.[141]

Показательно, что до декабря 2013 года события на Украине практически не освещались самыми авторитетными американскими СМИ (см. рис. 7). Более того, читателей "CNN" в ноябре, когда началась активная фаза украинского кризиса, было даже меньше, чем в предыдущие и последующие месяцы, а интерес читателей "The New York Times" к событиям на Украине снизился в декабре 2013 года. Это говорит о том, что исследуемые СМИ не стремились в эти месяцы привлечь к этой проблематике внимание своих читателей. Однако в марте 2014 года число статей "CNN", освещающих *кризис на Украине и роль России в нем*, почти в два раза больше количества статей украинских СМИ на эту тему. Отметим, что СМИ государства, находящегося за тысячи километров от происходящего, уделяли этому больше внимания, чем массмедиа России и Европы, расположенных по соседству с охваченной нестабильностью территорией. Учитывая огромную площадь

[141]Статистика посещения Интернет-ресурсов Compete.com. (https://siteanalytics.compete.com/nytimes.com/#.VGUFDL4kfh8).

распространения СМИ США, не трудно предположить объемы и последствия их воздействия.

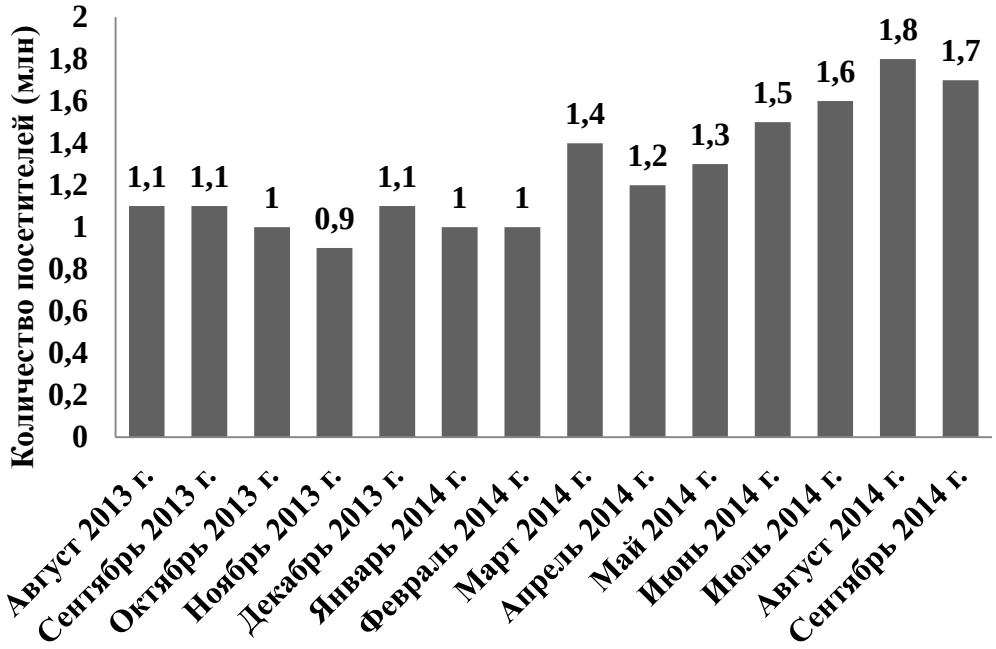
Рисунок 7.
Количество статей "CNN" (черный график) и The New York Times" (серый график), касающихся кризиса на Украине



Источники: сайт Интернет-портала "CNN". (http://edition.cnn.com); официальный сайт газеты "The New York Times". (http://www.nytimes.com).

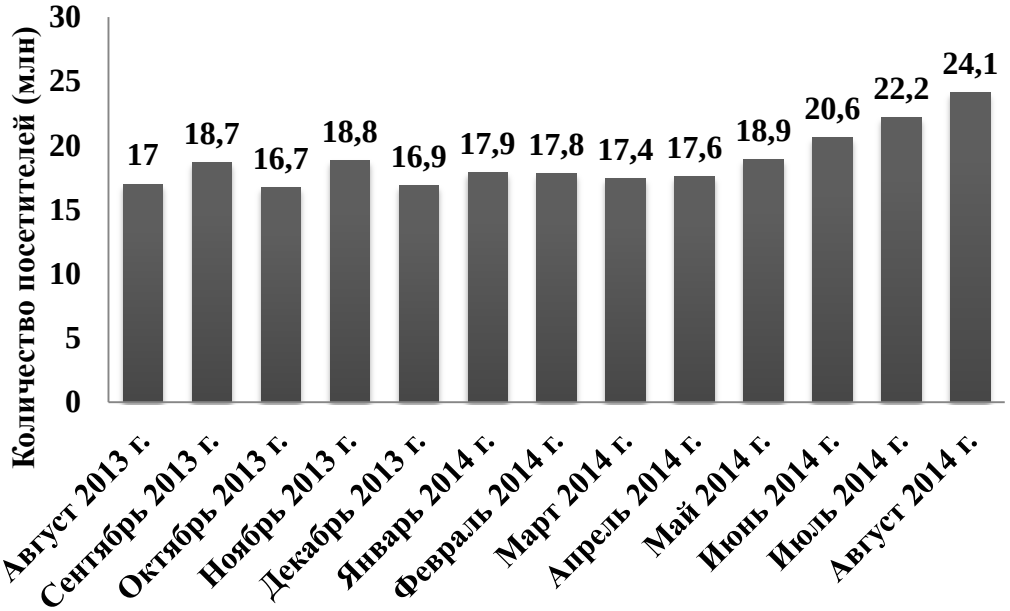
Несмотря на резкое увеличение количества статей об Украине в обоих изученных американских СМИ с февраля 2014 года, внимание к ним американских читателей росло не столь существенно, как в России и на Украине, о чем свидетельствует статистика посещений (см. рис. 8 и 9). Важно также, что интерес граждан США увеличился не столько в связи с включением Крыма в состав РФ в марте 2014 года, сколько позднее – в августе-сентябре. Вероятно, только тогда украинская проблематика уже была воспринята американским обществом, в том числе, в связи с военной фазой кризиса.

Рисунок 8.
Статистика посещения Интернет-портала "CNN"



Источник: статистика посещения Интернет-ресурсов Compete.com. (https://siteanalytics.compete.com/edition.cnn.com/#.VGUDJr4kfh8).

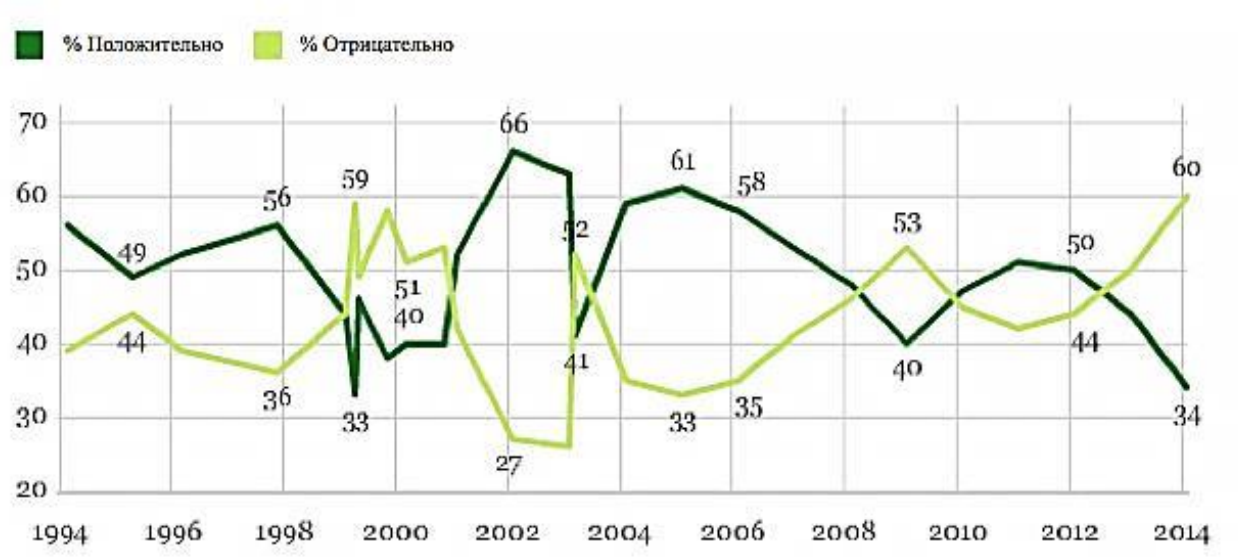
Рисунок 9.
Статистика посещения газеты "The New York Times"



Источники: статистика посещения Интернет-ресурсов Compete.com. (https://siteanalytics.compete.com/nytimes.com/#.VGUFDL4kfh8); официальноый сайт "The New York Times". (http://www.nytimes.com).

Результаты эффективности ИПВ целесообразно оценивать, в частности по данным социологических опросов. Так, согласно данным социологической службы Gallup, в 2014 году был зафиксирован самый высокий уровень негативного отношения американцев к России за последние 20 лет (см. рис. 10). Подобный уровень отношения к РФ имел место в 1999 году, когда шли военные действия в Чечне и Югославии.[142]

Рисунок 10.
Отношение населения США к России с 1994 по 2014 годов



В ходе ***контент-анализа СМИ Великобритании*** были исследованы интернет-статьи ежедневной службы новостей “BBC” (British Broadcasting Corporation) (основана в 1939 году) среднесуточная аудитория которой составляет 7,9 млн. человек[143], и ежедневной газеты “The Times” (выходит с 1785 году) со среднесуточной аудиторией в 393 тысячи человек.[144]

Количество статей по украинской проблематике за весь исследуемый период в СМИ Великобритании и США приблизительно равны. При этом графики изменения количества английских статей практически повторяют тенденции американских источников (см. рис. 11). Но интерес английских читателей к кризису на Украине, в отличие от американских, резко увеличился именно в марте 2014 года и продолжал неуклонно расти (см. рис. 12), несмотря на уменьшение количества информации на эту тему.[145]

Проранжированные по модальности статьи источников США и Великобритании, касающиеся кризиса на Украине, приведены в таблице 6.

---

[142] Americans' Views of Russia, Putin Are Worst in Years, Социологическая служба Gallup. (http://www.gallup.com/poll/167402/americans-views-russia-putin-worst-years.aspx?utm_source=alert&utm_medium=email&utm_campaign=syndication&utm_content=morelink&utm_term=Politics%20-%20USA).

[143]Статистика посещения Интернет-ресурсовCompete.com. (https://siteanalytics.compete.com/bbc.com/#.VGUWxb4kfh8).

[144]ABCs: National daily newspaper circulation. (http://www.theguardian.com/media/table/2014/jul/11/abcs-national-newspapers).

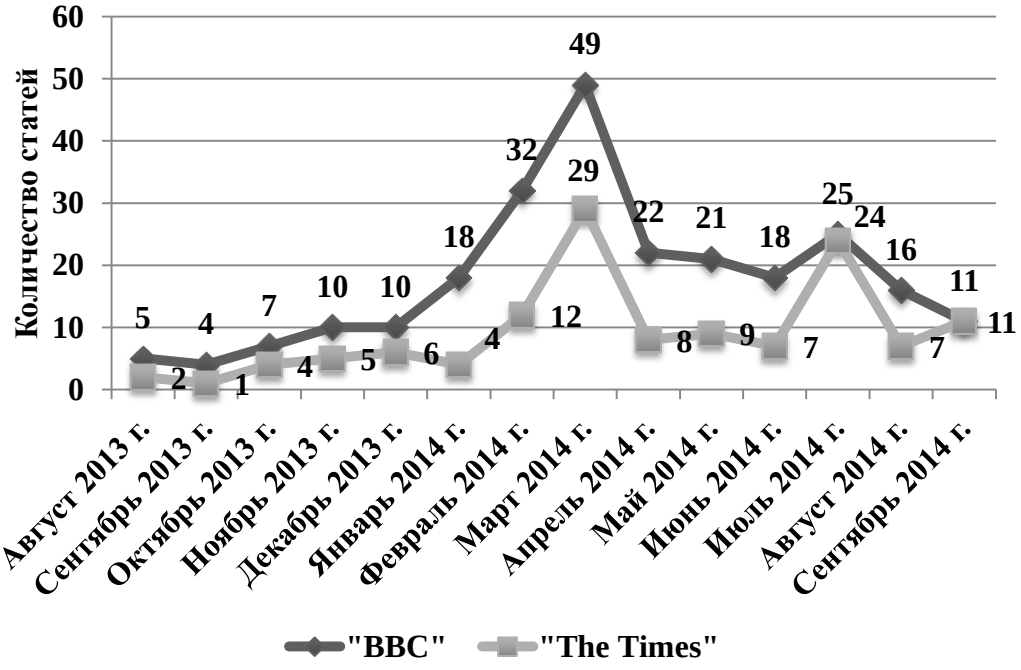
[145]Статистика посещения Интернет-ресурсов Compete.com. (https://siteanalytics.compete.com/bbc.com/#.VGUWxb4kfh8).

Официальный сайт BBC: aboutus.(http://www.bbc.co.uk/historyofthebbc/great_moments/index.shtml).

Официальный сайт Интернет-портала “BBC”. (http://www.bbc.co.uk).

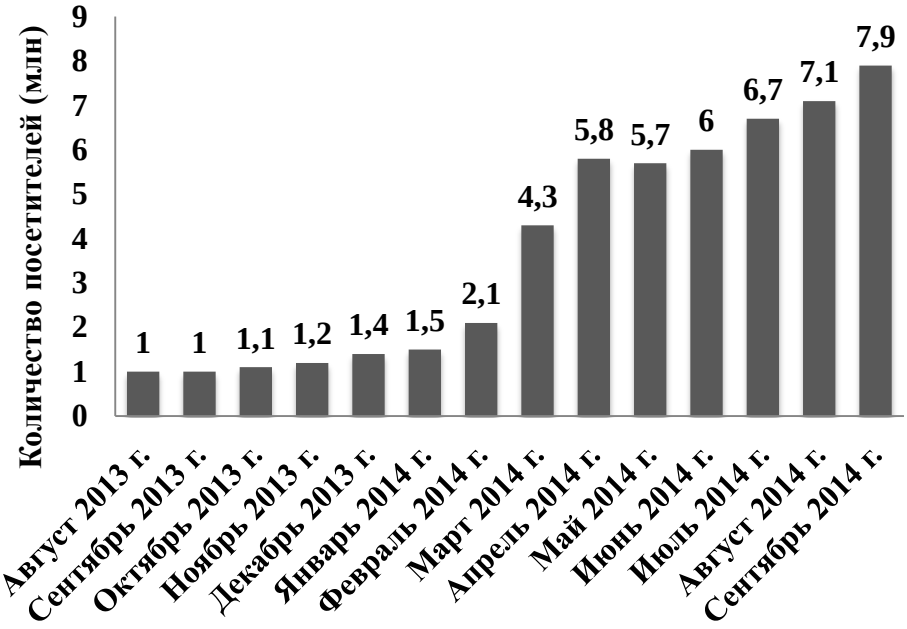
Официальный сайт “TheTimes”. (http://www.thetimes.co.uk).

