
**ВОЗМОЖЕН ЛИ РЕЖИМ КОНТРОЛЯ
ЗА РАСПРОСТРАНЕНИЕМ КИБЕРВООРУЖЕНИЙ?
ПОДХОДЫ РОССИИ И США**

Сергей Себекин*

Иркутский государственный университет

ORCID: 0000-0002-1975-8052

© С. Себекин, 2021 г.

DOI: 10.20542/2307-1494-2021-2-139-152

Аннотация В статье оценивается осуществимость контроля за распространением кибервооружений по аналогии с контролем за распространением оружия массового уничтожения. Исследуются и сравниваются позиции России и США по данному вопросу. Если российская позиция долгое время основывалась на тезисе о важности создания режима контроля за распространением кибервооружений, то США отрицают возможность и полезность такого подхода. В статье делается попытка доказать, что контроль за распространением кибервооружений и создание соответствующего особого международного режима (по аналогии с режимами нераспространения оружия массового уничтожения и конвенциональных вооружений) пока невозможны из-за целого комплекса как технических, так и чисто политических причин. Среди них широкая доступность кибероружия, эффект масштабируемости, проблемы с верификацией наличия кибероружия и т. д. В связи с этим предлагается создание особого режима контроля за неприменением кибероружия, который мог бы включать в себя запрет на кибератаки в отношении определенных целей, установление «красных линий», создание единой базы данных уязвимостей и вредоносных программ и т. п.

Ключевые слова кибероружие, нераспространение, Россия, США, оружие массового уничтожения

Title **Is the regime of control over proliferation of cyber weapons feasible? The Russian and U.S. approaches**

Abstract The article assesses the feasibility of control over proliferation of cyber weapons, by analogy with the control over proliferation of weapons of mass destruction. The Russian and U.S. approaches to this issue are considered and compared. While Russia's stance for a long time proceeded from the idea that the regime of control over proliferation of cyber weapons is needed, the United States have denied the feasibility and validity of this approach. The author argues that, at present, the

* Себекин Сергей Александрович – преподаватель кафедры политологии, истории и регионоведения Иркутского государственного университета, кандидат исторических наук.

Sergei Sebekin is a Lecturer at the Department of Political Sciences, History, and Area Studies, Irkutsk State University, Irkutsk, Russia.

control over proliferation of cyber weapons and the establishment of a special international regime (by analogy with weapons of mass destruction and conventional weapons non-proliferation regimes) is hardly feasible for a number of both technical and political reasons. They include the wide availability of cyber weapons, the scalability effect, and difficulties in identifying cyber weapons. Instead, a special regime of control over the non-use of cyber weapons is proposed. This regime could include, among other things, a ban on cyber attacks against certain targets, introduction of “red lines”, and creation of a unified database of vulnerabilities and malware.

Keywords cyber weapons, non-proliferation, Russia, United States, weapon of mass destruction

I. Характеристика проблемы

Вопросы контроля над вооружениями и сохранения системы стратегической стабильности в последнее время стоят особенно остро. Острота этих проблем определяется, прежде всего, взаимоотношениями между двумя ключевыми игроками на мировой арене – Россией и Соединенными Штатами, – а также тем, что именно вокруг этих взаимоотношений долгое время складывалась система контроля над вооружениями. Кризис данной системы был спровоцирован инициированным администрацией Дональда Трампа выходом США из ключевых инициатив, составлявших основу системы контроля за вооружениями, – Совместного всеобъемлющего плана действий (СВПД) по иранской ядерной программе, Договора о ликвидации ракет средней и меньшей дальности (ДРСМД) и Договора по открытому небу.¹ Однако градус напряженности в этой сфере частично удалось снизить с приходом в Белый Дом нового президента США Джо Байдена, который является последовательным сторонником сохранения режима контроля над вооружениями. Так, 26 января 2021 г. между В.В.Путиным и Дж.Байденом было достигнуто соглашение о продлении Договора между Россией и США о мерах по дальнейшему сокращению и ограничению стратегических наступательных вооружений (СНВ–III).² Дж.Байден также намерен вновь присоединить свою страну к Всеобъемлющему плану действий по иранской ядерной программе.³

