ГЛОБАЛЬНЫЕ ВОЕННО-ПОЛИТИЧЕСКИЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ТЕНДЕНЦИИ, УГРОЗЫ, ПЕРСПЕКТИВЫ

Ромашкина Н.П.[1]

Аннотация. *Представлен анализ актуальных военно-политических проблем в информационной сфере, которые носят глобальный, стратегический характер и требуют незамедлительного создания механизмов международного управления, одним из которых могут стать Правила поведения государств в информационном пространстве, принятия которых в ООН целенаправленно добивается Россия. В статье выявлены признаки наличия проблемы применения информационно-коммуникационных технологий (ИКТ) в военно-политических целях для осуществления враждебных действий и актов агрессии, представлены ИКТ-средства для применения в военной области и проанализированы возможности осуществления угроз, создающих проблему. Указаны тенденции, увеличивающие риски для военных объектов как части критически важной государственной инфраструктуры. Обоснован вывод о том, что защита таких объектов от ИКТ-угроз является одной из важнейших проблем современности.*

Ключевые слова: *информационно-коммуникационные технологии (ИКТ), информационное пространство, кибероружие, информационная угроза, киберугроза, кибератака, критически важные объекты государственной инфраструктуры.*

DOI: 10.21681/2311-3456-2019-1-2-9

Введение

Перемены в политической, экономической и социально-культурной сферах в 21 веке все больше зависят от ускоренного развития новых информационно-коммуникационных технологий (ИКТ), под которыми понимаются процессы и методы взаимодействия с информацией, осуществляемые с применением устройств вычислительной техники и средств телекоммуникации. В условиях современной четвёртой индустриальной революции, объединяющей возможности промышленного производства, информационных технологий, а также интернета вещей и услуг, индекс конкурентоспособности экономики государств имеет высокий уровень корреляции с индексом развития ИКТ [1]. А по оценкам Бостонской консалтинговой группы (The Boston Consulting Group), одной из лидеров в области аналитики экономики и управленческого консалтинга, влияние Интернета на эффективность деятельности компаний выше, чем любой другой технологии со времен предыдущей промышленной революции [2]. Таким образом, развитие ИКТ-средств ведет к прорывным результатам не только в виртуальном, но и вполне реальном, физическом пространстве. Вероятно, поэтому сегодня идет жесткая борьба за роли в этой революции.

Однако вместе с уникальными возможностями ИКТ несут и глобальные угрозы. Информационные диверсии в ИКТ-пространстве стали новым орудием негосударственных коллективных и индивидуальных субъектов [3,4,5]. Кроме того, информационные методы превращается в важный элемент военного потенциала государств, дополняющий, а иногда и заменяющий обычные военные средства. ИКТ могут стать детонатором развязывания межгосударственного военного конфликта, а кибервойны одних государств против других могут оказаться не менее разрушительными, чем традиционные [6]. Ни одна страна в мире не может считать себя защищенной от трансграничных информационных угроз и не в состоянии решить проблемы информационной безопасности в одиночку.

Несмотря на разногласия между государствами в ИКТ-сфере, стремительное нарастание угроз делает информационное пространство не только плацдармом для конфликта, но и территорией необходимого и неизбежного сотрудничества. Глубокое осознание этого факта привело к тому, что в конце прошлого века Россия стала инициатором международного обсуждения соответствующих проблем. С тех пор деятельность РФ в процессе обеспечении международной информационной безопасности (МИБ) в рамках ООН и других организаций направлена на выработку подходов к управлению ИКТ-пространством, а в результате – на установление международного правового режима для создания эффективной системы информационной безопасности.

Однако процесс выработки режима обеспечения МИБ идет медленнее нарастания угроз. Поиск компромисса в ходе переговоров на многосторонней основе – единственный способ минимизировать угрозы в этой сфере. А для этого надо прийти к общему пониманию существующих глобальных проблем. Таким образом, необходимость классификации ИКТ-угроз, являющихся признаками наличия этих проблем, является одной из важнейших, указанных в документах ООН, но пока еще не реализованных задач. В настоящее время существуют различные варианты классификации, представленные в национальных нормативно-правовых базах государств и организаций. Однако

1 Ромашкина Наталия Петровна, кандидат политических наук, член-корреспондент АВН РФ, руководитель Группы проблем информационной безопасности Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН, Москва, Россия. E-mail: Romachkinan@yandex.ru.