Рисунок 11.
Количество статей “BBC” и "The Times”, касающихся кризиса на Украине



Источники: официальный сайт Интернет-портала “BBC”. (http://www.bbc.co.uk); официальный сайт газеты “The Times”. (http://www.thetimes.co.uk).

Рисунок 12.
Статистика посещения Интернет-портала “BBC”



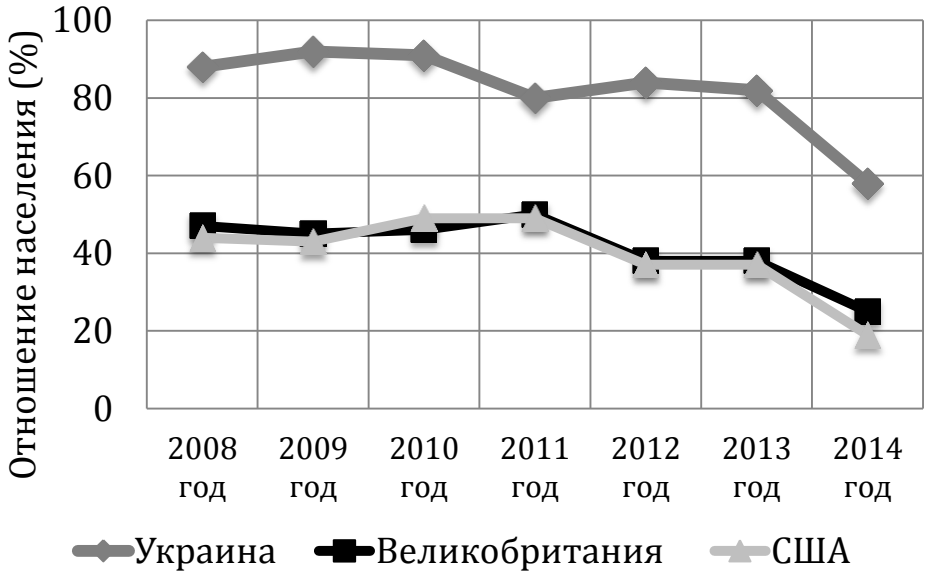
Источник: Статистика посещения Интернет-ресурсов Compete.com. (https://siteanalytics.compete.com/bbc.com/#.VGUWxb4kfh8).

Об эффективности ИПВ на Украине, в США и Великобритании также можно, в частности, судить по результатам социологических опросов, касающихся отношения граждан этих стран к России (результаты одного из которых представлены на рис. 13). Исследование проводилось с 17 марта по 5 июня 2014 года, были опрошены 48 643 человека из 44 стран мира. Им предстояло ответить на вопрос: «Как Вы относитесь к России: положительно или отрицательно?»

Согласно опросам российских и украинских аналитических центров (май и сентябрь 2014 года), россияне и украинцы видят отношения между странами следующим образом:

- по сравнению с маем 2014 года на Украине значительно возросло количество людей, поддерживающих закрытие границ с Россией (32% – май, 45% – сентябрь 2014 года); в России ситуация практически не изменилась (28% – май, 26% – сентябрь 2014 года);
- количество поддерживающих развитие дружеских и независимых отношений двух государств с открытыми границами без виз и таможен в России увеличилось на 8% (54% – май, 62% – сентябрь 2014 года), на Украине – уменьшилось на 10% (54% – май, 44% – сентябрь 2014 года).[146]

Рисунок 13.
Динамика отношения населения Украины, США и Великобритании к РФ за период 2008-2014 годов



Источник: Pew Research Center: Russia`s global image negative amid crisis in Ukraine. (http://www.pewglobal.org/2014/07/09/russias-global-image-negative-amid-crisis-in-ukraine/).

[146] Отчет аналитического центра Юрия Левады «Левада-центр»: отношения России и Украины в период кризиса на Украине 2013-2014 гг. (http://www.levada.ru/eng/russia-ukraine-relations-light-ukraine-crisis).

Интересными оказались результаты ***содержательного контент-анализа СМИ Казахстана,*** в ходе которого исследовались интернет-издания «Казахстанская правда» (основана в 1920 году) – ежедневное общенациональное издание, главный источник официальной и деловой информации в республике, среднесуточная аудитория которого составляет 11 тысяч человек[147], и “Tengri News” – относительно новое (с 2008 года) ежедневное общественно-политическое издание, среднесуточная аудитория которого составляет 60 тысяч человек.[148]

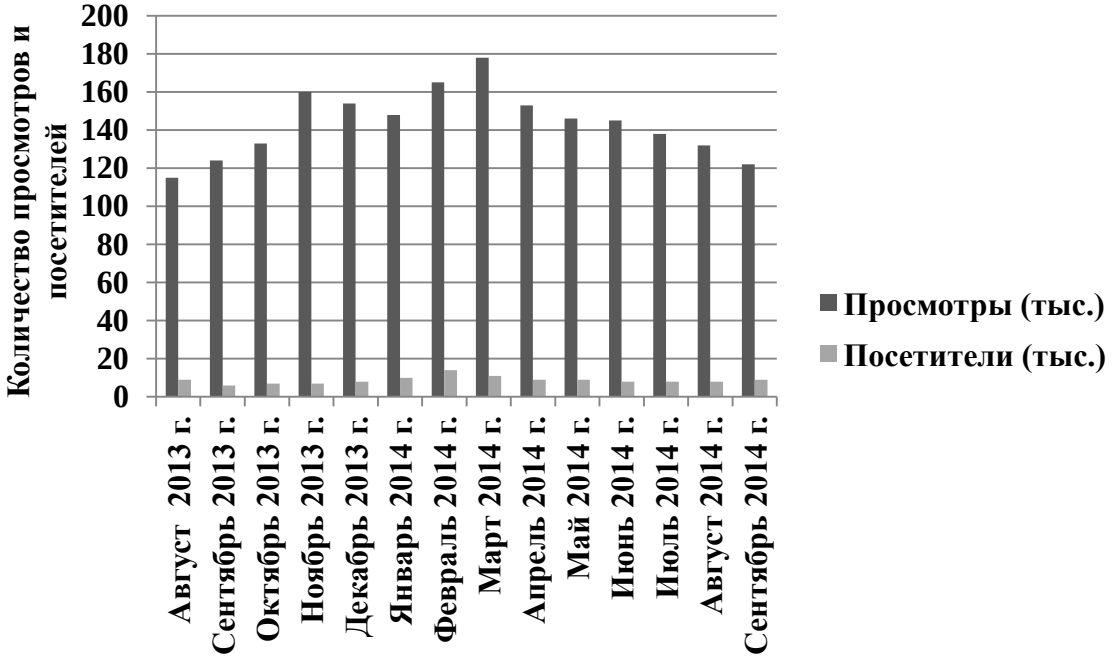
Рисунок 14.
Количество статей, касающихся кризиса на Украине, в издании “Tengri News” и «Казахстанская правда»



*Источники: о*фициальный сайт газеты «Казахстанская правда». (http://www.kazpravda.kz).;
официальный сайт издания «Tengri news». (http://tengrinews.kz);
Интернет-портал Liveinternet.
(http://www.liveinternet.ru/stat/tengrinews.kz/index.html?period=month;graph=table).

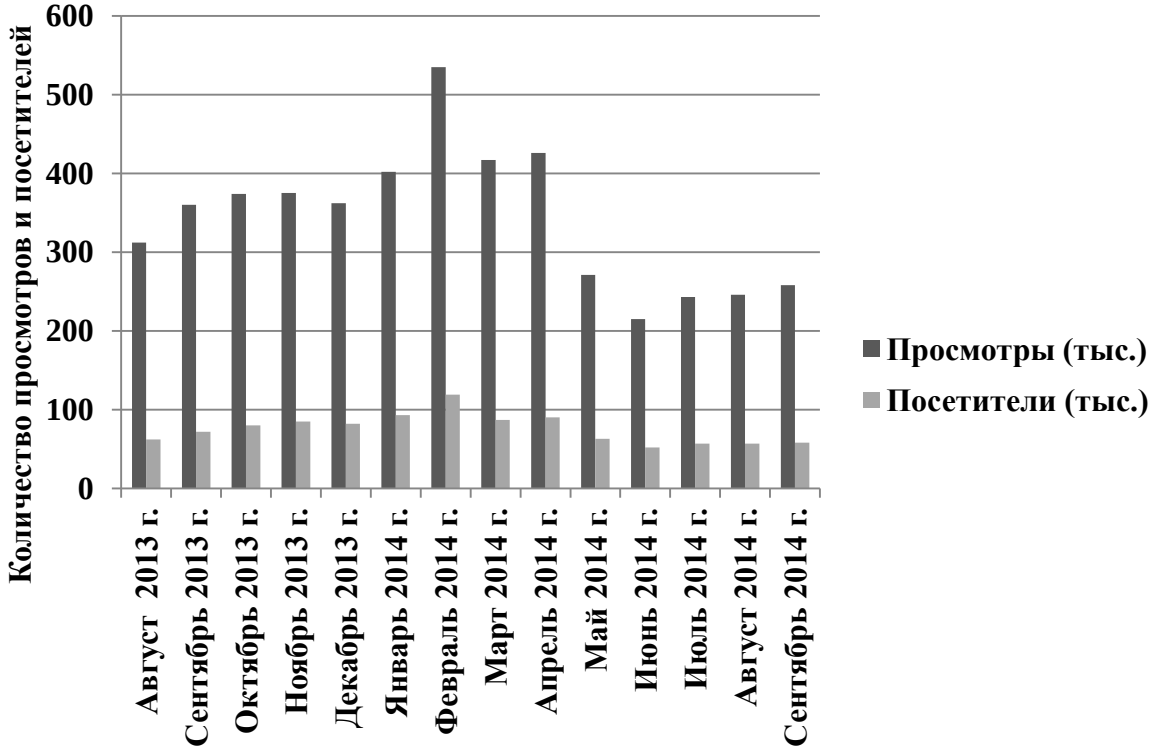
[147]Статистика посещения Интернет-ресурсов Liveinternet. (http://counter.yadro.ru/values?site=kazpravda.kz).
[148]Официальный сайт Zero.kz: статистика посещения Интернет-ресурсов.
(http://zero.kz/?c=11&sr=kz&pd=86400&p=1).

Рисунок 15.
Статистика посещения Интернет-издания «Казахстанская правда»



Источник: Интернет-портал Liveinternet.
(http://www.liveinternet.ru/stat/kazpravda.kz/index.html?period=month;graph=table).

Рисунок 16.
Статистика посещения Интернет-издания "Tengri News"



Источник: Интернет-портал Liveinternet.
(http://www.liveinternet.ru/stat/tengrinews.kz/index.html?period=month;graph=table).

Интерес вызывает следующая тенденция: несмотря на то, что в газете «Казахстанская правда» количество информации о событиях на Украине резко возросло уже в декабре 2013 года (см. рис. 14), интерес ее читателей к ним увеличился только в марте, притом не существенно. В целом можно говорить о достаточно равномерном характере графика изменения количества посетителей «Казахстанской правды» в течение всего года (см. рис. 15).

Другая тенденция наблюдается в “Tengri News”: его авторы увеличили количество статей по украинской проблематике в декабре 2013 года в ответ на рост своей аудитории в ноябре. В дальнейшем можно говорить об одинаковых тенденциях к изменению и в количестве информации об украинском кризисе, и в количестве читателей “Tengri News” (см. рис. 16).

Таким образом, динамика количества статей, просмотров и посетителей в негосударственных («Tengri news») и государственных («Казахстанская правда») СМИ существенно отличается. Особенно сильно различие просматривается в количестве статей: между графиками их изменения отсутствует корреляция.

Для Казахстана последствия применения методов ИПВ выражаются пока в большей степени неявно. В первую очередь речь идет о постепенном росте негативного отношения к России среди части населения страны, более подверженной информационно-психологическому воздействию.

При этом можно отметить наращивание двусторонних отношений Казахстана с Украиной за период кризиса. Так, Казахстан стал одним из первых, кто поддержал идею проведения внеочередных выборов президента Украины, и единственной страной СНГ, направившей своих национальных наблюдателей на эти выборы. Казахстан не присоединился к санкциям против Украины и ЕС в рамках Таможенного Союза. В ходе рабочего визита президента Н. Назарбаева на Украину в декабре 2014 года обсуждался вариант возобновления сотрудничества между странами, активизации сотрудничества в энергетической, машиностроительной, авиастроительной, космической отраслях и углубления кооперации в военно-технической сфере.[149] Были достигнуты договоренности о поставке на Украину угля из Карагандинского и Экибастузского угольных бассейнов и об углублении двустороннего сотрудничества Украины и Казахстана в рамках ВТО.

Общий анализ данных о модальности статей (таблица 5) показывает, что максимальные показатели количества статей СМИ Украины приходится в основном на статьи с отрицательной модальностью, причем иногда отрицательных сообщений в 3 раза больше суммы положительных и нейтральных. Украинские СМИ максимально пытались сформировать негативный образ соседа во всех контекстах, что способствовало проведению антироссийской политики. В Приложении С приведены конкретные примеры из статей СМИ Украины, касающихся роли РФ в кризисе на Украине, проранжированные по модальности.

Интересно, что российские газеты не так критичны по отношению к Украине: количество статей с отрицательной модальностью находится примерно на одном уровне с положительными упоминаниями. Кроме того, неожиданным стал вывод о том, что максимальное количество статей по всем выбранным темам и вопросам в обоих российских СМИ несли в тот период нейтральную окраску. Только Россия показала такой результат в данном контент-анализе. На втором месте по нейтральности за исследуемый период находился Казахстан.

На этом этапе США и Великобритания активно осуждали Россию за *эскалацию кризиса на Украине:* количество статей по этому вопросу было больше количества аналогичных статей украинских СМИ. При этом число американских публикаций превышало количество украинских в полтора раза. Напомним, что территория

[149]Официальный сайт президента Казахстана. (http://www.akorda.kz/ru/page/page_218776_vstrecha-s-premer-ministrom-ukrainy-arseniem-yatsenyukom#page).

распространения СМИ США самая большая, что говорит об эффективности их намерений при освещении событий максимально подчеркнуть негативную роль России в украинском кризисе на всей англоязычной территории планеты. При этом для американских и британских СМИ *тема двусторонних отношений РФ и Украины* либо не представляла интереса, либо умышленно замалчивалась, о чем свидетельствует отсутствие статей по этому вопросу.