Прежний градус напряженности, однако, сохраняется при обсуждении вопросов киберповестки. Несмотря на то, что во время российско-американского саммита в Женеве 16 июня 2021 г. Владимиру Путину и Джо Байдену удалось договориться начать двусторонние консультации по киберповестке и что на сегодняшний день Россия и США провели уже несколько раундов консультаций по кибербезопасности,⁴ пока еще рано говорить об устойчивом взаимопонимании в этой сфере. Так, еще во время упомянутого саммита Дж.Байден заявил, что если кибератаки со стороны России продолжатся, то ей придется нести за них ответственность, а у США есть существенный киберпотенциал, который может быть в этом случае задействован.⁵ Более того, 21 июня 2021 г. официальный представитель Белого дома Джен Псаки заявила, что США не собираются предварительно обозначать возможные ответные действия.⁶ Это значит, что в случае очередных подозрений США оставляют за собой право предпринимать меры, не ставя Россию в известность о них.⁷

Как бы там ни было, гонка кибервооружений пока продолжает набирать обороты. В этой связи на повестке стоит вопрос о возможности распространения

на сферу кибероружия опыта соглашений по контролю за распространением вооружений, а также о целесообразности создания глобальной системы контроля над кибервооружениями. Данный вопрос имеет смысл обсуждать именно в контексте российско-американских взаимоотношений, поскольку режим контроля над традиционными вооружениями традиционно складывался именно вокруг отношений между этими двумя ключевыми игроками. Если удастся наладить диалог с Соединенными Штатами по киберповестке, то появится возможность обсуждать вопросы кибербезопасности, включая нераспространение кибервооружений, в общем контексте стратегической стабильности. Если это не удастся сделать, то гонка кибервооружений лишь усилится, а проблема и вопрос о возможности контроля над ними лишь еще сильнее обострится.

II. Кибероружие или информационное оружие?

Кибероружие представляет собой программно-аппаратное обеспечение или прошивки микросхем, разработанные или применяемые для нанесения ущерба в киберсфере (посредством кибератак) любым цифровым устройствам, компьютерным системам, сетям, сайтам, а также любым связанным с ними оборудованием и объектам.

Таким образом, термин «кибер-» обозначает технологические аспекты вредоносного воздействия. При этом в российском дискурсе употребляется такое понятие, как «информационное оружие», охватывающее как информационно-технологические аспекты воздействия на информационно-коммуникационную инфраструктуру, так и информационно-психологические аспекты – психологическое воздействие на людей посредством манипуляций с информацией (путем ее искажения, введения в заблуждение граждан и военных, пропаганды, дезинформации и т. д.). В данном случае следует иметь в виду два момента. Первый заключается в том, что информационно-психологическое воздействие, в отличие от кибероружия (например, вируса “Stuxnet”, физически уничтожившего иранские ядерные центрифуги в 2007 г.), не наносит прямого физического ущерба и потому не может считаться полноценным оружием.⁸ Во-вторых, в международных дискуссиях о возможности создания режима нераспространения не ставится вопрос о контроле за распространением взглядов, идей и какой-либо информации.

С учетом этих оговорок, интерпретация термина «кибероружие» в данной статье не включает рассмотрение информационно-психологических средств воздействия. Кроме того, при обращении к тем официальным документам, в которых употребляется термин «информационное оружие», основное внимание уделяется чисто технической стороне вопроса – инструментам воздействия на программно-аппаратное обеспечение посредством кибератак, включая вирусы, червей, логические бомбы, зловредные утилиты, программные закладки и т. п.

III. Подходы России и США к проблеме контроля над кибероружием

Россия и США придерживаются полярных позиций по вопросу о необходимости и возможности контроля над кибервооружениями.

Российская позиция долгое время основывалась на тезисе о важности создания режима контроля за распространением кибервооружений.⁹ Еще в сентябре 2020 г. министр иностранных дел РФ С.В.Лавров упомянул в числе российских внешнеполитических приоритетов «создание условий для

установления международного правового режима нераспространения информационного оружия».¹⁰ Впервые российская официальная позиция по этому вопросу получила отражение в «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утвержденных указом Президента РФ еще в 2013 г. Согласно этому документу, одним из приоритетных направлений политики РФ по обеспечению международной информационной безопасности было «создание условий для установления международного правового режима нераспространения информационного оружия».¹¹ Однако в новой редакции «Основ государственной политики Российской Федерации в области международной информационной безопасности», утвержденных указом Президента РФ № 213 от 12 апреля 2021 г., данная формулировка уже отсутствует.¹²