ни один из них пока не стал общепринятым и удовлетворяющим интересам всех заинтересованных стран. Поэтому значимость постоянного мониторинга и исследования вредоносных информационных технологий неуклонно возрастает. Данная статья базируется на анализе международного опыта в этой сфере и той классификации угроз, которая представлена в документах РФ [7].

Так, в нормативно-правовой базе России под международной информационной безопасностью (МИБ) понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.[2]

В качестве одной из самых опасных угроз МИБ в российских документах указано применение информационного оружия в военно-политических целях для осуществления враждебных действий и актов агрессии. Важнейшими также признаны угрозы деструктивного ИКТ-воздействия на элементы критически важных объектов государственной инфраструктуры [8]; вмешательства во внутренние дела суверенного государства [9], нарушения общественной стабильности, разжигания межэтнической, межнациональной розни посредством ИКТ [10].[3]

Наличие этих опасностей представляет угрозу международному миру, а значит, требует незамедлительного поиска дополнительных механизмов международного управления. Одним из первых таких механизмов могут стать Правила поведения государств при обеспечении МИБ[4], принятия которых в ООН целенаправленно и настойчиво добивается Россия [11].

Применение ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии

Информационные операции в современном мире предоставляют уникальные возможности для создания деструктивного эффекта. Военные средства, способствующие проведению этих операций, включают стратегические коммуникации, межведомственные координационные группы, действия в киберпространстве и в космосе, поддержку информации, разведку, специальные технические процедуры и т.д. [12].

Бесспорным мировым лидером в этой сфере в течение многих являются США. По выражению известного американского политолога Джозефа Ная, «Та страна, которая возглавит информационную революцию, и будет обладать большей силой по сравнению со всеми другими странами» [13]. При этом стратегия достижения информационного превосходства, под которым в США понимается способность собирать, обрабатывать и распространять непрерывный поток информации, лишая противника возможности осуществлять подобные действия[5], совершенствуется уже несколько десятилетий, что нашло отражение в доктринальных документах и в практике применения информационных операций. Такая ситуация несет дополнительные риски, она напрямую связана с проблемой обеспечения стратегической стабильности. А потому требует особого внимания специалистов.

Одна из важнейших актуальных тенденций связана с тем, что защищенность ИКТ-систем имеют стратегическое значение для большинства стран мира. Эти системы стали важным фактором обеспечения суверенитета, обороноспособности и безопасности государства. При этом речь сегодня идет об угрозе развития так называемых информационных вооружений. По некоторым оценкам, уже более 30 государств обладают наступательным кибернетическим оружием (кибероружием).[6] ИКТ могут спровоцировать развязывание межгосударственного военного конфликта, в первую очередь, из-за возможности несоразмерного использования методов реагирования на угрозы и атаки: пострадавшая сторона может применить в ответ реальное оружие. Кроме того, конфликт может возникнуть по ошибке, т.к. в настоящее время отсутствует универсальная методология идентификации нарушителей, не выработаны критерии отнесения кибератак к вооруженному нападению, не сформированы универсальные принципы расследования инцидентов.

На сегодняшний день создан широкий спектр ИКТ-средств для применения в военной области. В частности, это борьба с системами управления и контроля — военная стратегия с применением информационной среды на поле боя для физического разрушения командной структуры противника; разведывательное противоборство — наступательные и оборонительные операции с помощью автоматизированных систем, которые, в свою очередь, являются потенциальными объектами кибератак; электронное противоборство — военные действия с использованием электромагнитной и направленной энергии для контроля противника, которые состоит из трех подраз-

2 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/114.html. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» / КонсультантПлюс. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.4901291400816738 5#07272430789919533.

3 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/114.html. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» / КонсультантПлюс. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&fld=134&dst=1000000001,0&rnd=0.4901291400816738 5#07272430789919533.