Интересно отметить, что негосударственные СМИ Казахстана ("Tengri news") также негативно высказывались в отношении *роли РФ в эскалации кризиса*, но количество негативных публикаций по этому вопросу было меньше чем в государственных СМИ («Казахстанская правда»). По другим вопросам положительные и отрицательные статьи в основном вообще отсутствуют.

Статьи о *роли РФ в ассоциации Украины с ЕС*, как и следовало ожидать, в основном интересовали саму Украину и Великобританию как члена Евросоюза. Украина рассматривала роль России в большинстве статей негативно, тогда как Великобритания придерживалась в этом вопросе нейтральной позиции. Нейтральность демонстрировали СМИ России, США и Казахстана.

Говоря о *санкциях против РФ*, наибольшую активность проявила пресса Украины и Великобритании. Украинские СМИ подчеркивали важность и необходимость введения санкций, в то время как модальность упоминаний в британских газетах, в основном, была нейтральной.

Тема присоединения Республики Крым к РФ наиболее полно отразилась в статьях СМИ Украины (79 статей), РФ (67 статей) и Великобритании (61 статья). В российских газетах за указанный период времени анализ показал максимальное количество публикаций с нейтральной модальностью и по этой теме. СМИ Украины и Великобритании трактовали событие с отрицательной оценкой. Пресса США посвятила этому вопросу 55 статей, 30 из которых – отрицательные, а Казахстана – 6 нейтральных статей.

Наибольшее количество публикаций с негативным содержанием в СМИ Украины занимала тематика *роли РФ в вооруженном конфликте на Юго-Востоке Украины:* 217 негативных из 264 статей в «Украинской правде» и «Укринформ». РФ также уделяла конфликту большое внимание: 137 статей в обоих СМИ, 87 из которых носят нейтральный характер. США опубликовали 50 статей на данную тему, Великобритания – 46, и большая из них обвиняет Россию в развязывании военных действий.

Крушение Боинга 777 компании «Малазийские авиалинии» (Амстердам – Куала-Лумпур) в районе вооружённого противостояния на Востоке Украины 17 июля 2014 года, в результате которого погибло 298 человек, стало ключевым для отношений России и Европы событием. Именно его освещение в мировых СМИ, повлиявшее на восприятие миллионов людей, стало катализатором многих негативных для РФ и Европы процессов. В ходе контент-анализа был исследован вопрос о том, как трактовался региональными СМИ вопрос непричастности России к этой катастрофе. До сентября 2014 года этой теме было посвящено 70 статей заданного объема «Украинской правды» и «Укринформ», что на 20% меньше количества публикаций *о санкциях и о роли России в эскалации кризиса на Украине* и на 10% меньше числа публикаций *о присоединении Крыма*. Среди них нет ни одной, подтверждающей непричастность России к катастрофе, при этом 55 публикаций носят ярко негативный характер. Интересно отметить, что "CNN" и "The New York Times" посвятили этой теме 61 статью, что превышает количество публикаций по другим выделенным вопросам, однако в 2,5 раза меньше количества статей, посвященных *роли РФ в эскалации украинского кризиса*. Пресса Казахстана уделила трагедии достаточно большое внимание по сравнению с другими темами.

Таким образом, контент-анализ позволил выделить вопросы по украинской проблеме, на которых делался основной акцент СМИ выбранных стран в период с августа 2013 г. по

сентябрь 2014 г. Для обеих газет Украины – это максимально негативное освещение вопросов о *роли России в вооруженном конфликте на Юго-Востоке Украины*. «Коммерсант» и «Российская газета» максимальное внимание уделили теме *эскалации кризиса на Украине.* Оба американских источника максимально освещали для своей аудитории вопросы *роли России в эскалации кризиса на Украине* и *крушения малазийского Боинга*. Подобная ситуация наблюдается и в отношении казахских газет, но при этом общее количество их статей по украинской проблеме в разы меньше числа американских. “CNN” также сравнительно много публикаций посвятила теме *присоединения Крыма*. Показательно, что английская пресса уделила *трагедии малазийского самолета*, в которой погибло 210 граждан ЕС (192 гражданина Нидерландов, 10 — Великобритании, 4 – Бельгии и 4 — Германии) значительно меньше внимания, чем *роли России в эскалации кризиса на Украине*.

Некоторые примеры практического применения методов ИПВ на Украине в период кризиса, дополняющие данные таблицы 1 с их теоретическим описанием, представлены в таблице 6.

Таким образом, информационно-психологическая операция на Украине включает сложную совокупность согласованных и скоординированных по целям, месту и времени операций стратегического характера, которые проводились как до перехода кризиса в активно-силовую фазу, так и в условиях эскалации. При этом динамика информационного противоборства отражала события реальной политики: переход «майдана» в летальную фазу 19-20 февраля 2014 года и последовавшее насильственное свержение президента В.Ф. Януковича; обращение президента В.В. Путина за санкцией Совета Федерации на использование ВС РФ на Украине 28 февраля 2014 года; этапы процесса присоединения Крыма к России в марте; распространение насильственных действий в Новороссии и начало вооруженного подавления оппозиции украинскими войсками в апреле, нарушение ими первого перемирия в июле и контрнаступление ополчения Юго-Востока в конце августа, минские договоренности 5-19 сентября 2014 года и последующие события. Указанная политическая реальность создавала своего рода жесткий «поддон» общественного восприятия событий. На это восприятие накладывался глубокий отпечаток информационно-психологической кампании, которая резко обострила отношения России, Украины и Запада, превратила локальный кризис в военно-политическую и экономическую конфронтацию глобального значения.

События на Украине, к сожалению, позволяют утверждать, что цели этой глобальной операции – достижение устойчивого результата в формировании общественного мнения в заданном автором воздействия ключе; создание механизмов, при воздействии на которые произойдет запланированная (ожидаемая субъектом воздействия) реакция в массовом общественном подсознании; стимулирование необходимых процессов; управление социальным поведением; свержение власти и подчинение воли руководителей страны – сегодня достигаются.

Таблица 6.
Примеры применения методов ИПВ на Украине в 2013-2014 годах

Группа методов	Метод	Пример применения метода
Трансляция деформированных образов	***Искажение объемов***	Существенное занижение данных о количестве украинских беженцев (всего 5 статей в «Украинской правде» за июнь 2013 г.). Завышение количества участников Евромайдана: «Украинская правда» от 24.11.2013: 150 тыс. человек, что больше, чем данные СМИ Европы и РФ. Преуменьшение количества погибших украинских военных в «зоне АТО».
	Упрощение темы	«Мы глубоко обеспокоены планами России провести масштабные воздушные учения ***неподалеку от украинской границы*** на этой неделе. Подобные маневры провокационны и ведут только к эскалации ситуации», – отметила Псаки».[150] Официальное заявление МО РФ: учения проходили на полигоне Ашулук (Астраханская обл.) ***в 1000 км от территории Украины***.[151]
	Внедрение деформированной информации	«Захват вооруженными людьми двух аэропортов в Крыму министр внутренних дел Украины расценивает как российское «военное вторжение и оккупацию».[152]
	Изменение причинно-следственных/ временных/ пространственных связей	"The Times": «Решение Совета Федерации РФ (об использовании вооруженных сил РФ на территории Украины) является де-факто захватом Крыма».[153]

[150]Официальный сайт «УКРИНФОРМ». (http://www.ukrinform.ua/rus/news/provokatsionnie_manevri_rossii_obespokoili_ssha_1655017).
[151]Официальный сайт МО РФ. (http://www.ntv.ru/novosti/1186676).
[152] "The Times". (http://www.thetimes.co.uk/tto/news/world/europe/article4018940.ece).
[153]"The Times". (http://www.thesundaytimes.co.uk/sto/news/ireland/article1382221.ece).

	Имитационная дезинформация	«Министр иностранных дел РФ Сергей Лавров на четырехсторонних переговорах сегодня заявил, что не поддерживает идею «непроницаемости государственной границы». «Об этом мы не договорились», – заявил он. Другими словами, российские наемники, военная техника и оружие из России, по-прежнему, будут идти потоком в Украину».[154]
Использование референтных групп	***Идентификация с референтной группой***	Студенты ряда вузов Киева, Львова и Ивано-Франковска призвали своих коллег в других городах присоединиться к забастовке за евроинтеграцию.[155]
	Метод ссылки на авторитет	«Официальный представитель Пентагона Джон Кирби заявил, что Россия стянула к границе с Украиной более 10 тыс. солдат, причем сейчас они расположены еще ближе к границе, чем весной».[156]
Сравнение и контраст	***Сравнение***	Многочисленные примеры сравнения представителей власти РФ с лицами, имеющими негативные образы в общественном сознании, в СМИ Украины, США и Европы.
	Контраст	Использование визуального ряда для формирования положительного отношения к Евромайдану (счастливые лица людей всех возрастов на фоне флага ЕС) и отрицательного – к действующей власти (фото агрессивно настроенных представителей украинской милиции) в СМИ Украины, США, Европы.

[154]«УКРИНФОРМ». (http://www.ukrinform.ua/rus/news/utratim_illyuzii_1658540).
[155]«Украинская правда». (http://www.pravda.com.ua/rus/photo-video/2013/11/27/7003221/).
[156]«УКРИНФОРМ». (http://www.ukrinform.ua/rus/news/rossiyskaya_armiya_priblizilas_k_ukraine___pentagon_1653487).

Рефрейминг информации	***Перенос выводов и умозаключений***	1. Смещение акцента участников Майдана с вопроса европейской интеграции Украины на требования смены руководства страны перед выводом кризиса в боевую фазу с использованием всех видов СМИ Украины. 2. “CNN”: «На всероссийском молодежном форуме «Селигер-2014» В.В. Путин сказал, что Москва не хочет и не намерена участвовать в каком-либо масштабном конфликте. «Мы всегда должны быть готовы отразить любую агрессию в отношении России и (потенциальные враги) должны понимать, что с нами лучше не связываться, что касается возможного вооружённого конфликта», – отметил Президент. Это заявление было сделано в тот же день, когда британский источник в правительстве сообщил о значительном продвижении российских войск на территорию Украины».[157]
	Формирование предопределений	“CNN”: «Россия готовится к передаче более мощного оружия на территорию Украины, и это может произойти в любое время», - заявил секретарь Пентагона со ссылкой на последние данные разведки США. Считается, что вооружение будет передано на Украину «скорее всего сегодня», но неясным остается факт участия в операции русских войск».[158]
Ненасильственное убеждение	***Официальные заявления***	Официальное заявление экс-премьера Украины Ю.В. Тимошенко от 30 ноября 2013 г. с призывами «выступить против диктатуры и насилия В. Януковича».[159]
	Общественные собрания	Массовая многомесячная акция «Евромайдан» в центре Киева. Проведение народного вече на Площади Независимости в Киеве 1.12.2013[160]. Факельные шествия в Киеве 01.01.2014 г., 29.04.2013, 01.01.2015[161]

[157]“CNN”. (http://edition.cnn.com/2014/08/29/world/europe/ukraine-crisis/index.html?iref=allsearch).
[158]“CNN”. (http://edition.cnn.com/2014/07/25/world/europe/ukraine-crisis/index.html?iref=storysearch).
[159]«Украинская правда». (http://www.pravda.com.ua/rus/news/2013/11/30/7003807/).
[160]«УКРИНФОРМ». (http://www.ukrinform.ua/rus/news/maydan_provedet_narodnoe_veche_1_dekabrya_1581934).
[161]Официальный сайт «Первого канала». (http://www.1tv.ru/).

Глава 5. Национальная и международная деятельность России в процессе обеспечения информационной безопасности

Система РФ по обеспечению информационной безопасности

Термин «информационная безопасность» (ИБ) появился в российской нормативно-правовой базе в качестве самостоятельной составляющей понятия «безопасность» в Федеральном законе «О безопасности» 1992 года: «Совет безопасности РФ рассматривает вопросы внутренней и внешней политики в области *обеспечения* безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, информационной, экологической и иных видов *безопасности*, охраны здоровья населения, прогнозирования, предотвращения чрезвычайных ситуаций и преодоления их последствий, обеспечения стабильности и правопорядка…» (Ст. 13).[162]

В Федеральном законе «Об участии в международном информационном обмене» от 1996 года (утратил силу в 2006 году) ***информационная безопасность*** определялась как «*состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства*».[163]

Это определение было конкретизировано в Доктрине информационной безопасности Российской Федерации[164], принятие которой в 2000 году стало важным результатом одного из первых этапов процесса формирования нормативно-правовой организационной структуры системы обеспечения ИБ. Доктрина явилась развитием Концепции национальной безопасности России.

Согласно национальному стандарту РФ ГОСТ 13335-1 от 2006 года, ***информационная безопасность*** включает *все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки*.[165]

Вариации определений ИБ были основаны на британском стандарте BS 7799 (ISO 17799) «Информационно-технологическая безопасность» (Information Technology Security) разработанным Британским институтом стандартов (British Standards Institution) в 1995 году: ***информационная безопасность*** *– это защищенность ресурсов информационной системы от факторов, представляющих угрозу для конфиденциальности, целостности и доступности информации.*

В настоящее время в России действует более 50 законов, которые связаны с обеспечением ИБ, а также множество нормативных правовых актов Президента и Правительства РФ (см. Приложение D).

Россия является одной из стран-организаторов ежегодного международного мини-симпозиума «Современные тенденции в криптографии» для поддержки научных исследований в области теоретической и практической криптографии, а в 2011 году

[162] Закон РФ от 5 марта 1992 г. N 2446-I« о безопасности». (http://base.garant.ru/10136200/).
[163] Федеральный закон от 04.07.1996 N 85-ФЗ (ред. от 29.06.2004) Об участии в международном информационном обмене. (http://www.consultant.ru/document/cons_doc_LAW_48401/).
[164] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г., № Пр-1895). Москва: Ось-89, 2004.
[165] Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. (http://docs.cntd.ru/document/gost-r-iso-mek-13335-1-2006).

инициировала международный форум по кибербезопасности с целью выработки правил поведения в киберпространстве.