Российские эксперты придерживаются различных взглядов на эту проблему.¹³ Некоторые из них считают перспективной идею создания режима нераспространения кибероружия по аналогии с режимом контроля за распространением оружия массового уничтожения (ОМУ).¹⁴ Однако ряд российских экспертов (среди которых А.Г.Арбатов и П.А.Шариков) отрицают возможность осуществления контроля за кибервооружениями по аналогии с уже имеющимися соглашениями в других сферах.¹⁵

Позиция США заключается в том, что создание режима контроля над кибервооружениями по аналогии с режимами контроля над ОМУ не только бесполезно, но и попросту невозможно. Главная причина Вашингтону видится в непоследовательности России и в том, что РФ отрицает автоматическую применимость существующих международных правовых норм к киберпространству. В частности, как заявила заместитель координатора Управления по кибервопросам при Государственном департаменте США Мишель Маркофф, «если некоторые государства отказываются прямо подтвердить, что основные элементы существующего международного права применимы к киберпространству и не желают соблюдать уже согласованные добровольные нормы, то что нам даст попытка выработать новый договор?». ¹⁶ Маркофф также утверждала, что на кибертехнологии невозможно воздействовать при помощи традиционных договоренностей в сфере контроля над вооружениями и что «на выработку нового юридически обязывающего договора ушло бы десять или более лет, что стало бы бесполезной тратой времени и отвлечением ресурсов».¹⁷

Так или иначе, по мнению американских экспертов, «Соединенные Штаты давно отвергают попытки навязать традиционные меры контроля над вооружениями наступательным киберпотенциалам» и всячески «сопротивляются искушению участвовать в “донкихотских усилиях” по контролю над вооружениями в киберпространстве».¹⁸ Об этом же говорится и в «Отчете комиссии по киберпространству» Конгресса США, в котором утверждается, что даже «традиционные методы контроля над вооружениями трудно согласовать, не говоря уже об их применимости к кибероружию».¹⁹

IV. Почему невозможен режим контроля за распространением кибероружия?

На сегодняшний день контроль за распространением кибервооружений и создание особого международного режима по аналогии с режимом нераспространения оружия массового поражения и конвенциональных вооружений

представляются невозможными в силу целого комплекса как технических, так и чисто политических причин.

Среди технических причин можно выделить следующие.

Во-первых, это доступность кибероружия. В отличие от ядерного оружия, получению которого препятствуют мощные научно-технологические и финансовые барьеры, в случае с кибероружием аналогичные барьеры отсутствуют.²⁰ Кибероружие относительно дешево и может быть создано собственными силами с гораздо меньшими затратами времени и усилий.²¹ Ядерным оружием достоверно обладает лишь небольшой круг субъектов, и поэтому осуществлять контроль за его распространением относительно легко. Кибероружие же может заполучить почти любой актор, включая геополитически слабые государства, «государства-изгои» и широкий спектр негосударственных игроков от киберпреступников до террористов.²²

Во-вторых, кибероружие можно скрытно использовать, быстро уничтожить и столь же быстро восстановить.²³ Если наличие и распространение ОМУ и конвенционального оружия можно определить и отслеживать с помощью верификационных механизмов, разведки, радиолокации и спутникового наблюдения, то создание и распространение кода, битов и байтов в трансграничном киберпространстве контролировать практически невозможно.²⁴ Трудно не заметить запуск ядерной боеголовки или обычной ракеты, передвижение регулярных войск и частей, взлет истребителей и т. д. Кибератаки же по своей природе носят мгновенный характер, не поддаются предварительному прогнозированию, недоступны для прямого наблюдения и в ряде случаев обнаруживаются лишь спустя месяцы после осуществления.

В-третьих, кибероружие обладает эффектом масштабируемости, в соответствии с которым применение одного и того же оружия может иметь совершенно разные по масштабу эффекты и последствия.²⁵ Таким образом, в отличие от ОМУ и конвенционального оружия, кибероружие невозможно ранжировать иерархически, что делает трудным разработку какой-либо классификации кибервооружений, а значит и осуществление контроля за их распространением.

В-четвертых, темпы развития кибероружия и эволюции киберугроз очень высоки.²⁶ В такой наукоемкой сфере, как разработка и совершенствование ядерного оружия, внедрение инноваций требует больших затрат времени (не говоря уже о средствах), что дает государствам время на корректировку соглашений о контроле над вооружениями и выработку каких-либо технических инструментов проверки наличия ядерного оружия. В отличие от этого, производство и совершенствование кибероружия занимают значительно меньше времени,²⁷ поэтому адаптировать любую международную систему контроля к столь динамичным изменениям будет крайне трудно.