4 Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. United Nations A/69/723. [Электронный ресурс]. URL: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

5 Joint Vision 2010 [issued in 2006], The Defense Technical Information Center. Official website [Электронный ресурс]. URL: http://www.dtic.mil/jv2010/jv2010.pdf.

6 Ромашкина Н.П. Стратегическая стабильность: новые вызовы инфосферы. Российский совет по международным делам [Электронный ресурс]. URL: http://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery/.

делений: электронная атака, электронная защита и поддержка электронного противоборства (в русскоязычных источниках эквивалентом понятия «электронное противоборство» часто является «радиоэлектронная борьба» — РЭБ[7]); военные средства, способствующие проведению информационных операций, в частности, включающие стратегические коммуникации, вмешательства в киберпространстве и космосе, военную поддержку информации, разведку, совместные операции электромагнитного спектра и т.д. [14].

Связанные с этими возможностями проблемы можно отнести к различным элементам военной организации и инфраструктуры. Но важнейшим, безусловно, является блок ИКТ-угроз в сфере ядерного оружия (ЯО) (рис. 1). Сегодня существуют различные мнения в отношении вероятности и последствий вредоносного воздействия ИКТ-средств на систему командования, управления и контроля над ЯО: от полного отрицания до доказательств резкого увеличения такой вероятности. Однако, и в науке вообще, и в военной стратегии, в частности, необходимо исходить из худших вариантов развития событий. Следовательно, эта проблема должна находиться в фокусе внимания ученых и практиков, в первую очередь, из государств – обладателей ЯО. При этом речь не идет о необходимости в корне менять основополагающие принципы управления. ИКТ-угрозы обостряют, осложняют, углубляют, усиливают и видоизменяют те проблемы, которые всегда существовали в обеспечении безопасности ЯО.

Угрозы, создающие проблему применения ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии, признаки наличия и возможности осуществления этих угроз представлены в таблице 1.

Информационная безопасность военных объектов как части критически важной инфраструктуры государства

К критически важным объектам инфраструктуры государства (КИ) относят системы и средства, которые настолько жизненно важны для страны, что нарушение их работы или уничтожение оказывает необратимое негативное воздействие на национальную и экономическую безопасность, здравоохранение, правопорядок и т.д. При этом под безопасностью КИ понимается защищенность от угроз, реализуемых посредством применения специальных информационных технологий для разрушения либо для недопустимого использования этих объектов [15]. Даже если эти объекты не подключены к Интернету напрямую, устройства автоматизированной системы управления технологическим процессом (АСУ ТП), используемые для дистанционного контроля по защищенным коммуникационным линиям, могут быть взломаны в результате атаки на другие объекты, где функционируют АСУ ТП. Изоляция сети от внешних систем, считавшаяся незыблемым требованием 10–15 лет назад, больше не рассматривается как эффективная защитная мера, т.к. стала невыгодной экономически и трудно реализуемой на практике. Поэтому угроза крупномасштабной комплексной атаки на критически важную инфраструктуру более чем реальна и ускоренно возрастает (рис. 2).

Сегодня уже более 30 стран обладают программным обеспечением (ПО) для нападения на объекты КИ. При этом показатель опасности для АСУ ТП в настоящее время оценивается специалистами как критический или высокий. В 2018 г. были зафиксированы ежемесячные кибератаки на каждый четвертый компьютер на про-

Рис. 1. Стратегические ядерные вооружения: некоторые ИКТ-уязвимости и потенциальные последствия

7 Российская армия получит средства РЭБ нового поколения. 3 ноября 2016. Медиагруппа Звезда [Электронный ресурс]. URL: http://tvzvezda.ru/news/opk/content/201611031232-3nca.htm.

Таблица 1.