В 2012 году в рамках создания Государственной системы обнаружения и предупреждения компьютерных атак (ГосСОПКА), нацеленной на консолидацию усилий всех министерств и ведомств РФ для эффективного противодействия компьютерным атакам и опасным деструктивным воздействиям, в России создан и функционирует центр реагирования на компьютерные инциденты в органах государственной власти РФ (gov-cert.ru), в полномочия которого входит сбор и анализ информации о компьютерных атаках, а также взаимодействие с центрами по компьютерным инцидентам (Computer Emergency Response Team – CERT) других стран и организаций.[166]

В принятом в 2013 году документе «Основы государственной политики в области международной информационной безопасности на период до 2020 года» дается определение ***международной информационной безопасности (МИБ)*** как *такого состояния глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.*[167]

«Весь мир наблюдает за лавинообразным ростом угроз в информационной среде, и Россия оказалась в числе первых государств, которые озаботились поиском решений в сфере международной информационной безопасности». Решить задачу исключительно в национальном формате не по силам даже ведущим мировым державам. Необходимо формирование комплексной системы МИБ. Россия «стремится к установлению двусторонних и многосторонних отношений, способствующих обеспечению безопасности в информационной сфере».[168]

Под ***системой международной информационной безопасности,*** необходимой для оказания противодействия угрозам стратегической стабильности и обеспечения равноправного стратегического партнерства в глобальном информационном пространстве понимается *совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.*[169]

К *триаде угроз*, связанных с *применением информационного оружия*, во-первых, *в военно-политических целях для осуществления враждебных действий и актов агрессии*, во-вторых, *в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры* и, в третьих, *для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ* «Основы» добавили *опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни*. По сути это стало реакцией России на «цветные революции» и события «арабской весны», когда социальные сети и блоги активно использовались для создания и координации протестного движения.

Согласно «Основам государственной политики в области международной информационной безопасности на период до 2020 года», Россия ставит целью содействие установлению международного правового режима, направленного на создание условий для

[166]Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации. Международное название GOV-CERT.RU. (http://gov-cert.ru/index.html).
[167]Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Сайт Совет Безопасности Российской Федерации. (http://www.scrf.gov.ru/documents/6/114.html).
[168]Итоги Инфофорум 2014. (http://2014.infoforum.ru/infoforum-2014-itogi/).
[169]Там же.

формирования эффективной системы информационной безопасности. Для этого, среди прочего, необходимо создать основы, обеспечивающие снижение риска использования ИКТ для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности. Напомним, что в Концепции внешней политики РФ указано, что Россия будет добиваться выработки под эгидой ООН правил поведения при обеспечении МИБ.

С 10 января 2014 года в Совете Федерации стал доступным для обсуждения проект концепции Стратегии кибербезопасности РФ[170], которая обрисовывает первоначальную структуру организационных усилий, однако она не принята до настоящего времени в связи с ускоренным нарастанием и трансформацией угроз в этой сфере.

Нарастание угрозы использования информационных и коммуникационных технологий в противоправных целях, а также в нарушение принципов международного права постоянно подчеркиваются Министерством иностранных дел России. На заседании коллегии МИД РФ по теме: «Глобальные вызовы в области информационных технологий. Задачи МИД по обеспечению международной информационной безопасности» в мае 2015 года обсуждалась необходимость принятия адекватных мер в самом широком масштабе в борьбе с современными военно-политическими, террористическими и криминальными угрозами в информационной сфере, которые носят глобальный характер. Российским приоритетом при этом остается выработка универсальных правил ответственного поведения государств в информационном пространстве, которые бы препятствовали попыткам совершения актов агрессии, закрепляли бы принципы уважения государственного суверенитета, невмешательства во внутренние дела других государств, основных прав и свобод человека. Подчеркивается необходимость работы на важнейших площадках по продвижению российских инициатив в области международной информационной безопасности – в ООН и других международных организациях. Особо выделено значение взаимодействия Российской Федерации в рамках таких структур, как СНГ, ШОС, ОДКБ, БРИКС. На коллегии было признано востребованным дальнейшее углубление партнерских связей со странами, разделяющими подходы и позиции России в вопросах обеспечения МИБ. Акцентировалось значение развития двустороннего взаимодействия со всеми государствами, проявляющими готовность противостоять попыткам милитаризации информационной сферы, содействовать выработке международных норм и принципов, обеспечивающих мирное и стабильное использование глобальных телекоммуникационных сетей. По итогам заседания были намечены конкретные меры, направленные, в частности, на обеспечение участия Российской Федерации в саммитах ШОС и БРИКС в июле 2015 года, а также ряде важных форумов в других странах, посвященных вопросам международной информационной безопасности.

Проблемы международного сотрудничества в сфере информационной безопасности

Развитие и распространение информационных операций, милитаризация информационных технологий и рост неуправляемости в сфере ИКТ оказывают разрушительное влияние на всю систему международных отношений и договоренностей. Особенно это угрожает тем странам, в которых активно развиваются информационно-телекоммуникационные системы, автоматизированные системы государственного и военного управления, управление предприятиями и инфраструктурами, совершенствуются системы подготовки кадров высшей квалификации по вопросам обеспечения ИБ как на техническом, так и на правовом уровне при оптимальном сочетании этих форм.

[170]Концепция Стратегии кибербезопасности Российской Федерации. Сайт Совета Федерации Федерального Собрания Российской Федерации. (http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf).

Правовое обеспечение формируется по мере того, как развитие технологий вызывает изменение социальных отношений, требующих дополнительного регулирования. В современном информационном законодательстве, как российском, так и зарубежном, постепенно появляется все больше технических норм и терминов, что в целом представляет собой инновационный процесс.

Вместе с тем, границы многих терминов до сих пор остаются юридически нечеткими (понятия информационной войны, информационной борьбы, информационного противоборства, информационного оружия и относимых к ним средств воздействия, их признаков и классификации), что приводит к разногласиям в понимании угроз, борьбе с которыми должны быть адресованы разные правовые нормы и институты. Поэтому одной из первостепенных задач является конкретизация понятийного аппарата в международных документах и выработка общепринятых определений в сфере ИБ для эффективного взаимодействия государственных органов с общественными структурами и бизнесом.

Национальные сегменты информационных сетей подпадают под правовой режим, определяемый национальными юрисдикциями. Между тем, проблема ИБ ввиду ее ярко выраженного трансграничного характера может решаться гораздо более эффективно при их согласовании, унификации и интернационализации.

В настоящее время важнейшим и насущным стало создание международных режимов запрещения разработки, производства и применения информационного оружия, а также механизмов для борьбы с информационным терроризмом и криминалом, включая создание межгосударственной системы мониторинга угроз безопасности ИКТ. Разработка мер по углублению сотрудничества требуют *сферы непреступного применения ИКТ транснационального характера*: неправильное восприятие воздействия в условиях отсутствия общепринятого понимания международных норм, касающихся государственного использования ИКТ может сказаться на принятии решения в кризисных ситуациях. Такие меры могут быть направлены на обмен информацией и передовыми методами, устранение последствий происшествий, создание доверия, снижение риска и повышение транспарентности и стабильности. Обнадеживающим шагом в этом направлении стало совместное решение президентов РФ и США создать двустороннюю рабочую группу по вопросам угроз в сфере ИКТ в контексте международной безопасности, которое было подписано в июне 2013 года на саммите G8. Группа планировала встречаться на регулярной основе, проводить оценку возникающих угроз, разрабатывать, предлагать, координировать совместные меры по реагированию на такие угрозы и по укреплению доверия. Первое заседание, состоявшееся в ноябре 2013 года, было очень продуктивным. Но в условиях осложнения отношений с США этот процесс затормозился, и в течение 2014 года не состоялось ни одной встречи группы.

Очевидно, что первоочередной задачей является разработка нормативной и информационно-технологической базы для исключения взаимных подозрений в случае кибердиверсий против информационно-управляющих систем стратегических сил и систем предупреждения о ракетном нападении сторон, а также против систем управления АЭС, космическими аппаратами, энергетическими и транспортными инфраструктурами и т.д. Параллельно целесообразно развивать методы сотрудничества в борьбе с киберпреступностью в банковско-финансовых организациях, системах и коммуникациях.

Впоследствии, возможно, откроется путь к взаимному отказу от наиболее дестабилизирующих средств информационной войны – по аналогии с договорами об ограничении вооружений. На этой основе можно затем придать таким документам многосторонний характер, превратить их в нормы и механизмы глобального управления в сфере ИБ.

Однако в пространстве ИКТ существуют специфические проблемы. Так, значительно труднее осуществлять контроль над выполнением подобных договоренностей. Если в

области контроля над другими видами вооружений можно отследить пуски ракет, изменение радиоактивности, последствия разработки и применения токсикологических и химических соединений, размещение элементов инфраструктуры, проводить инспекции и т.д., то в информационной среде подобные методы не применимы. Такие возможности, вероятно, откроются в дальнейшем с развитием науки и технологий, чему необходимо уделять особое внимание на государственном уровне. Кроме того, нельзя говорить о запрещении развития ИКТ, т.к. они могут и должны использоваться во благо человечества, поэтому международная деятельность должна быть нацелена на противодействие их применения лишь в военных, террористических и криминальных целях. Еще одна проблема связана с тем, что в настоящее время практически невозможно доказать нарушение подобных режимов. Поэтому переговорный процесс в настоящее время должен быть направлен на выработку международных документов о правилах поведения и о сдержанности стран в применении ИКТ, в первую очередь, в военной сфере, а также об ответственности государств за их нарушение.

Международная деятельность России в сфере ИКТ

Поскольку подрывная деятельность с использованием ИКТ приобретает все более сложный и опасный характер, ни одно государство не может справиться с этими угрозами в одиночку.

Россия стала инициатором международного обсуждения проблем информационной безопасности, предотвращения её милитаризации, противодействия терроризму в ИКТ, когда в 1998 году предложила Соединённым Штатам подписать на уровне президентов заявление по вопросам обеспечения информационной безопасности. Проект документа предусматривал совместное определение вызовов и угроз в данной сфере, выработку понятийного аппарата, вынесение вопроса о глобальной информационной безопасности на рассмотрение ООН, включая разоруженческие аспекты проблемы, а также выход на разработку международного многостороннего договора о борьбе с информационным терроризмом и преступностью. Обсуждение проекта заявления не привело к сближению сторон, однако в самом общем виде информационная безопасность была упомянута в «Совместном заявлении об общих вызовах безопасности на рубеже XXI века», подписанном президентами РФ и США в сентябре 1998 года.[171]

В том же году в адрес Генерального секретаря ООН было направлено специальное Послание по проблеме международной информационной безопасности министра иностранных дел РФ, в котором указывалось на необходимость предотвращения появления принципиально новой — информационной — сферы конфронтации и развязывания принципиально новых конфликтов. Указанная инициатива получила практическую реализацию в проекте резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», внесенном Россией на рассмотрение Первого комитета ГА ООН. Резолюция ГА ООН 53/70 была принята без голосования 4 декабря 1998 года.

В окончательно принятой резолюции, в отличие от представленного Россией проекта, не было прямых ссылок на использование информационных технологий в военных целях, конкретных определений понятий «информационное оружие» и «информационная война», упоминания о необходимости разработки режима запрещения создания и применения информационного оружия, а также положения о сопоставимости воздействия информационного оружия и ОМУ. По заявлениям российских представителей, наибольшее

[171]Совместное заявление об общих вызовах безопасности на рубеже XXI века. 2 сентября 1998 г. (http://www.businesspravo.ru/Docum/DocumShow_DocumID_62942.html).

противодействие разоруженческим идеям и задачам предотвращения межгосударственного противоборства в информационном пространстве оказали США.

Однако после принятия этой резолюции вопрос о проблемах и результатах в процессе обеспечения информационной безопасности стоит на повестке дня ООН до настоящего времени. РФ выносит документ с таким названием на рассмотрение Генеральной Ассамблеи более 10 лет.

Резолюция ГА ООН 54/49 от 1 декабря 1999 года «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» впервые указала на угрозы международной информационной безопасности применительно не только к гражданской, но и к военной сфере.

В докладе Генерального секретаря ООН от 10 июня 2000 года «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» отражены предложенные Россией «Принципы, касающиеся международной информационной безопасности», в которых предложены базовые термины и 5 основных принципов деятельности государств в международном информационном пространстве.

В соответствии с резолюциями ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» в 2004 году была создана Группа правительственных экспертов (ГПЭ) ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

В 2010 году российское председательство в Группе завершилось принятием доклада, формулировки которого позволили заложить основу предметной дискуссии по МИБ.

В XXI веке многие страны неоднократно подтверждали необходимость осуществления международного сотрудничества в этой сфере. Усилия прилагаются в рамках ШОС, БРИКС, СНГ, Организации американских государств, Форума АТЭС, Регионального форума АСЕАН, Экономического сообщества западноафриканских государств, Африканского союза, ЕС, ОБСЕ и Совета Европы, а также в форме двустороннего сотрудничества. Результатами этой деятельности, в частности, стало обсуждение Конвенции ООН об обеспечении международной информационной безопасности[172], предложенной Россией в 2011 году, и другие документы.

Предложенная Россией Конвенция направлена на решение проблемы недостаточности понятийного аппарата и его несоответствие существующим угрозам в информационной сфере. Документ предполагал закрепление на международном уровне ряда понятий – информационная война, информационная безопасность, информационное оружие, терроризм в информационном пространстве и других, которые пока не стали категориями международного права. В российском проекте Конвенции четко прописаны вопросы сохранения суверенитета государства над его информационном пространством, а также положения, направленные на защиту от «действий в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологической обработки населения, дестабилизирующей общество»[173].

Российский проект Конвенции является противовесом так называемой Будапештской конвенции (Конвенции Совета Европы по киберпреступности), которая рассматривается западными странами в качестве документа «глобального» характера в вопросах кибербезопасности. Россия не подписала этот документ, так как не согласна с содержанием некоторых его положений, в частности, статьи 32 о «трансграничном доступе», в соответствии с которой спецслужбы одних стран могут проникать в компьютерные сети других стран и проводить там операции без ведома национальных властей.

[172]Конвенция об обеспечении международной информационной безопасности (концепция). Сайт Совета Безопасности Российской Федерации. (http://www.scrf.gov.ru/documents/6/112.html).
[173]Там же.

Разногласия России и западных стран во главе с США в процессе обсуждения документа связаны с оценкой информационных угроз и необходимости выработки обязательных международных средств противодействия им. Российская сторона считает, что необходимо предусмотреть весь комплекс мер, связанных с возможным противоправным (враждебным) использованием информации или ИКТ. По мнению Соединенных Штатов, достаточно ограничиться вопросами киберугроз. Таким образом, американский подход исключает из сферы международно-правового регулирования информационно-психологические операции. США обосновывают свою позицию тем, что внесение этих вопросов в круг проблем информационной безопасности может рассматриваться как желание оказать давление на «гражданское общество», угрожать «свободе слова» и «усиливать авторитарные тенденции».

2 декабря 2014 года в ходе заседания Первого комитета 69-й сессии Генеральной Ассамблеи ООН консенсусом принята очередная выдвинутая Россией резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[174] (см. Приложение Е), в которой сохранены положения резолюции прошлого года о важности уважения прав человека и основных свобод в сфере ИКТ. С каждым годом все больше государств становятся соавторами этого документа. В 2014 году ими стали более 50 стран – самое большое число государств, заявивших о желании присоединиться к нему в качестве соавторов за все эти годы. Коспонсорство документа приобретает подлинно глобальный характер, охватывая все регионы мира.