В-пятых, в сфере контроля над соответствующими технологиями двойного назначения также существуют значительные трудности. Всем известно о существовании как «мирного», так и «военного» атома. При этом на сегодняшний день разработаны механизмы верификации (система гарантий МАГАТЭ и направление на места инспекторов для осуществления контроля за «мирными» ядерными установками) с целью контроля за тем, чтобы обладающая ядерной промышленностью страна не использовала мирный атом в военных целях. В сфере же кибертехнологий провести границу между «мирными» и «военными» технологиями гораздо сложнее. Те или иные, зачастую транснациональные, акторы

имеют возможность вести как оборонительные, так и наступательные кибероперации с использованием одних и тех же инструментов.

Наконец, трудно идентифицировать и конкретные политические механизмы верификации нераспространения кибероружия. В отличие от ядерного и конвенционального оружия, для контроля над которыми существуют вполне четкие и эффективные механизмы верификации (в частности, в рамках гарантий МАГАТЭ), определить аналогичные механизмы для кибервооружений гораздо сложнее.

Теоретически можно выделить два пути достижения этой цели. Первый путь заключается в том, что при создании режима контроля за распространением кибервооружений государства-участники предполагаемого соглашения должны на добровольной основе предоставлять доступ к национальным сетям и системам для проверки наличия потенциально опасного кода. Какое правительство согласится на такой шаг? Где гарантия того, что при проведении проверки в государственные системы не будут внедрены «бэкдор»²⁸ или логическая бомба?²⁹ Не воспользуются ли партнеры механизмами проверок для анализа государственных систем на предмет наличия уязвимостей, чтобы в последующем иметь подробную карту слабых мест систем и сетей?

Предоставление доступа к национальным сетям и системам немыслимо с точки зрения национальной безопасности и сохранения государственного суверенитета. Именно по этой причине Россия еще в 2001 г. отказалась ратифицировать Будапештскую Конвенцию Совета Европы о киберпреступности. Согласно статье 32 данной конвенции, «любая из Сторон имеет право, без согласия другой Стороны... посредством компьютерной системы на своей территории получать доступ к компьютерным данным, расположенным на территории другой Стороны, при получении правомерного и добровольного согласия со стороны лица, обладающего законным правом на предоставление данных этой Стороне посредством вышеупомянутой компьютерной системы».³⁰ Другими словами, Россия отказалась ратифицировать конвенцию именно потому, что она создает предлог для неконтролируемого доступа в ее сети и получения критически важной информации. Подобного рода соглашения скорее способны подорвать стабильность, нежели укрепить ее.

Второй путь контроля за распространением кибероружия заключается в кибершпионаже, который с точки зрения международного права является вполне приемлемым. Проблема заключается в тех масштабах, которых должен достигнуть такого рода шпионаж. В случае с ядерным оружием следует иметь в виду, что им обладает очень ограниченное количество государств, тогда как кибероружие доступно очень широкому кругу акторов в силу очень низкой стоимости его создания или приобретения.

Помимо указанных соображений, оба упомянутых способа контроля за распространением кибероружия неэффективны из-за огромных затрат при проблематичности достигаемых результатов. Кибероружие может храниться на изолированном от сети устройстве (или даже на флеш-накопителе) или быть создано в кратчайшие сроки после окончания масштабного мониторинга.

Туманными представляются и возможности доказать наличие кибероружия у какой-либо стороны. На сегодняшний день отсутствуют общепризнанные механизмы сбора и предоставления международному сообществу исчерпывающей доказательной базы. Отсутствуют и прецеденты обращений в Международный суд ООН для разрешения разногласий по киберповестке: этого не стали делать, например, США, постоянно обвиняющие Россию в систематических кибератаках и

вмешательстве в демократический процесс. Вероятно, Соединенные Штаты попросту не хотят раскрывать свои методы проведения расследований в киберсфере. Вопрос о создании специализированного международного кибертрибунала также не поднимался. В отдельных случаях установление виновных с их последующим разоблачением и предоставлением исчерпывающей доказательной базы возможно и в этой сфере. Однако установление виновных на международном уровне, когда государственным органам, которые ведут расследование, необходимо раскрыть методику сбора информации и предоставить доказательную базу на всеобщее обозрение, представляется гораздо более проблематичным.