Проблема применения ИКТ в военно-политических целях для осуществления враждебных действий и актов агрессии

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие ИКТ-вооружений	Ускоренная милитаризация ИКТ-пространства.	**ИКТ-средства для применения в военной области:** ● борьба с системами управления и контроля; ● разведывательное противоборство; ● электронное противоборство; ● военные средства, способствующие проведению информационных операций.
	Включение ИКТ-сферы в интегрированное поле боевых действий в стратегиях некоторых стран.	
	Наличие наступательного кибероружия и кибервойск у 30 государств.	
	Наращивание возможностей наступательных и оборонительных информационных и кибероперациий странами НАТО.	
	Планы создания средств кибервойны у 140 стран.	
	Сложность выявления автора ИКТ-атаки, возможность использования «ложного флага», что ведет к отсутствию ответственности.	
Использование «мягкой силы» с применением ИКТ во враждебных военно-политических целях, для вмешательства во внутренние дела государств	Рост количества фактов вмешательства во внутренние дела государств с применением ИКТ:	**Альтернативные военному давлению методы и средства воздействия на противника:** ● **экономические** (ИКТ-воздействие на промышленные и финансовые объекты); ● **информационные** (пропагандистское иновещание, Интернет (поисковые системы, социальные сети, сетевые «зеркала»), мобильные приложения, смс) для подготовки и проведения массовых беспорядков, антиправительственных демонстраций, политических акций, государственных переворотов.
	● Революция «Солидарности», Польша, 1980-1990;	
	● «Бархатная революция», Чехословакия, 1989;	
	● «Бульдозерная революция», Югославия, 2000;	
	● подготовка вторжения с применением ИКТ, Афганистан, 2001;	
	● «Революция роз», Грузия, 2003;	
	● вторжение с применением ИКТ, Ирак, 2003;	
	● «Оранжевая революция», Украина, 2004;	
	● «Революция тюльпанов», Киргизия, 2005;	
	● «Жасминовая революция», Тунис, 2011;	
	● «Твиттерная революция» («Революции лотоса»), Египет, 2011;	
	● гражданская война, Ливия, 2011;	
	● «Евромайдан», Украина, 2013-2014;	
	● «Революция розеток», Армения, 2015;	
	● гражданская война, Сирия, 2011 – наст. время;	
	● подготовка государственного переворота, Венесуэла, 2019.	

мышленных предприятиях РФ. Вредоносные программы разрабатываются в настоящее время во многих странах, однако 83% всех площадок, используемых для распространения «зловредов», расположены всего в 10 государствах. Лидером этого рейтинга являются США, где находится четверть всех источников заражения. Целями таких «вредоносов» могут быть органы государственной власти, банки, спутниковые, нефтегазовые и транспортные системы, электро- и атомные станции, коммуникационные системы, порты, аэропорты, военные объекты, что может привести к страшным последствиям как на государственном, так и на глобальном уровне. Таким образом, подобные вредоносные программы представляют собой перспективное стратегическое оружие, а растущая сложность оборудования и ПО КИ ведет к росту вероятности ошибок и уязвимостей, что может быть использовано противником.

Отметим некоторые общемировые тенденции, увеличивающие угрозы для таких объектов:

- использование личных мобильных устройств на критически важных объектах;
- переход на цифровые системы управления производственными и технологическими процессами на таких объектах;
- подключение офисных и промышленных корпоративных сетей объектов инфраструктуры к Интернету;
- сложность трансконтинентальных цепочек поставок программного обеспечения систем управления производственными и технологическими процессами.

Эти тенденции касаются всех объектов КИ. Но наибольшее беспокойство вызывают угрозы системе командования и управления ядерным оружием (рис. 1).

Одной из самых серьезных угроз в военной ядерной сфере является возможность влияния ИКТ на рост вероятности несанкционированного запуска баллистических ракет (БР), а также на принятие решения о применении ЯО [16]. Задача защиты БР от несанкционированных пусков возникла с момента создания первых ракет. Она