В 2014 году ГПЭ созывалась уже в четвертый раз – ранее в 2004-2005, 2009-2010 и 2012-2013 годах. В работе группы принимали участие представители Белоруссии, Бразилии, Великобритании, Ганы, Германии, Египта, Израиля, Индии, Италии, Испании, Катара, Кении, Китая, Колумбии, Малайзии, Мексики, Пакистана, Республики Корея, России, США, Франции, Эстонии, Южной Африки, Японии и др. Мандат этой ГПЭ предполагает дальнейшее исследование существующих и потенциальных угроз в информационной сфере и совместных мер по их устранению, в т.ч. нормы, правила и принципы ответственного поведения государств, меры укрепления доверия, вопросы использования ИКТ в конфликтах и того, как международное право применяется к использованию ИКТ государствами. По итогам четырех заседаний Группа призвана сформулировать практические рекомендации, которые должны стать результатом международного компромисса. [175]

В июле 2015 года вышел третий доклад ГПЭ[176], который был представлен на юбилейной 70-й сессии Генеральной Ассамблеи ООН. Группа «изучила существующие и потенциальные угрозы, порожденные использованием ИКТ государствами, и проанализировала меры для борьбы с ними, в том числе разработку норм, правил, принципов и мер укрепления доверия. Кроме того, Группа рассмотрела вопрос о применимости норм международного права к использованию ИКТ государствами. Основываясь на работе предыдущих групп, Группа нынешнего созыва добилась существенных успехов в этих

[174]Резолюция, принятая Генеральной Ассамблеей 2 декабря 2014 года [по докладу Первого комитета (A/69/435)] 69/28. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Организация Объединенных Наций A/RES/69/28.
(http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/662/43/PDF/N1466243.pdf?OpenElement).

[175] Крутских А., Стрельцов А. Международное право и проблема обеспечения международной информационной безопасности. Международная жизнь. Ноябрь 2014.
(https://interaffairs.ru/author.php?n=arpg&pg=1167#).

[176]Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Организация Объединенных Наций. Генеральная Ассамблея. Семидесятая сессия. Пункт 93 предварительной повестки дня.* Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174.
(http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=R).

сферах».[177] Доклад оценивается российскими членами Группы в качестве революционного, а американскими – в качестве победы дипломатии США[178].

Доклад включает следующие договоренности с учетом позиций 20 государств (в том числе США, Китай и развивающиеся страны) по вопросу о применимости международного права в информационной сфере:

- не легализовать и не регулировать конфликты в информационном пространстве, а предотвращать использование ИКТ в военно-политических целях;
- отказаться от взаимных обвинений в кибератаках, как это нередко происходит, без серьезных на то доказательств;
- использовать ИКТ исключительно в мирных целях;
- признать незаконной и вредоносной деятельность по внедрению закладок в IT-продукцию (впервые);
- не осуществлять или заведомо поддерживать деятельность в сфере ИКТ, направленную на нанесение преднамеренного ущерба критически важной инфраструктуре или создание иных препятствий в ее использовании или функционировании (при этом государства должны принимать надлежащие меры для защиты их критически важной инфраструктуры от угроз в сфере ИКТ);
- подтвердить суверенное право государств распоряжаться информационно-коммуникационной инфраструктурой на своей территории и определять свою политику в сфере международной информационной безопасности.

Важными результатами работы ГПЭ 4-го созыва стали пункт 12 о принятии Группы к сведению Правил поведения в области обеспечения международной информационной безопасности, предложенные Казахстаном, Китаем, Кыргызстаном, Российской Федерацией, Таджикистаном и Узбекистаном, представленные на Генеральной Ассамблее ООН в январе 2015 г.[179] (текст Правил находятся в Приложении F), а также разработанные рекомендации по устранению существующих и потенциальных угроз международному миру и безопасности, проистекающих из использования ИКТ государствами и негосударственными субъектами; по укреплению доверия; наращиванию потенциала и применению норм международного права.

Работу ГПЭ планируется продолжить в 2016 году и представить ее результаты на 72-й сессии Генассамблеи ООН в 2017 году. Глобальной целью при этом по-прежнему будет принятие Конвенции об обеспечении международной информационной безопасности, а более ближнесрочной – разработка и принятие дополнительных добровольных и необязательных норм ответственного поведения государств в глобальной ИКТ-среде.

На основании докладов ГПЭ можно выделить основные угрозы МИБ на современном этапе.

1. *Наращивание потенциала в сфере ИКТ рядом государств для военных целей, разведки и в политических целях.*
2. *Трудности и неопределенность в идентификации источника инцидента в сфере ИКТ* и отсутствие общепринятого понимания, какие государственные меры в

[177] Там же.

[178]Интервью спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Посла по особым поручениям МИД России А.В. Крутских газете «Коммерсант», опубликованное 17 августа 2015 года. Сайт Министерства иностранных дел Российской Федерации. (http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/1655289).

[179]Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. Организация Объединенных Наций. Генеральная Ассамблея. Шестьдесят девятая сессия. Пункт 91 повестки дня. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/69/723. (http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723&Lang=R).

связи с этим приемлемы, что создает риск нестабильности и неверного восприятия угрозы, возникновения конфликта и нанесения ущерба экономике.

3. *Рост вероятности использования ИКТ в будущих конфликтах.*
4. *Нападения на критически важные объекты инфраструктуры и связанные с ними информационные системы государств с использованием ИКТ.*
5. *Использование ИКТ в террористических целях для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру.*
6. *Использование ИКТ в террористических целях для вербовки сторонников, финансирования, обучения и подстрекательства*, что может поставить под угрозу международный мир и безопасность.
7. *Многообразие злонамеренных негосударственных субъектов (включая преступные группировки и террористов)*, их различные мотивы, быстротечность злонамеренных нападений в сфере ИКТ.
8. *Вредоносные инструменты и методологии преступников в сфере ИКТ и хакеров.*
9. *Использование ИКТ* для *обмена, сбора, передачи информации, организации подрывной деятельности и пропаганды.*
10. *Внедрение вредоносных программ,* которое может привести к *подрыву доверия к товарам и услугам, а также к бизнесу в целом.*
11. *Разный уровень развития потенциала обеспечения безопасности в сфере ИКТ между государствами*, который может привести к повышению уязвимости в условиях взаимосвязанного мира.

По результатам работы группы можно выделить основные вопросы относительно применимости международного права к информационной среде, по которым ведется активная международная дискуссия.

- Каким образом трактуется противоправное использование ИКТ в рамках современной системы международно-правовых норм?
- Может ли противоправное использование ИКТ быть классифицировано как агрессия в соответствии с резолюцией ГА ООН 3314 «Определение агрессии» 1974 года?
- Может ли применяться термин «оружие» к ИКТ?
- Какие юридические факты противоправного использования ИКТ, могут квалифицироваться как использование вооруженных сил (по смыслу ст. 39 Устава ООН) и породить право на самооборону (по смыслу ст. 51 Устава ООН)? Как предотвратить злоупотребления в этой области?
- Можно ли рассматривать национальную информационную инфраструктуру как военный объект, против которого может быть применено «традиционное оружие» или ИКТ?
- Как избежать злоупотреблений со стороны государств при определении субъектов, ответственных за противоправное использование ИКТ?
- Является ли использование ИКТ в целях нарушения социальной, политической стабильности и общественного порядка в другом государстве противоправным и можно ли его классифицировать как вмешательство во внутренние дела суверенного государства (по смыслу ст. 2 (4) Устава ООН)?
- Как определить ответственность государств за действия уполномоченных ими лиц с целью противоправного использования ИКТ?
- Каким образом определить театр ведения военных действий в информационном пространстве?
- Как оценить связь между противоправным использованием ИКТ и подрывом государственного суверенитета?

- Какие международные и национальные институты и на основании каких критериев уполномочены оценивать угрозы, возникающие в связи с противоправным использованием ИКТ против международного мира и безопасности, а также их последствия?
- Как можно решить задачу поиска баланса между безопасностью и свободой, правом на доступ к информации и ответственностью государств за действия в информационном пространстве?

Обеспокоенность стран вызывают *попытки установления контроля над глобальным информационным пространством через использование ИКТ*. При этом особую важность приобретает *вопрос уважения прав человека и основных свобод в информационной сфере*. Однако их соблюдение не должно противопоставляться другим важнейшим принципам международного права – невмешательству во внутренние дела государств и уважению национального суверенитета.

Исходя из этих данных, можно выделить основные направления международной деятельности по обеспечению МИБ.

1. Создание национальных и глобальных условий для разработки, производства и применения средств обеспечения МИБ.
2. Организация международного сотрудничества в сфере ИКТ.
3. Совершенствование кадрового обеспечения и организационных мер, обучение специалистов и проведение научных исследований в области информационной и кибербезопасности.
4. Обеспечение защиты ИКТ от вредоносного воздействия и уменьшение потенциального ущерба от атак на системы.
5. Защита общественной безопасности и бизнеса в сфере ИКТ.
6. Борьба с киберпреступностью и информационным терроризмом.
7. Защита информации и средств ее обработки в вооруженных силах для успешного осуществления сложных сценариев на всех уровнях командования.
8. Международная деятельность по предотвращению конфликтов в ИП в противовес подходам, предполагающим их легитимизацию. В связи с этим исследовательский мандат ГПЭ целесообразно расширить, включив в него вопросы использования ИКТ в конфликтах и применимости международного права к действиям государств в ИП.
9. Разработка дальнейших шагов по укреплению доверия и прочих мер в целях снижения риска возникновения неправильного восприятия в результате дезорганизации или нарушений, связанных с применением ИКТ:

- продолжение межгосударственного диалога по нормам государственного использования ИКТ, сокращению коллективного риска и защиты критической национальной и международной инфраструктуры;
- принятие мер по укреплению доверия, повышению уровня стабильности в связи с последствиями государственного использования ИКТ, включая обмен мнениями стран по вопросу об использовании ИКТ в конфликтах;
- обмен информацией о национальных законах, стратегиях, технологиях, принципах и передовых методах обеспечения ИБ;
- определение мер оказания содействия созданию потенциала обеспечения информационной безопасности в менее развитых странах;
- выработка общей терминологии и определений в связи с положениями резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 64/25 Генеральной Ассамблеи ООН.[180]

[180] Резолюция A/64/386. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. (http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/538/56/PDF/N0953856.pdf?OpenElement).

За последние несколько лет российские эксперты участвовали в межведомственных консультациях с Белоруссией, Бразилией, Германией, Израилем, Индией, Южной Кореей, США, Францией, Кубой. Вопросы МИБ обсуждались в формате ООН, ОБСЕ, ОДКБ, ШОС, Регионального форума АСЕАН, Института ООН по исследованию проблем разоружения (ЮНИДИР), ежегодных международных форумах «Партнерство государств, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму», международного исследовательского консорциума информационной безопасности в г. Гармиш-Партенкирхене (Германия). Председательствуя в группе БРИКС, в 2015 г. Россия впервые вынесла на повестку дня тему управления Интернетом.

Решение проблем ИКТ в XXI веке зависит от успешного сотрудничества между партнерами, поэтому особую значимость приобретает деятельность по созданию международной правовой базы по защите информационного пространства, позволяющей осуществлять совместные действия и создавать совместные механизмы по следующим направлениям:

- правовая база, обязывающая государства помогать развивать «отстающим» странам систему обеспечения информационной и кибербезопасности;
- правовая защита критических инфраструктур;
- правовая база по использованию ИКТ в конфликтах;
- законодательное закрепление общих стандартов обеспечения кибербезопасности;
- единое процессуальное законодательство по вопросам борьбы с киберпреступностью, информационным терроризмом и по предотвращению возможности кибервойны;
- правовое обеспечение МИБ бизнес-структур.

За последние несколько лет был подготовлен и принят ряд международно-правовых актов и международных документов, создающих первоначальную основу для функционирования системы РФ по обеспечению международной информационной безопасности, среди которых наиболее значимы:

- доклады Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций а контексте международной безопасности (носят характер действующих рекомендаций ООН);
- Соглашения между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности (2009 год);
- Положение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в сере обеспечения информационной безопасности (2010 год);
- Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилия о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (2010 год);
- Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности (2013 год);
- Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (2013 год).
- Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности (2014 год).

- Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (2015 год).

Исследование документов, официальных заявлений и аналитических материалов позволяет сделать вывод, что Россия выступает за демилитаризацию международного информационного пространства, за необходимость доработки и адаптации механизмов международного права применительно к ИКТ, а также за создание новых норм, подчеркивая, что гонка вооружений в информационном пространстве способна дестабилизировать сложившиеся договоренности о разоружении и международной безопасности и в других сферах.

Приложения

Приложение А. ПРИМЕРЫ КИБЕРАТАК XXI ВЕКА

Название атаки	Дата атаки	Описание	Нанесенный ущерб, последствия	Предполагаемый создатель
I love you	***05. 2000***	Разослан на почтовые ящики жителей Филиппин. В теме письма содержалась строка «ILoveYou», к письму приложен скрипт «LOVE-LETTER-FOR-YOU.TXT.vbs». Расширение «.vbs» было по умолчанию скрыто, что и заставило пользователей думать, что это был простой текстовый файл. При открытии вирус рассылал копию самого себя всем контактам в адресной книге Windows, а также на адрес отправителя. Он также совершал ряд вредоносных изменений в системе пользователя.	Поразил более 3 млн. компьютеров по всему миру. Предполагаемый ущерб: более $10 млрд.	Житель Филиппин Реонель Рамонес, а также несколько студентов компьютерной школы AMA Computer College в Маниле.
Code Red	***13.07.2001***	Атаковал компьютеры с работающим веб-сервером Microsoft IIS.	Ущерб $2.62 млрд. Через две недели вирус запрограммирован на запуск DDoS атак (распределенный отказ в обслуживании) на	Вирус выдавал сообщение на экране «Hacked By Chinese!» («Взломано китайцами!»), хотя в

			определенные веб-сайты, в том числе сервер Белого Дома США.	действительности он, вероятно, создан этническими китайцами на Филиппинах.
Nimda	***2001***	Атаковал компьютеры с работающим веб-сервером Microsoft IIS.	Заражение по всему миру, в том числе РФ. Например, с 19.09 по 22.09 2001 г. парализовал работу служебных и частных ПК города в Свердловской области.	Студент университета в Сакраменто (США).
Slammer (Sapphire)	***25-26.01. 2003***	Распространяет свои копии как приложение по почте. Когда пользователь запускает приложение, оно создает файл под названием ISERVC.EXE во временной папке и активизирует его.	Отсутствие интернета в Южной Корее, нарушение работы банкоматов и замедление работы интернета в США.	Полицейским удалось найти сайт китайской хакерской группировки, на котором излагалась возможность эксплуатации бреши в Microsoft SQL Server и приводилось описание червя, напоминающего Slammer.
Sasser	***03.05.2004***	Распространяется по глобальным сетям, используя уязвимость в службе LSASS Microsoft Windows. Не требует взаимодействия с пользователем атакуемой машины для заражения ПК. Признак заражения – сообщение об ошибке LSA Shell (Export version) и следующее за ним сообщение о необходимости перезагрузить ПК из-за ошибки процесса lsass.exe.	Десятки тысяч служебных и частных ПК «зависли» и отключились на несколько часов. Большой ущерб нанесен электронным системам итальянских железных дорог и почты. На некоторое время вышли из строя компьютеры МВД Италии. За информацию о создателе вируса компания Microsoft назначила премию в размере $250 тыс.	18-летний учащийся профтехучилища из небольшой деревни Ваффензен (округ Ротенбург-Вюмме) близ Бремена был арестован по обвинению в компьютерном саботаже с тяжелыми последствиями.