В целом, режим контроля за распространением кибероружия не может поддерживаться лишь односторонними обвинениями в адрес какой-либо страны – он требует официального международно-правового подтверждения с целью наложения соразмерных санкций против нарушителя. Пока подобных прецедентов не было, и вряд ли они появятся в ближайшем будущем.

Позиции влиятельных государств относительно применимости международного права к киберконфликтам серьезно различаются. Так, Москва настаивает на необходимости адаптировать существующую международно-правовую базу к специфике киберпространства, в то время как Вашингтон утверждает, что уже существующее международное право полностью применимо к киберконфликтам, ссылаясь на статью 51 Устава ООН и статью 5 Вашингтонского договора (о коллективном реагировании на агрессию в отношении государства-члена НАТО). Россия и США также придерживаются разных позиций относительно использования информационно-коммуникационных технологий (ИКТ) в военных целях, распространения национального суверенитета на ИКТ-инфраструктуру и необходимости регулирования интернета на национальном уровне.

Проблему осложняют и терминологические разногласия. Так, США неоднократно обвиняли Россию в том, что, употребляя термин «информационный» и стремясь осуществлять контроль над «информационным вооружением», РФ прежде всего хочет не допустить распространения у себя политически неуютной информации и идей. США считают, что обсуждение подобных вопросов на международном уровне неуместно. В частности, об этом в резкой форме говорится в докладе Госдепартамента США «О международной безопасности в киберпространстве: модели для снижения рисков».³¹

Следует также учитывать, что создание режима контроля за распространением ядерного оружия стало возможно благодаря разрушительной силе последнего. Именно страх перед ядерной войной и взаимным уничтожением подтолкнул СССР и США к разработке и заключению серии соглашений о контроле над ядерными вооружениями. Кибероружие на данный момент не обладает столь мощной разрушительной силой, и пока накоплено слишком мало эмпирического опыта для того чтобы прогнозировать эффекты и последствия от его применения.

Так или иначе, на данный момент никто не в состоянии адекватно измерить реальный киберпотенциал того или иного государства, что крайне осложняет согласование и реализацию любых договоров по нераспространению кибероружия. К тому же в современных условиях никакое государство не откажется от такого заманчивого и доступного инструмента. Кибероружие особенно привлекательно для развивающихся государств, не имеющих значительного военного потенциала и потому заинтересованных в наличии асимметричных ресурсов для противостояния более сильным противникам.

V. Возможные пути решения проблемы

Итак, адекватно измерить реальный киберпотенциал государства пока невозможно, что лишает соглашения по контролю за распространением кибервооружений смысла. Речь может идти о создании не режима контроля за распространением кибероружия, а режима неприменения такого оружия.

В частности, имеются определенные возможности снизить стимулы для неизбирательного и разрушительного применения кибероружия. Речь может идти о запрете на осуществление кибератак против определенных объектов критической инфраструктуры.³² К таким объектам могут быть отнесены системы командования и контроля за ядерным оружием, объекты сферы здравоохранения, ядерной промышленности, космической инфраструктуры (будь то спутники или наземная космическая инфраструктура) и любые другие объекты, нарушение в работе которых может привести к угрозе жизни и здоровью людей, экологической катастрофе и т. д.

Запреты могут быть наложены и на такие кибератаки, которые имеют масштабные разрушительные последствия. Особо разрушительные кибератаки могут быть квалифицированы в качестве актов агрессии. Под эгидой ООН или в каком-либо другом формате государства могли бы взять на себя взаимные обязательства не осуществлять такие кибератаки, эффект от которых будет достигать уровня вооруженного конфликта. Отдельным государствам целесообразно провести свои «красные линии» – установить пороги допустимых эффектов и последствий кибервторжения, превышение которых повлечет за собой ответственность.

В данном случае снова возникает проблема установления ответственности, что ставит вопрос о создании в перспективе специального международного органа по расследованию киберинцидентов. Такой орган может быть сформирован под эгидой ООН с участием всех заинтересованных сторон. Важно, чтобы в рамках этого органа государства выработали общепризнанную методологию расследования кибератак, что потребует полноценного обмена опытом анализа подобных инцидентов.