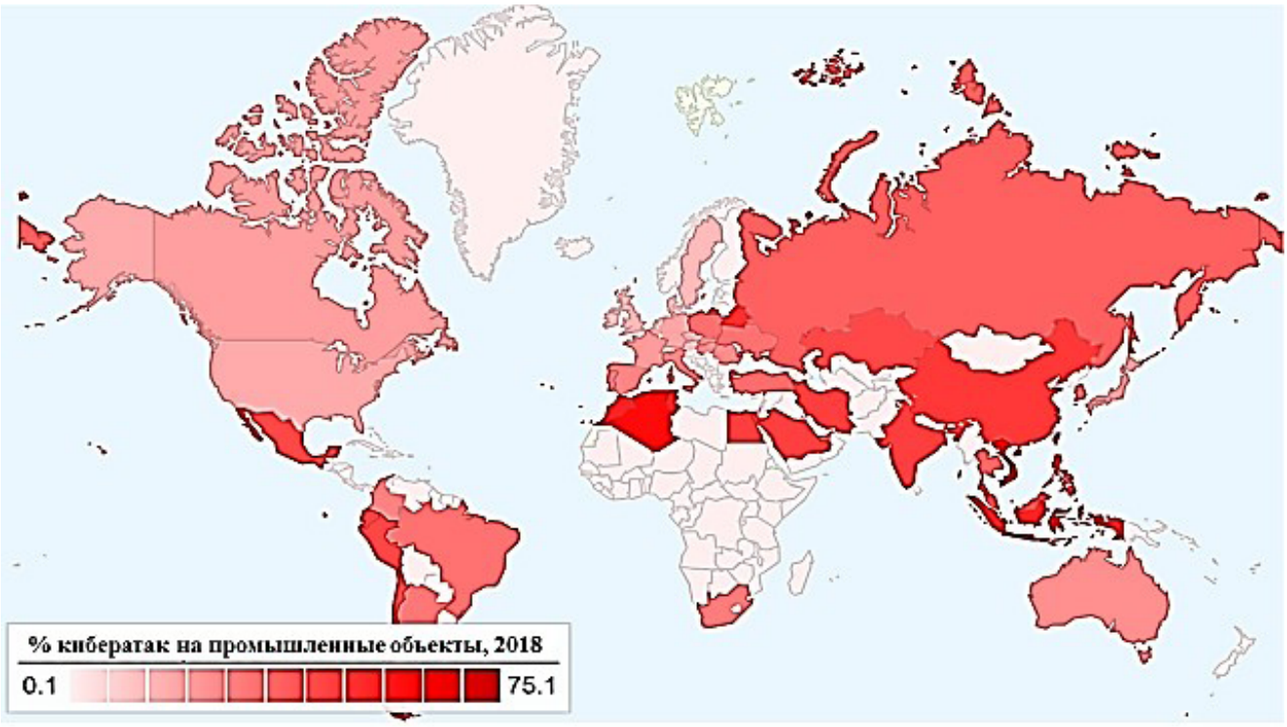

Рис. 2. География кибератак на промышленные системы, 2018 г.

каждый раз решается заново при создании новых БР, постановке их на дежурство, подготовке и проведении испытательных, учебно-боевых и контрольно-боевых пусков. Несмотря на то, что и США, и Россия (СССР) всегда уделяли этому большое внимание, за десятилетия существования ЯО в обеих странах были случаи технических сбоев и человеческих ошибок, которые могли бы спровоцировать ядерный запуск. Избежать такой ситуации в будущем будет еще сложнее, т.к. проблема снижения вероятности случайного запуска будет стоять более остро по мере перехода войск стратегического назначения в разных странах на цифровые технологии передачи информации. Так, по данным Минобороны России, Ракетные войска стратегического назначения (РВСН) РФ полностью перейдут на цифровые технологии уже к 2020 г.[8]

Эта угроза продиктована возможностью получения ложной информации от систем предупреждения о ракетном нападении (СПРН) о запуске БР со стороны противника. В связи с тем, что кибератаки становятся все более изощренными, растет вероятность обхода хакерами существующей системы защиты для отправки сигнала о запуске ракет. Кроме того, могут быть повреждены или разрушены каналы коммуникаций, созданы помехи в системе управления вооруженными, в том числе, ядерными, силами, а также снижена уверенность военных, принимающих решения, в работоспособности систем управления, командования и контроля. Таким образом, в кризисной ситуации ИКТ-нападения могут негативно повлиять на принятие решения об ответных действиях. Эти проблемы в настоящее время активно обсуждаются на Западе экспертами с глубоким знанием ядерных сил РФ и США, поэтому отвергать или игнорировать их в России нецелесообразно и опасно.

Угрозы, создающие проблему обеспечения ИКТ-безопасности объектов военно-промышленного комплекса (ВПК), признаки наличия и возможности осуществления этих угроз представлены в таблице 2.