		Сообщения появляются не только при первом заражении, но и при каждой последующей атаке.		
Mytob	***16.08 2005***	Является приложением Windows (PE EXE-файл), размер около 143КБ (упакован FSG). Распространяется, используя уязвимость в сервисе LSASS Microsoft Windows, а также через интернет в виде вложений в зараженные электронные письма. Рассылается по всем найденным на зараженном компьютере адресам эл. почты.	Атака на системы печатных изданий, радио и ТВ-компаний США (в т.ч., газета New York Times и ТВ-каналах ABC и CNN). Также взломаны базы данных нескольких банков и произведены махинации со счетами. Были инфицированы сотни тысяч ПК по всему миру.	Не известен
Нет данных	***27-28. 04.2007***	Хакерские атаки на веб-сайты правительственных учреждений Эстонии после решения властей страны о начале работ по эксгумации и идентификации останков советских воинов, захороненных у монумента Воину Освободителю.	Взломан интернет-сайт правящей Реформистской партии. Ограничен доступ на сайт правительства Эстонии. Через некоторое время блокирован доступ на сайты президента, парламента и МИД страны.	Не известен

Комплексная платформа для кибератак: операция «Красный октябрь» ('Red October'), бэкдор. Win32.Sputnik (по базе ЛК)	***2007 - 2013***	Серия атак на компьютерные сети правительственных учреждений, дипломатических организаций / посольств, образовательных / исследовательских организаций, сектора коммерции, энергетических и нефтегазовых компаний, аэрокосмической отрасли, военных ведомств в различных странах мира. Масштабная кибершпионская сеть. Атакованные платформы: Windows, Windows Mobile. Обнаружена в январе 2013 г. Программная среда платформы создана для того, чтобы выполнять «задания», направляемые от командно-контрольных серверов, и предназначенные для кражи информации.	Число заражений: 101-500 в более, чем 20 странах Восточной Европы, бывшего СССР, Центральной Азии, Западной Европы и Северной Америки.	Предположительно создана китайскими хакерами. Вредоносные модули «Красного октября» созданы русскоговорящими программистами.
Conficker	***21.11.2008***	Быстрое распространение связано со службой Server Service. Используя «дыру» в ней, червь скачивает себя из интернета. Может распространяться через USB-накопители, создавая файлы autorun.inf и RECYCLED\{SID}\RANDOM_NAME.vmx. В системе червь хранится в виде dll-файла со случайным именем, состоящим из латинских букв, например - c:\windows\system32\zorizr.dll.	К апрелю 2009 г. успел проникнуть более, чем в 12 млн. ПК. Пострадали цифровые системы кораблей британских ВМС, Палата общин британского парламента. Вирус легко взламывает пароли, а потом использует зараженные машины для рассылки спама или как базы для хранения украденной информации.	Не известен.

GhostNet	***8.21.04.2009; 08.07.2009***	Атакованы ПК, контролирующие работу энергосетей по всей территории США. Разведслужбы США утверждали, что взломщики не пытались нарушить работу системы энергообеспечения, однако могли внедрить программы, способные нарушить работу энергосетей во время кризиса или войны. Власти Южной Кореи заявили о массированной кибератаке на важнейшие правительственные и банковские сайты страны.	Похищение информации о новом многоцелевом истребителе пятого поколения Joint Strike Fighter (F-35 Lightning II) с компьютерной системы Пентагона. Скопировано несколько терабайт данных, касающихся дизайна и электронной системы нового самолета. Информация может быть использована при разработке систем защиты от данного типа истребителей. С 7 на 8 июля интернет-порталы одиннадцати южнокорейских организаций, среди которых – сайты президентской администрации, МО, парламента, нескольких банков и интернет-портала Naver, стали недоступны. ВП, ставшая причиной атаки DDoS, заразил более 18 тыс. ПК.	Не известен
Aurora	***2009-2010***	Набор инструментов для кибершпионажа и кражи данных, обнаруженный в январе 2010 г. атаковал платформы Windows. Появился в июле – декабре 2009 г.	Атака направлена на десятки организаций. Google, Adobe Systems, Juniper Networks и Rackspace подтвердили, что подверглись атаке. По сообщениями СМИ, в числе жертв операции также оказались Yahoo!, Symantec, Northrop Grumman, Morgan Stanley и Dow Chemical. Число заражений: 11-100 в США.	Команда Elderwood, имеющая связи с Китаем, а также другие группы китайского происхождения, напр., Comments Crew.

			Жертвы: IT-сектор, разработчики ПО, финансовые институты.	
Нет данных	***06.2011***	Украдены данные, касающиеся номеров счетов основных держателей банковской карты, их имен и фамилий, контактной информации.	Взломана компьютерная сеть RSA, подразделения компании EMC, получив доступ к информации о технологии SecurID, которая применяется для обеспечения безопасности корпоративных ПК. Решения на базе SecurID для защиты информационной инфраструктуры используются правительственными и коммерческими организациями по всему миру. В результате атаки на базу данных владельцев пластиковых карт банка в Северной Америке пострадало 360 тыс. чел., крупнейшие ИТ-компании (Facebook, eBay, Google, Cisco, Motorola, IBM, Intel), оборонные фирмы (Northrop Grumman), финансовые, исследовательские организации (Еврокосмическое агентство).	Не известен

Stuxnet	***2007–2011***	Первый компьютерный «червь», перехватывающий и модифицирующий информационный поток между логическими контроллерами Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens. Обнаружена в июне 2010 г. Цель: киберсаботаж. Может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов и т. п. Первое кибероружие, способное причинять физический ущерб, разработанное специально для саботажа процесса по обогащению урана на определенных объектах. Иранские власти официально признали, что компьютерные программы систем управления ядерных объектов страны: Бушерская АЭС и завод в Натанзе, были подвергнуты атаке Stuxnet. По западным источникам, Stuxnet был обнаружен в компьютерах в Индии, Китае, Индонезии, около 60% Stuxnet были сосредоточены в Иране.	Число жертв: от 100 тыс. до 300 тыс. объектов ядерной отрасли. Одновременный ввод в резонансную частоту большого количества центрифуг.	«ЛК»: «Очевидно, что кампания спонсируется государством». Различные международные публикации указывают на США и Израиль как на авторов Stuxnet и организаторов акций против иранской ядерной программы без применения военной силы и с целью психологического давления на Иран.

Троянская программа Duqu	***2008-2012***	Атаковала платформы Windows в нескольких странах с целью кибершпионажа: искали информацию о системах контроля производства и о торговых отношениях между конкретными организациями. Обнаружена в апреле 2011.	Число заражений: 11-100 в Иране, Судане, Франции, Венгрии.	Организаторы имеют отношение к разработчикам Stuxnet и Flame.
Комплексная платформа для кибератак Flame	***2007 - 2012***	Обнаружена в мае 2012 г. Атакованные платформы: Windows с целью кибершпионажа. Распространяется через USB-накопители и через LAN. Способна собирать файлы данных, удалённо менять параметры ПК, записывать звук, скриншоты и подключаться к чатам. Код ВП имеет объём 20 МБ, что почти в 20 раз больше Stuxnet. Инструмент для комплексных атак с функциями, напоминающими поведение червя.	Число жертв: 500-1000 ПК, в образовательных / исследовательских организациях, правительственных учреждениях, большинство из которых находилось в Иране. Значительное число пострадавших в Израиле, Палестине, Судане, Сирии, Ливане, КСА, Египте, замечены в Европе и Северной Америке. Атакован один из серверов МАГАТЭ и размещены адреса электронной почты ста сотрудников организации.	Ответственность взяла на себя организация Parastoo (популярное женское имя в Иране, в переводе с фарси – «ласточка»). Хакеры призвали сотрудников МАГАТЭ, чьи данные были украдены, подписать петицию с требованием о проведении «открытого расследования» деятельности Израиля в области ядерной энергетики.

Троянская программа Flashback/ Flashfake	***04.2012***	Поражено более 700 тыс. компьютеров MacOS X по всему миру. Зараженные компьютеры объединены в ботнет, и злоумышленники могут устанавливать на них любые дополнительные вредоносные модули. Один из модулей занимается подменой трафика в браузере. Преступники также могут загружать на зараженные компьютеры ВП для кражи данных, рассылки спама и т.д.	После изучения поведения сети зараженных компьютеров и способов заражения выяснено, что уязвимость находится на стороне модуля Java, встроенного в операционную систему от Apple. После чего Apple выпустила несколько обновлений для того, чтобы оградить пользователей от возможности заражения.	Нет данных.
Нет данных	***26.02.2013***	Используемый для размещения фотографий Twitter-аккаунт информационного агентства Франс Пресс @AFPPHOT был взломан, после чего на нем появились документы, связанные с вооруженным конфликтом в Сирии. Работа аккаунта быстро остановлена.	Нет данных	Ответственность взяла на себя сетевая группировка Сирийская электронная армия (Syrian Electronic Army, SEA), поддерживающая президента Б. Асада. Их действия были связаны с данными некоторых СМИ, которые распространяли новости о событиях в Сирии.

Нет данных	***21.03.2013***	Взломана страничка метеослужбы BBC в сети микроблогов Twitter. Аккаунт, который просматривают около 60 тыс. пользователей, начал публиковать сообщения политического характера около часа дня по местному времени.	Нет данных.	Ответственность взяла на себя Сирийская электронная армия (Syrian Electronic Army, SEA).
Нет данных	***14.04.2013***	Микроблог кандидата в президенты Венесуэлы Н. Мадуро в Twitter взломан за несколько часов до закрытия избирательных участков в день выборов президента. В микроблоге появились сообщения, написанные якобы от его имени о предстоящем обмане избирателей в ходе выборов.	Кибератака затронула ряд сайтов, связанных с правительством Венесуэлы.	Предположительно хакеры из Перу.
Нет данных	***23.04.2013***	Взломан аккаунт на сайте микроблогов Twitter информационного агентства Associated Press. В социальной сети размещено ложное сообщение о том, что в Белом доме прогремело 2 взрыва, в результате чего президент США Б. Обама ранен. Позже пресс-секретарь президента Дж. Карни опроверг эту информацию.	Нет данных.	Нет данных.
Нет данных	***07.08.2013***	Взломаны неосновные аккаунты Международного мультимедийного пресс центра РИА Новости и RIA Novosti Deutsch.	Хакеры разместили ложную информацию о смерти президента СССР М. Горбачева. Оба фальшивых твита провисели около 5 мин. и были удалены.	Нет данных.

Нет данных	***02-03 2014***	Хакерами взломана база данных одной из крупнейших онлайн-площадок по купле-продаже товаров eBay.	Похищены, а затем предлагались на продажу личные записи 233 млн. пользователей и сотрудников eBay: имена, пароли, номера телефонов, адреса электронной почты, физические адреса, даты рождения. Похищенные данные могли сделать людей уязвимыми для хищения полной личной информации о них. EBay не уточнила масштабы инцидента.	Ответственность за нападение на eBay взяла на себя Сирийская Электронная армия (Syrian Electronic Army).
Нет данных	***18.09.2013 – 11.06.2014***	Кибервзлому подверглась платежная система сети ресторанов P.F. Chang's Chinese Bistro.	Похищенные данные около 800 тысяч кредитных и дебетовых карт были выставлены на продажу в Интернете 09.06.2014 по цене $ 18 — $ 140 в зависимости от свежести информации.	Нет данных.
Нет данных	***07.2013, обнаружена 05.2014***	Кибервзлому хакеров подвергся Департамент здравоохранения штата Монтаны США.	Похищены личные данные белее 1 млн. человек: номера социального страхования, медицинские записи, записи медицинского страхования, имена, адреса, свидетельства о рождении, банковские реквизиты всех сотрудников Департамента.	Нет данных.

Троянская программа Duqu 2.0	***2014-2015***	Активное в настоящее время чрезвычайно сложное ПО, обновлённая версия вредоносного ПО 2011 г. – Duqu. Вредоносным заражениям подверглись площадки мероприятий «Группы 5+1» по решению иранской ядерной проблемы, в рамках которых проходили встречи мировых лидеров. Duqu 2.0 не имеет нормального механизма закрепления: код базируется исключительно в памяти компьютера. Возможно, содержит большое количество украденных сертификатов. Тактика и методы группы Duqu 2.0 на целое поколение опережают все угрозы. Атакованные платформы: Windows. Цели и функции: кибершпионаж, кража данных, слежка, удалённый контроль.	Число заражений: 11-100 в странах Запада, Ближнего Востока и Азии. Жертвы: политики, IT-сектор, разработчики ПО, высокотехнологичные компании, отдельные пользователи, частные компании, производители электроники.	Разработчики Duqu. Предположительно при поддержке государственных структур.
Троянская программа, набор инструментов для кибер-шпионажа, бэкдор Wild Neutron	***2011-2015***	Активная в настоящее время ВП для преднамеренного заражения часто посещаемых сайтов с целью кибершпионажа и кражи данных. Обнаружена в 2013 г. Атакованные платформы: Windows, OS X. Группа, атакующая крупные IT-компании, разработчиков шпионского ПО (FlexiSPY), исламистские форумы и Bitcoin-компании, что позволяет	Число заражений:11-100 во Франции, РФ, Швейцарии, Германии, Австрии, Словении, Казахстане, ОАЭ, Алжире, США и др. Жертвы: IT-сектор, разработчики ПО, финансовые институты, отдельные пользователи, сектор коммерции, частные компании, фармацевтические компании, промышленность, сектор	Точных данных о происхождении нет. В некоторых экземплярах вредоносного кода встречается строка на румынском языке “La revedere” («до свидания») для окончания сессии коммуникации с

		предположить, что у нее гибкие и необычные интересы и цели.	инвестиций.	командно-контрольным сервером. В «ЛК» обнаружили также команду и на русском языке – написанное латиницей слово «успешно».