Одним из возможных вариантов является создание единой глобальной базы раскрытия известных уязвимостей нулевого дня в программно-аппаратном обеспечении,³³ а также когда-либо применявшихся вредоносных программ.³⁴ Такая база должна пополняться в режиме реального времени. Своевременное реагирование, устранение «слабых мест» и создание систем защиты против известных видов оружия, а также сам факт открытости этой базы могут существенно снизить эффективность значительной части кибервооружений, нацеленных на те или иные системы и эксплуатирующих определенные уязвимости.

Оптимальным вариантом было бы добровольное согласие стран-участников на раскрытие имеющихся у них возможностей в данной сфере, что повысило бы общий уровень доверия. Так или иначе, необходимо предпринимать усилия для установления приемлемых правил поведения в киберпространстве и укрепления доверия в этой сфере.

Таким образом, России следует отказаться от идеи принятия каких-либо формальных и юридически обязывающих соглашений и установления официального правового режима контроля за распространением кибероружия по аналогии с режимом нераспространения ОМУ. В этой связи, исключение из новой редакции «Основ государственной политики Российской Федерации в области

международной информационной безопасности» от 12 апреля 2021 г. прежней формулировки «создание условий для установления международного правового режима нераспространения информационного оружия» может интерпретироваться как отход от идеи контроля над кибервооружениями. Представляется, что российским интересам в большей степени отвечало бы создание режима контроля за неприменением кибероружия.

ПРИМЕЧАНИЯ

¹ Подробней о Договоре по открытому небу см. Sokov N. The U.S. withdrawal from the Open Skies Treaty // Pathways to Peace and Security. 2021. № 1(60). С. 133–150.

² Рощепий И. Россия и США договорились продлить СНВ-3 // Парламентская газета. 26 января 2021.

³ Wintour P. Hopes rise of breakthrough on US return to Iran nuclear deal // The Guardian. 1 April 2021.

⁴ Черненко Е.В. Рябков: Россия и США провели уже четыре раунда консультаций по кибербезопасности // Коммерсантъ. 22 июля 2021.

⁵ Закваскин А., Комарова Е. «Отыграть ситуацию»: почему в Белом доме вновь заговорили о возможности кибератак против России // RT на русском. 19.06.2021. URL: <https://russian.rt.com/world/article/874772-baiden-putin-kiberataki> (дата обращения 25.09.2021).

⁶ Press Briefing by Press Secretary Jen Psaki. The White House. 21 June 2021. URL: <https://www.whitehouse.gov/briefing-room/press-briefings/2021/06/21/press-briefing-by-press-secretary-jen-psaki-june-21-2021> (accessed 25.09.2021).

⁷ Себекин С.А. Женевская кибероттепель: надейся на лучшее – готовься к худшему. Россия в глобальной политике: Мнения. 30 июня 2021. URL: <https://globalaffairs.ru/articles/zhenevskaya-kiberottepel> (дата обращения 25.09.2021).

⁸ Дылевский И.Н., Запивахин В.О., Комов С.А., Коротков С.В., Петрунин А.Н. Международный режим нераспространения информационного оружия: утопия или реальность? // Военная мысль. 2014. № 10. С. 3–4.

⁹ Markoff J., Kramer A.E. U.S. and Russia differ on a Treaty for Cyberspace // The New York Times. 27 June 2009.

¹⁰ Лавров С.В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 28.09.2020. URL: <https://eer.ru/article/gosudarstvo/u79/2020/09/28/2944> (дата обращения 05.04.2021).

¹¹ Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утверждены Президентом РФ 24 июля 2013 г. № Пр-1753. URL: <http://base.garant.ru/70641072> (дата обращения 06.04.2021).

¹² Основы государственной политики Российской Федерации в области международной информационной безопасности. Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213. URL: <http://www.scrf.gov.ru/security/information/document114> (дата обращения 09.10.2021).

¹³ VI Московская конференция по международной безопасности. Материалы конференции. 26–27 апреля 2017 г. – М.: Министерство обороны Российской Федерации. 2017. С. 93, 107. URL: <http://www.pircenter.org/media/content/files/14/15106557720.pdf> (дата обращения 05.04.2021).