Заключение

Отказ от продолжения диалога по проблемам международной информационной безопасности может привести к тяжелым последствиям. С учетом нарастания угроз в области МИБ для того, чтобы сделать информационное пространство более устойчивым и безопасным, необходимо решить целый комплекс очень сложных задач.

Представляются целесообразными следующие шаги.

1. Продолжать двусторонние (РФ-США) и многосторонние (с привлечением «третьих» ядерных государств) переговоры по ограничению и сокращению стратегических ядерных вооружений.
2. Включать важнейшие специальные вопросы информационной (кибер) безопасности в переговоры по ядерным вооружениям и стратегической стабильности на двусторонней (Россия-США, Россия-КНР) и многосторонней основе с участием России.
3. Разрабатывать конкретные меры по укреплению доверия (в частности, обмен данными об информационных угрозах, практическое межгосударственное сотрудничество).
4. Государствам – обладателям ЯО:

- совершенствовать информационную безопасность критически важной государственной инфраструктуры, в частности, военных объектов;

8 К 2020 году РВСН полностью перейдут на цифровые технологии передачи информации. Министерство обороны Российской Федерации (Минобороны России) [Электронный ресурс]. URL: https://structure.mil.ru/structure/forces/strategic_rocket/news/more.htm?id=12142122%40egNews.

Таблица 2.

Проблема обеспечения информационной безопасности военных объектов как части критически важной инфраструктуры государства

Угроза	Признаки наличия угрозы	Возможности осуществления угрозы
Развитие ИКТ-средств для вредоносного воздействия на объекты ВПК	Наличие ИКТ-угроз для различных элементов военной организации и инфраструктуры. Важнейшие: стратегические вооружения, система предупреждения о ракетном нападении (СПРН), система командования и контроля над ядерным оружием (ЯО), ПРО, ПВО.	● Кибернападения на объекты военной или связанной с ней гражданской инфраструктуры; ● физический вред ПО, элементной базе, линиям связи и сетям военного объекта; ● дистанционный «логический» вред с помощью ВП, «логических бомб» и т.д.; ● умышленный или непреднамеренный удаленный вред через компьютерные сети (в т.ч. Интернет) или в результате контакта с компьютером; ● кибершпионаж и создание киберагентурных сетей; ● киберсаботаж; ● создание неуверенности командования и персонала в бесперебойной и эффективной работе систем.
	Рост масштабов применения ударных роботизированных средств с дистанционным управлением, искусственного интеллекта в военных целях, автоматизированных систем принятия решений и т.д., которые могут подвергаться кибератакам.	
	Перевод войск стратегического назначения в разных странах на цифровые технологии передачи информации, что сделает их более уязвимыми для технических ошибок и преднамеренных кибератак.	
Снижение уровня стратегической стабильности	Влияние развития ИКТ на рост вероятности:	
	● несанкционированного запуска баллистических ракет (БР), на принятие решения о применении ЯО;	
	● получения ложной информации от СПРН о запуске БР со стороны противника из-за растущей изощренности кибератак;	
	● повреждения или разрушения каналов коммуникаций, создания помех в системе управления вооруженными, в том числе, ядерными, силами;	
	● снижения уверенности военных, принимающих решения, в работоспособности систем управления, командования и контроля ВС.	
	Влияние роста вероятности выведения из строя или уничтожения ЯО посредством ИКТ на будущее процессов ядерного разоружения и нераспространения.	
	Влияние ИКТ-факторов на уровень стратегической стабильности.	

- повышать эффективность подготовки персонала (обеспечивать унификацию специалистов, их правильное территориальное рассредоточение, дублирование обработки данных, узкую специализацию программного обеспечения и т. д.);
- укреплять боевую устойчивость вооруженных сил (стратегических сил сдерживания) в условиях возможного выхода из строя объектов критически важной государственной инфраструктуры.