Приложение В. ПРИЛОЖЕНИЯ К СОГЛАШЕНИЮ МЕЖДУ ПРАВИТЕЛЬСТВАМИ ГОСУДАРСТВ-ЧЛЕНОВ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
от 16 июня 2009 года № Б/Н

Приложение 1

Перечень основных понятий в области обеспечения международной информационной безопасности

«Информационная безопасность» – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

«информационная война» – противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;

«информационная инфраструктура» – совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации;

«информационное оружие» – информационные технологии, средства и методы, применяемые в целях ведения информационной войны;

«информационная преступность» – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;

«информационное пространство» – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

«информационные ресурсы» – информационная инфраструктура, а также собственно информация и ее потоки;

«информационный терроризм» – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

«критически важные структуры» – объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

«международная информационная безопасность» – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

«неправомерное использование информационных ресурсов» – использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств Сторон либо норм международного права;

«несанкционированное вмешательство в информационные ресурсы» – неправомерное воздействие на процессы формирования, создания, обработки, преобразования, передачи, использования, хранения информации;

"угроза информационной безопасности» – факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве/

Приложение 2

Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.

Источником этой угрозы являются создание и развитие информационного оружия, представляющего непосредственную угрозу для критически важных структур государств, что может привести к новой гонке вооружений и представляет главную угрозу в области международной информационной безопасности.

Ее признаками являются применение информационного оружия в целях подготовки и ведения информационной войны, а также воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные структуры.

2. Информационный терроризм.

Источником этой угрозы являются террористические организации и лица, причастные к террористической деятельности, осуществляющие противоправные действия посредством или в отношении информационных ресурсов.

Ее признаками являются использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети Интернет или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе, а также иные негативные воздействия на информационные ресурсы.

3. Информационная преступность.

Источником этой угрозы являются лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

Ее признаками являются проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление DOS-атак (отказ в обслуживании) и иных негативных воздействий; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов и методов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т.д.

4. Использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран.

Источником этой угрозы является неравномерность в развитии информационных технологий в различных государствах и существующая тенденция к увеличению "цифрового разрыва" между развитыми и развивающимися странами. Некоторые государства, имеющие преимущества в развитии информационных технологий, умышленно ограничивают развитие прочих стран и получение доступа к информационным технологиям, что приводит к возникновению серьезной опасности для государств с недостаточными информационными возможностями.

Ее признаками являются монополизация производства программного обеспечения и оборудования информационных инфраструктур, ограничение участия государств в международном информационно-технологическом сотрудничестве, препятствующее их развитию и увеличивающее зависимость этих стран от более развитых государств; встраивание скрытых возможностей и функций в программное обеспечение и оборудование, поставляемые в другие страны, для контроля и влияния на информационные ресурсы и (или) критически важные структуры этих стран; контроль и монополизация рынка информационных технологий и продуктов в ущерб интересам и безопасности государств.

5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Источником этой угрозы являются государства, организации, группа лиц или частные лица, использующие информационную инфраструктуру для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Ее признаками являются появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в сети Интернет и других сетях информационного обмена информации:

искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения;

пропагандирующей идеи терроризма, сепаратизма и экстремизма;

разжигающей межнациональную, межрасовую и межконфессиональную вражду.

6. Угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Источниками этих угроз являются стихийные бедствия и другие опасные природные явления, а также катастрофы техногенного характера, возникающие внезапно или в результате длительного процесса, способные оказать масштабное разрушительное воздействие на информационные ресурсы государства.

Их признаками являются нарушение функционирования объектов информационной инфраструктуры и, как следствие, дестабилизация критически важных структур, государственных систем управления и принятия решений, результаты которой прямо затрагивают безопасность государства и общества.

Приложение С. ПРИМЕРЫ СТАТЕЙ УКРАИНСКИХ СМИ О РОЛИ РФ В КРИЗИСЕ НА УКРАИНЕ ПО МОДАЛЬНОСТИ[181]

Контекст упоминания, событие, тематика	Примеры статей с положительной модальностью	Примеры статей с нейтральной модальностью	Примеры статей с отрицательной модальностью
Роль РФ в ассоциации Украины с ЕС	«Мы (Украина) можем начать новые отношения между Украиной и РФ, но как интегрированная часть ЕС, как полностью независимое государство».	«Подписание соглашения об ассоциации с Евросоюзом создаст дополнительные возможности для сотрудничества Украины и Таможенного союза. Об этом заявил премьер Николай Азаров в Минске на совместной с премьером Беларуси Михаилом Мясниковичем пресс-конференции».	«… советник президента РФ Сергей Глазьев заявил, что в случае подписания соглашения об ассоциации с Евросоюзом Украина перестанет быть для России стратегическим партнером и фактически утратит статус субъекта международного права».
Двусторонние отношения РФ и Украины	«Н. Азаров подчеркнул, что Украина и Россия настроены на то, чтобы в двусторонних отношениях полностью устранить те противоречия, которые накопились за последние три с половиной года, включая главные - разногласия по контракту на поставку газа и нарушение	«Мы (Украина) предложили провести переговоры по урегулированию вопросов, вызывающих противоречия в трехстороннем формате (комиссия по торгово-экономическому сотрудничеству) при участии Украины, ЕС и России. Это чрезвычайно важный	«К сожалению, Украина, как никогда, стоит на пороге широкомасштабной агрессии со стороны нашего северного соседа. Действительно сейчас на границах Украины расположены российские войска, наиболее мощная группировка находится в аннексированном Крыму».

[181] Таблица построена на базе:
Официальный сайт интернет-издания «Украинская правда». (http://www.pravda.com.ua/rus/).
Официальный сайт государственного информационного агентства «УКРИНФОРМ». (http://www.ukrinform.ua/rus/).

	двусторонней производственной кооперации».	международный вопрос в условиях мировой рецессии, которая продолжается. После длительных и сложных переговоров Российская Федерация дала согласие на проведение таких переговоров».	
Переговоры РФ и Украины по проблеме поставок газа	«Отвечая на вопрос, какова вероятность, что встреча состоится в эти сроки, Новак сказал: «Я думаю, на 80% она состоится. Все заинтересованы, чтобы возобновились поставки газа, чтобы зимой не было никаких проблем с поставками газа»».	«Украина в ближайшие несколько лет может полностью отказаться от импорта газа из России, если действующий газовый контракт не будет пересмотрен».	«Российская Федерация пытается дискредитировать Украину как транзитера углеводородов, лоббируя в Евросоюзе собственные проекты»
Роль РФ в вооруженных действиях на Юго-Востоке Украины	—	«Обстановка в Донецке остается напряженной. В течение всего дня жители сообщают о том, что практически по всему городу слышны взрывы и работа тяжелых орудий».	«Они (РФ) продолжают свою тактику по дестабилизации ситуации в Украине (…) Почти 100 тысяч войск находится на границах Украины различными подразделениями в направлениях Чернигова, Харькова, Донецка. И эти войска находятся в боевой готовности уже несколько недель».

Санкции в отношении РФ	------	«Немецкие экономисты подсчитали возможные убытки от штрафных мер против Кремля в случае обострения ситуации в Украине. Их вывод: Запад может позволить себе проявить твердость».	“19 июня ЕвроПравда сообщала о том, что Комитет постоянных представителей стран-членов ЕС в Брюсселе согласовал проект решения Совета министров иностранных дел ЕС, которое будет утверждено в понедельник, 23 июня. Вопреки ожиданиям, в этом документе Евросоюз не планировал запуск третьего этапа санкций относительно Российской Федерации». «По мнению Премьера, Путин ставил цель разбить единство ЕС и США. "Наступил момент, когда мне начало казаться, что ему это удалось, но нет. Он потерпел поражение. Ценности свободы и демократии намного мощнее, чем российские танки и артиллерия и его автократичный режим. ЕС, США наложили санкции. Последний пакет санкций, наложенных на Россию, это реальная угроза российской экономике», - отмечает Яценюк, и добавляет, что недавно получил «тяжелую весть» о том, что прибыли Газпрома упали на 40%».

Присоединение Республики Крым к РФ	____	«Совет Федерации России единогласно ратифицировал договор между РФ и самопровозглашенной властью Крыма о вхождении полуострова и Севастополя в состав РФ».	«Мы, представители российской интеллигенции, обязаны предостеречь власть от совершающейся исторической ошибки - стремления взять под контроль с помощью вооруженных сил часть другой, еще недавно братской страны - Украины. Первый шаг - присоединение Крыма к России - уже сделан, первая кровь уже пролилась. Дальнейшие шаги на этом пути чреваты кровопролитием непредсказуемого масштаба, изоляцией России, превращением ее в страну-изгоя, а, в конечном счете, в страну третьего мира, на десятилетия отброшенную с цивилизационного пути».
Непричастность РФ к крушению малазийского Boeing-777	-----	«Президент Украины Петр Порошенко дал поручение пригласить российских экспертов для расследования причин авиакатастрофы малазийского лайнера в Донецкой области».	«Россия пытается скрыть доказательства своей непосредственной причастности к гибели пассажирского самолета Boeing-777».

Приложение D. БАЗОВЫЕ ДОКУМЕНТЫ РФ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[182]

Название документа	Содержание, цель, задачи
Конституция Российской Федерации	Признает и гарантирует права и свободы человека, в т.ч. информационные: свобода мысли и слова (ч. 1 ст. 29), право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29). Закрепляет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23), право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23).
Стратегия национальной безопасности РФ до 2020 года, 2009	Системообразующий документ в вопросах стратегического планирования обеспечения национальной безопасности, в частности, информационной сферы.
Доктрина информационной безопасности РФ, 2000	Сформулированы национальные интересы РФ в информационной сфере; выделены угрозы информационной безопасности РФ, внешние и внутренние источники этих угроз, способы обеспечения безопасности информации в стране.
Военная доктрина РФ, 2014	Определяет использование ИКТ в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности в качестве основных внешних военных опасностей. В качестве первой внутренней военной опасности указана деятельность, направленная на насильственное изменение конституционного строя России, дезорганизацию функционирования органов государственной власти, важных государственных, военных объектов и информационной инфраструктуры РФ. К основным внутренним угрозам относится деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая

[182] Построена на основе: Национальная безопасность России. Информационная безопасность. Сайт Совета Безопасности Российской Федерации. (http://www.scrf.gov.ru/documents/6/).

	целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества. К характерным чертам и особенностям современных военных конфликтов относится, в т.ч., комплексное применение военной силы, политических, экономических, информационных и иных мер невоенного характера, реализуемых с широким использованием протестного потенциала населения и сил специальных операций; массированное применение информационно-управляющих систем; воздействие на противника на всю глубину его территории одновременно в глобальном информационном пространстве, в воздушно-космическом пространстве, на суше и море; применение непрямых и асимметричных способов действий; использование финансируемых и управляемых извне политических сил, общественных движений. Первыми в числе основных задач РФ по сдерживанию и предотвращению военных конфликтов сформулированы: оценка и прогнозирование, в т.ч. с использованием современных технических средств и информационных технологий. Выделены задачи оснащения ВС и других войск вооружением, военной и специальной техникой, в т.ч. развитие сил и средств информационного противоборства и др; основные задачи развития военной организации, в т.ч. совершенствование системы информационной безопасности ВС, других войск и органов; пути выполнения основных задач строительства и развития ВС, других войск и органов, в т.ч., эффективное обеспечение информационной безопасности, развитие сил и средств информационного противоборства. Сформулированы задачи оснащения ВС, других войск и органов вооружением, военной и специальной техникой, в т.ч., развитие сил и средств информационного противоборства, качественное совершенствование средств информационного обмена на основе использования современных технологий и международных стандартов, единого информационного пространства ВС, других войск и органов как части информационного пространства РФ. К задачам военно-политического сотрудничества России отнесено развитие диалога с заинтересованными государствами о национальных подходах к противодействию военным опасностям и военным угрозам, возникающим в связи с масштабным использованием ИКТ в военно-политических целях.

Концепция внешней политики РФ, 2013	Развитие собственных эффективных средств информационного влияния на общественное мнение за рубежом, обеспечение усиления позиций российских СМИ в мировом информационном пространстве, предоставляя им необходимую государственную поддержку, активное участие в международном сотрудничестве в информационной сфере, принятие необходимые меры по отражению информационных угроз суверенитету и безопасности РФ.
Стратегия развития информационного общества в Российской Федерации, 2008	Закрепляет цель, задачи, принципы и основные направления государственной политики в области использования и развития информационных и телекоммуникационных технологий, науки, образования и культуры для продвижения России по пути формирования и развития информационного общества.
Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года, 2013	Разработана для формирования единого системного подхода государства к развитию отрасли информационных технологий с целью создания основ деятельности в области комплексного развития отрасли, в т.ч. за счет взаимодействия ее участников; обеспечения информационной безопасности и высокого уровня обороноспособности страны, в т.ч. за счет создания современных средств реагирования и предупреждения глобальных информационных угроз. Содержит определение отрасли информационных технологий. Определяет принципы, цели и основные направления развития отрасли в целом и ее отдельных сегментов, роль ИКТ в экономике государства, роль государства в развитии отрасли, механизмы и способы достижения поставленных целей. Включает основные индикаторы развития отрасли информационных технологий для базового и форсированного сценариев развития.
Основные направления научных исследований в области обеспечения информационной безопасности РФ, 2008	Выделяет гуманитарные проблемы обеспечения информационной безопасности России, научно-технические проблемы и проблемы кадрового обеспечения информационной безопасности РФ (физико-математические, технические).
Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и	Разработаны в целях реализации основных положений Стратегии национальной безопасности РФ до 2020 г. Одним из путей предотвращения угроз ИБ РФ является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в РФ.

технологическими процессами критически важных объектов инфраструктуры РФ, 2012	
Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, 2013	Определяет основные угрозы в области МИБ, цель, задачи и приоритетные направления государственной политики РФ в области МИБ.
Концепция информационной безопасности детей, 2015	Направлена на защиту детей от дестабилизирующего воздействия информационной продукции и создание условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия; содержит основные принципы обеспечения информационной безопасности детей, приоритетные задачи и механизмы реализации государственной политики в области ИБ детей.
Конвенция об обеспечении международной информационной безопасности (концепция) *(открыта для обсуждения в 2011 г.)*	Направлена на регулирование деятельности государств по обеспечению международной информационной безопасности.
ФЗ от 27 декабря 1991 года N 2124-1 «Закон о средствах массовой информации»	Определяет свободу массовой информации в РФ, содержит основные понятия в сфере СМИ. Устанавливает недопустимость цензуры и злоупотребления свободой СМИ. Определяет организацию деятельности СМИ. Устанавливает порядок распространения массовой информации, отношения СМИ с гражданами и организациями, права и обязанности журналиста, международное сотрудничество в области массовой информации, ответственность за нарушение законодательства о СМИ.
ФЗ «О связи» от 07.07.2003 N 126-ФЗ (принят ГД ФС РФ 18.06.2003, действующая редакция от 07.03.2014)	Регулирует в том числе и услуги по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет.
ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006 N 149-ФЗ (ред. от 28.12.2013)	Регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных». ФЗ № 261-ФЗ от 25 июля 2011 г. «О внесении изменений в ФЗ «О персональных данных»	Направлены на защиту персональных данных, осуществление контроля и надзора за выполнением организационных и технических мер по обеспечению безопасности персональных данных в государственных информационных системах персональных данных.
ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (ред. от 02.07.2013)	Содержит ограничения на распространение определенных видов информации среди детей.
ФЗ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»	Устанавливает полномочия трех федеральных органов исполнительной власти в сфере использования электронной подписи.
Гражданский кодекс РФ	Содержит нормы, регулирующие отношения по поводу интеллектуальных прав и результатов интеллектуальной деятельности.
Уголовный кодекс РФ	Предусматривает ответственность за компьютерные преступления, а некоторые его статьи, касающиеся «традиционных» видов преступлений, к примеру, мошенничество, могут быть применены к преступлениям, совершенным с использованием компьютера.
Кодекс Российской Федерации об административных правонарушениях	Предусматривает ответственность за правонарушения в области информации, за непредоставление в установленных случаях информации, за нарушение правил обращения с информацией и др.
Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 N 351 и Постановление Правительства РФ «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных	Приняты в целях повышения эффективности использования информационных технологий и обеспечения при этом информационной безопасности.