5. Расширять совместные международные исследовательские проекты с участием российского научно-экспертного сообщества для обсуждения проблем организации партнерства в области международной информационной безопасности.
6. Активизировать научные исследования по разработке теоретических, методологических и практических подходов к решению проблемы стратегической стабильности.
7. Для России необходимо совершенствовать эффективность системы сертификации импортных программных средств и элементной базы, планируемых для применения на критически важных для обороны и безопасности страны объектах, а также систему обеспечения информационной безопасности разрабатываемых современных компьютерных технологий в условиях расширения импортозамещения программно-аппаратных компонентов программного обеспечения и оборудования с целью перехода в обозримой перспективе на полностью отечественную элементную базу.
8. Создавать под эгидой ООН международный режим контроля над вредоносным ИКТ:

- принятие правил ответственного поведения государств в области обеспечения международной информационной безопасности;
- разработка международных норм в отношении средств и методов предотвращения и устранения киберконфликтов;
- ограничение и/или отказ от наступательных ИКТ-возможностей;
- запрет на ИКТ-атаки на конкретные объекты;
- контроль за распространением ИКТ-вооружений.

Литература

1. Schwab K. The fourth industrial revolution: What It Means and How to Respond? //Foreign Affairs. December 12, 2015. URL: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.
2. Зарецкий А.Д., Иванова Т.Е. Промышленные технологии и инновации. 2-е издание. – СПб: Кубанский государственный университет, 2018.
3. Варфоломеев А.А. Кибердиверсия и кибертерроризм: пределы возможностей негосударственных субъектов на современном этапе // Военная мысль. 2012. № 12.
4. Матвиенко Ю.А. Информационно-психологическая война как одна из форм разрешения социально-политических противоречий в современном обществе// Информационные войны. 2015. № 4.
5. Information Security Threats during Crisis and Conflicts of the XXI Century / Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO, 2016. URL: https://www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.
6. U.S. Cyberattacks Target ISIS in a New Line of Combat // The New York Times. April 24, 2016 // https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.
7. Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016. URL: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.
8. Broad W., Markoff J., Sanger D. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. 2011. January 15. URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.
9. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1.
10. Сундиев И.Ю., Смирнов А.А., Костин В.Н. Новое качество террористической пропаганды: медиаимперия ИГИЛ // Информационные войны. 2015. № 1.
11. Ромашкина Н.П. Перспективы международной информационной безопасности / Безопасность и контроль над вооружениями 2017–2018. Преодоление разбалансировки международной стабильности / отв. ред. А. Г. Арбатов, Н. И. Бубнова. – М.: ИМЭМО РАН; Политическая энциклопедия, 2018.
12. Molander R., Riddile A., Wilson P. Strategic information warfare: a new face of war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1996. 33 p. URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf
13. Nye J. S. Controlling Cyber Conflict // Project Syndicate. Aug. 8, 2017 // https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08/russian.
14. Molander R., Wilson P., Mussington D., Mesic R. Strategic information warfare rising war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1998. URL: https://www.rand.org/pubs/monograph_reports/MR964.html.
15. Сангалов В.А. Угрозы национальной безопасности России в информационной сфере // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – Тамбов: Издательство «Грамота». 2015. № 8-3 (58) // http://www.gramota.net/materials/3/2015/8-3/44.html.
16. Sherman F. Aborting Unauthorized Launches of Nuclear-Armed Ballistic Missiles through Postlaunch Destruction // Science and Global Security, 1990, Volume 2, No. 1.

Рецензент: *Гладышев Вадим Георгиевич, доктор технических наук, профессор, член-корреспондент Академии военных наук РФ, gladyshevvg@mail.ru.*

GLOBAL MILITARY POLITICAL PROBLEMS IN INTERNATIONAL INFORMATIONAL SECURITY: TRENDS, THREATS AND PROSPECTS

N.P. Romashkina[9]

Abstract. *Article presents analysis of the most relevant military and political problems in informational sphere, which carry global and strategical nature. Existence of these threats requires immediate development of mechanisms of international administration. One of such mechanisms may be rules of states actions in ensuring international informational security. Russia is purposefully striking for acceptance of these rules in UN. Article proves that the problem of application of informational communicational technologies (ICT) with military and political purposes for realization of hostile actions and acts of aggression is critical. Indications of such problem was found in the article along with ICT means for military operations and the most relevant trends requiring actions at national and international levels. This problem is related to the issues of security of material and informational objects of critically important state infrastructure (CI). Article demonstrates worldwide trends leading to the increase of threats related to military objects as part of CI. Author explains the conclusion that the problem of safety of these objects from threats, realized through application of special informational technologies is one of the main problems of the present.*