органов» от 24.05.2010 N 365 (ред. от 22.11.2013)	
Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (№ 1119 от 1 ноября 2012 г.)	Устанавливает 4 уровня защищенности персональных данных в зависимости от их состава, типа актуальных угроз и количества. Устанавливает требования к защите персональных данных при их обработке в информационных системах для каждого из уровней защищенности.
Постановление Правительства РФ от 25 июня 2012 г. № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг»	Устанавливает порядок определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг.
Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»	Возложение на ФСБ РФ полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, находящиеся на территории России и в дипломатических представительствах и консульских учреждениях РФ за рубежом.
ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»	Определяет алгоритм блочного шифрования с длиной блока 64 бита и длиной ключа 256 бит, а также режимы шифрования и режим выработки имитовставки.

ГОСТ Р ИСО/МЭК 13335-1-2006 ***ГОСТ Р ИСО/МЭК ТО 19791-2008*** ***ГОСТ Р 53114-2008*** ***ГОСТ Р 53131-2008 ИСО/МЭК ТО 24762:2008*** ***ГОСТ Р 34.10-2012*** ***ГОСТ Р 34.11-2012***	Определяют национальные стандарты РФ в сфере информационных технологий: методы и средства обеспечения ИБ; оценка безопасности автоматизированных систем, менеджмент безопасности ИКТ; обеспечение информационной безопасности в организации, основные термины и определения; защита информации, рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий; криптографическая защита информации, процессы формирования и проверки электронной цифровой подписи; алгоритмы вычисления двух функций хэширования с длинами хэш-кодов 256 и 512 бит.

Приложение Е. РЕЗОЛЮЦИЯ 69 СЕССИИ ГЕНЕРАЛЬНОЙ АССМБЛЕИ ООН «ДОСТИЖЕНИЯ В СФЕРЕ ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИЙ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ»

Шестьдесят девятая сессия
Пункт 91 повестки дня

Резолюция, принятая Генеральной Ассамблеей 2 декабря 2014 года

[по докладу Первого комитета (A/69/435)]

69/28. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Генеральная Ассамблея,

ссылаясь на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 2 декабря 2011 года, 67/27 от 3 декабря 2012 года и 68/243 от 27 декабря 2013 года,

ссылаясь также на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе,

напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13–15 мая 1996 года,

учитывая итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 года, а также принятые на нем рекомендации[183],

[183] См. A/51/261, приложение.

учитывая также результаты Всемирной встречи на высшем уровне по вопросам информационного общества (первый этап — Женева, 10–12 декабря 2003 года, второй этап — Тунис, 16–18 ноября 2005 года)[184],

отмечая, что распространение и использование информационных технологий и средств затрагивают интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности,

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам,

считая необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях,

отмечая важность уважения прав человека и основных свобод в сфере использования информационно-коммуникационных технологий,

отмечая также вклад государств-членов, представивших Генеральному секретарю свои оценки по вопросам информационной безопасности в соответствии с пунктами 1–3 резолюций 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 65/41, 66/24, 67/27 и 68/243,

принимая к сведению доклады Генерального секретаря, содержащие эти оценки[185],

отмечая с удовлетворением инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению в Женеве в августе 1999 года и в апреле 2008 года международных встреч экспертов по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также результаты этих встреч,

считая, что оценки государств-членов, содержащиеся в докладах Генерального секретаря, а также международные встречи экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий,

учитывая, что во исполнение резолюции 66/24 Генеральный секретарь учредил в 2012 году на основе справедливого географического распределения группу правительственных экспертов, которая в соответствии со своим мандатом рассмотрела существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве, а также провела

[184] См. A/C.2/59/3 и A/60/687.

[185] A/54/213, A/55/140 и Corr.1 и Add.1, A/56/164 и Add.1, A/57/166 и Add.1, A/58/373, A/59/116 и Add.1, A/60/95 и Add.1, A/61/161 и Add.1, A/62/98 и Add.1, A/64/129 и Add.1, A/65/154, A/66/152 и Add.1, A/67/167, A/68/156 и Add.1 и A/69/112 и Add.1.

исследование соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем,

с удовлетворением отмечая результативную работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и подготовленный в итоге соответствующий доклад, препровожденный Генеральным секретарем,

принимая к сведению оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов,

7. *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

8. *полагает*, что целям таких стратегий соответствовало бы продолжение изучения соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

9. *просит* все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[186], информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

   a) общая оценка проблем информационной безопасности;

   b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

   c) содержание концепций, упомянутых в пункте 2 выше;

   d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне;

10. *приветствует* начало работы Группы правительственных экспертов и уполномочивает Группу продолжить с учетом оценок и рекомендаций, содержащихся в упомянутом выше докладе, в целях содействия выработке общего понимания исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия, вопросов использования информационно-коммуникационных технологий в конфликтах и того, как

[186] A/68/98.

международное право применяется к использованию информационно-коммуникационных технологий государствами, а также концепций, упомянутых в пункте 2 выше, и представить доклад о результатах данного исследования Генеральной Ассамблее на ее семидесятой сессии;

11. *постановляет* включить в предварительную повестку дня своей семидесятой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

62-е пленарное заседание,
2 декабря 2014 года

Приложение F. ПРИЛОЖЕНИЕ К ПИСЬМУ ПОСТОЯННЫХ ПРЕДСТАВИТЕЛЕЙ КАЗАХСТАНА, КИТАЯ, КЫРГЫСТАНА, РОССИЙСКОЙ ФЕДЕРАЦИИ, ТАДЖИКИСТАНА И УЗБЕКИСТАНА ПРИ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ОТ 9 ЯНВАРЯ 2015 ГОДА НА ИМЯ ГЕНЕРАЛЬНОГО СЕКРЕТАРЯ

A/69/723

[Подлинный текст на китайском и русском языках]

Правила поведения в области обеспечения международной информационной безопасности

Генеральная Ассамблея:

ссылаясь на резолюции Генеральной Ассамблеи о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях;

ссылаясь также на свои резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 13 декабря 2011 года, 67/27 от 3 декабря 2012 года и 68/243 от 27 декабря 2013 года;

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации;

признавая необходимость предотвращения возможности использования информационно-коммуникационных технологий в целях, которые не совместимы с задачами обеспечения международной стабильности и безопасности, и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности;

подчеркивая необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий и в этом контексте отмечая ту роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации;

подчеркивая важность безопасного, непрерывного и стабильного функционирования Интернета и необходимость защиты Интернета и других сетей информационно-коммуникационных технологий от возможного неблагоприятного воздействия и подверженности рискам; подтверждая необходимость выработки общего понимания вопросов безопасности Интернета и дальнейшего сотрудничества на национальном и международном уровнях;

вновь подтверждая, что политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств, государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня;

учитывая оценки и рекомендации, содержащиеся в итоговом докладе Группы правительственных экспертов, созданной в 2012 году в соответствии с резолюцией 66/24 на основе справедливого географического распределения, которая в соответствии со своим мандатом изучила существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия в информационном пространстве и провела исследование соответствующих международных концепций, которые направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

подтверждая необходимость изучения общего понимания того, как нормы, основанные на положениях существующего международного права, относящихся к сфере использования информационно-коммуникационных технологий государствами, применение которого является необходимой предпосылкой для снижения рисков нарушения международного мира, безопасности и стабильности, будет применяться к поведению государств и использованию информационно-коммуникационных технологий государствами в соответствии с параграфом 16 доклада Группы правительственных экспертов от 24 июня 2013 года (A/68/98);

отмечая, что с учетом уникальных особенностей информационно-коммуникационных технологий со временем могут быть разработаны дополнительные нормы в соответствии с параграфом 16 доклада Группы правительственных экспертов;

признавая, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к главным опорам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности, как отмечается в резолюции Генеральной Ассамблеи 64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»;

отмечая необходимость активизации усилий по преодолению цифрового разрыва путем облегчения передачи информационно-коммуникационных технологий развивающимся странам и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности, как отмечается в резолюции Генеральной Ассамблеи 64/211;

принимает следующие Правила поведения в области обеспечения международной информационной безопасности:

1. Цели и область применения

Основная цель настоящих Правил поведения заключается в определении прав и обязанностей государств в информационном пространстве, стимулировании их конструктивного и ответственного поведения и укрепления сотрудничества между ними для противостояния общим вызовам и угрозам в информационном пространстве с тем, чтобы

создать мирную, безопасную, открытую и основанную на сотрудничестве информационную среду и чтобы использование информационно-коммуникационных технологий и информационных и коммуникационных сетей способствовало полномасштабному социальному и экономическому развитию и благосостоянию народов, и не противоречило целям обеспечения международного мира и безопасности.

Правила поведения открыты для присоединения любых государств на добровольной основе.

2. Правила поведения

Каждое государство, добровольно соблюдающее настоящие Правила поведения, обязуется:

1. Соблюдать Устав Организации Объединенных Наций и общепризнанные принципы и нормы международного права, которые включают, помимо прочего, уважение суверенитета, территориальной целостности и политической независимости всех государств, уважение прав и основных свобод человека, а также уважение многообразия истории, культуры и социального устройства всех стран.

2. Не использовать информационно-коммуникационные технологии и информационные и коммуникационные сети для осуществления действий, которые противоречат задачам поддержания международного мира и безопасности.

3. Не использовать информационно-коммуникационные технологии и информационные и коммуникационные сети для вмешательства во внутренние дела других государств и в целях подрыва их политической, экономической и социальной стабильности.

4. Сотрудничать в борьбе с преступной или террористической деятельностью с использованием информационно-коммуникационных технологий и информационных и коммуникационных сетей и сдерживать распространение информации террористического, сепаратистского или экстремистского характера, а также разжигающей ненависть на национальной, расовой или религиозной почве.

5. Прикладывать усилия к обеспечению безопасности на всех этапах поставок продукции и предоставления услуг в сфере информационно-коммуникационных технологий, предотвращать использование другими государствами своей доминирующей позиции в сфере информационных технологий, включая, среди прочего, доминирование в основных ресурсах, критической инфраструктуре, ключевых технологиях, продуктах и услугах информационно-коммуникационных технологий и информационных и коммуникационных сетях, для подрыва права государств на независимый контроль над продуктами и услугами информационно-коммуникационных технологий или для создания угроз их политической, экономической и социальной безопасности.

6. Подтверждать права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии.

7. Признавать, что права, которые человек имеет в оффлайновой среде, должны также защищаться и в онлайновой среде. В полной мере уважать права и свободы в информационном пространстве, в том числе на поиск, получение, передачу и распространение информации, принимая во внимание то, что в соответствии с Международным пактом о политических и гражданских правах (статья 19) пользование этими правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые должны быть установлены законом и являться необходимыми:

a) для уважения прав и репутации других лиц;
b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

8. Все государства должны играть одинаковую роль в международном управлении Интернетом и нести равную ответственность за управление Интернетом, его безопасность, непрерывность и стабильность функционирования, а также развитие с тем, чтобы содействовать созданию многосторонних, прозрачных и демократических международных механизмов управления Интернетом, которые позволят обеспечить справедливое распределение ресурсов, способствовать доступу для всех, а также гарантировать стабильное и безопасное функционирование Интернета.

9. Все государства должны в полной мере сотрудничать с другими заинтересованными сторонами и способствовать углублению осознания всеми элементами общества, в том числе частным сектором и институтами гражданского общества, своей ответственности за обеспечение информационной безопасности, включая формирование культуры информационной безопасности и поддержку усилий по защите объектов критической информационной инфраструктуры.

10. Развивать меры укрепления доверия в целях повышения предсказуемости и снижения вероятности недопонимания, а также риска возникновения конфликта. Эти меры включают, среди прочего, добровольный обмен информацией о национальных стратегиях и организационных структурах, направленных на обеспечение информационной безопасности страны, публикацию «белых книг» и обмен наилучшими практиками в тех случаях, когда это практически возможно и целесообразно.

11. Оказывать содействие развивающимся странам в «наращивании потенциала» в сфере информационной безопасности и по преодолению «цифрового разрыва».

12. Укреплять двустороннее, региональное и международное сотрудничество. Способствовать тому, чтобы Организация Объединенных Наций играла важную роль в таких областях, как стимулирование выработки международных правовых

норм в области информационной безопасности, мирное разрешение международных споров, повышение качественного уровня сотрудничества государств в сфере информационной безопасности, а также в других сферах. Интенсифицировать координацию между соответствующими международными организациями.

13. Любой спор, который может возникнуть в ходе деятельности, охватываемой настоящими Правилами поведения, должен разрешаться с помощью процедур мирного урегулирования, воздерживаясь от применения военной силы или угрозы силой.

Об авторах

Евсеев В.В. – старший научный сотрудник Группы проблем информационной безопасности Центра международной безопасности ИМЭМО РАН; заведующий отделом евразийской интеграции и развития ШОС Института стран СНГ; кандидат технических наук, ученое звание: старший научный сотрудник.

Идаятов А.К. – эксперт по проблемам информационной безопасности; кандидат политических наук.

Ковалев В.И. – заместитель главного редактора журналов «Стратегическая стабильность» и «Информационные войны»; кандидат технических наук.

Ромашкина Н.П. – старший научный сотрудник, руководитель Группы проблем информационной безопасности Центра международной безопасности ИМЭМО РАН; кандидат политических наук, профессор АВН РФ.

Топычканов П.В. – старший научный сотрудник Группы проблем информационной безопасности Центра международной безопасности ИМЭМО РАН; кандидат политических наук.