Key words: *Information and communication technology (ICT), information space, cyber weapon, informational threat, cyber threat, cyberattack, critical national infrastructure (CI).*

9 Nataliya P. Romashkina, Ph.D. (Polit.), Corresponding Member of the Academy of Military Sciences of the Russian Federation, Head of the Informational Security Problems Group of the Primakov National Research Institute of World Economy and International Relations (IMEMO) of the Russian Academy of Sciences, Moscow, Romachkinan@yandex.ru.

References

1. Schwab K. 2015. The Fourth Industrial Revolution: What It Means and How to Respond? //Foreign Affairs. December 12, URL: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.
2. Zaretskiy A.D., Ivanova T.E. Promyshlennye tehnologii I innivatsii. 2-e izdanie. – SPb: Kubanskii gosudarstvennyi universitet, 2018.
3. Varfolomeev A.A. Kiberdiversiya I kiberterrorizm: predely vozmozhnostey negosudarstvennyh subektov na sovremennom etape // Voennaya mysl. 2012. № 12.
4. Matvienko Y.A. Informatsionno-psihologicheskaya voina kak odna iz form razresheniya sotsialno-politicheskih protivorechii v sovremennom obschestve [Information-Psychological War as One of Forms of Sociopolitical Contradiction Resolution in the Modern Society] // Informatsionnye voiny. 2015. №4.
5. Information Security Threats during Crisis and Conflicts of the XXI Century. Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO. 2016. URL: https://www.imemo.ru/files/File/en/publ/2016/2016_001.pdf.
6. U.S. Cyberattacks Target ISIS in a New Line of Combat // The New York Times. April 24, 2016 // https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.
7. Problemy informatsionnoy bezopasnosti v mezhdunarodnyh voenno-politicheskih otnosheniyah [Informational Security Problems in Modern International Crises and Conflicts of XXI Century]. N.P. Romashkina, A.V. Zagorski, eds. Moscow, IMEMO RAN. 2016. URL: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.
8. Broad W., Markoff J., Sanger D. 2011. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. January 15. URL: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.
9. Sheremet I.A. Ugrozy tehnosphere Rossii i protivodeistvie im v sovremennyh usloviyah // Vestnik akademii voennyh nauk. 2014. № 1.
10. Sundiyev I.U., Smirnov A.A., Kostin V.N. 2015. Novoye kachestvo terroristicheskoy propagandy: mediaimperiya IGIL [New Quality of Terrorist Proraganda: ISIL Media Empire] // Informachionnye voiny. № 1.
11. Romashkina N.P. Perspektivy mezhdunarodnoi informatsinnoi bezopasnoati / Bezopasnost i control nad vooruzheniami 2017–2018. Preodolenie razbalansirovki mezhdunarodnoi stabilnosti / otv. red. A. G. Arbatov, N. I. Bubnova. – M.: IMEMO RAN; Politicheskya enshiklopediya, 2018.
12. Molander R, Riddile A., Wilson P. 1996. Strategic information warfare: a new face of war. Library of Congress Cataloging in Publication Data, RAND (Firm). URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf.
13. Nye J. S. Регулирование киберконфликтов // Project Syndicate. Aug. 8, 2017 // https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08/russian.
14. Molander R., Wilson P., Mussington D., Mesic R. 1998. Strategic information warfare rising war. Library of Congress Cataloging in Publication Data, RAND (Firm). URL: https://www.rand.org/pubs/monograph_reports/MR964.html.
15. Сангалов В.А. Угрозы национальной безопасности России в информационной сфере // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – Тамбов: Издательство «Грамота». 2015. № 8-3 (58) // http://www.gramota.net/materials/3/2015/8-3/44.html.
16. Sherman F. 1990. Aborting Unauthorized Launches of Nuclear-Armed Ballistic Missiles through Postlaunch Destruction // Science and Global Security, 1990. Volume 2, No. 1.