-
- ¹⁴ Дылевский И.Н., Запихахин В.О., Комов С.А., Коротков С.В. и др. Ук. соч.
- ¹⁵ Arbatov A. New Era of Arms Control: Myths, Realities and Options. Carnegie Moscow Center Commentary. 24 October 2019. URL: <https://carnegie.ru/commentary/80172> (accessed 07.04.2021); Шарилов П.А. Информационное сдерживание: трансформация парадигмы стратегической стабильности. Российский совет по международным делам (РСМД): Аналитика и комментарии. 5 сентября 2013. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnoe-sderzhivanie-transformatsiya-paradigmy-strat> (дата обращения 09.10.2021).
- ¹⁶ Черненко Е.В. Борьба за мир во всем кибере // Коммерсантъ. 14 марта 2021.
- ¹⁷ Там же.
- ¹⁸ Ford C.A. International security in cyberspace: new models for reducing risk // Arms Control and International Security Papers. V. 1. № 20. 2020. P. 4–5.
- ¹⁹ U.S. Cyberspace Solarium Commission Report. March 2020. Washington D.C.: U.S. Congress, 2020. P. 18. URL: https://drive.google.com/file/d/1ryMCIL_dZ30QyJFqFkf10MxIXGT4yv/view (accessed 09.04.2021).
- ²⁰ Nye J.S. Nuclear lessons for cyber security // Strategic Studies Quarterly. 2011. V. 5. № 4. P. 20, 22, 36; Карасев П.А. США наращивают киберсилы. РСМД: аналитика и комментарии. 2 августа 2017. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/ssha-narashchivayut-kibersily> (дата обращения 21.09.2021).
- ²¹ Бартош А.А. Защита от неизвестного супостата // Независимое военное обозрение. 8 июля 2021; Демидов О.В., Черненко Е.В. Грозный ум на страже кибербезопасности // Индекс безопасности. 2014. Т. 20. № 3 (110). С. 157; Карасев П.А. Ук. соч.; Рождественская Я. Гонка кибервооружений ускоряется // Коммерсантъ. 12 октября 2015; Никитович Н. Стратегия и тактика кибервойн: в ожидании серьезных межгосударственных конфликтов // Information Security. 2013. № 5. URL: <https://lib.itsec.ru/articles2/cyberwar/strategiya-i-taktika-kibervoyun-v-ozhidanii-sereznyh-mezhgosudarstvennyh-konfliktov> (дата обращения 22.09.2021); Черненко Е.В. «Мы пока не так уязвимы, как американцы, но быстро их догоняем» // Коммерсантъ. 25 апреля 2011; Smeets M. How much does a cyber weapon cost? Nobody knows // Net Politics Program Blog Post. Council on Foreign Relations web-site. 21.11.2016. URL: <https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows> (accessed 22.09.2021).
- ²² Boulanin V. Arms Production Goes Cyber: A Challenge for Arms Control. Stockholm International Peace Research Institute (SIPRI) Commentary. 30 May 2013. URL: <https://www.sipri.org/node/361> (accessed 18.09.2021); Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch. The Brookings Institution Conference Proceedings. – Washington D.C.: The Brookings Institution, 2011. P. 19. URL: https://www.brookings.edu/wp-content/uploads/2012/04/20110920_cyber_defense.pdf (accessed: 09.09.2021); Geers K. The challenge of cyber attack deterrence // Computer Law & Security Review. 2020. № 26. P. 299; Карасев П.А. Ук. соч.
- ²³ Nye J.S. Deterrence and dissuasion in cyberspace // International Security. Winter 2016/2017. V. 41. № 34. P. 61.; Borghard E.D., Loneragan S.W. Why are there no cyber arms control agreements? // Net Politics Program Blog Post. Council on Foreign Relations web-site. 16.01.2018. URL: <https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements> (accessed 20.09.2021).
- ²⁴ Deterrence in Cyberspace. P. 19; Шарилов П.А. Ук. соч.
- ²⁵ Blank S. Can information warfare be deterred? // Information Age Anthology. V. III: The Information Age Military. Eds. D.S.Alberts and D.S.Papp. – Washington D.C.: Command and Control Research Program, 2001. P. 139; Goodman W. Cyber deterrence: tougher in theory than in practice? // Strategic Studies Quarterly. 2010. V. 4. № 3. P. 116, 128; Nye J.S. Nuclear lessons for cyber security. P. 20; Sterner E. Retaliatory deterrence in cyberspace // Strategic Studies Quarterly. 2011. V. 5. № 1. P. 73.

²⁶ Boulanin V. Op. cit.

²⁷ Borghard E.D., Lonergan S.W. Op. cit.

²⁸ “Backdoor” («черный ход») – дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

²⁹ «Логическая бомба» – вредоносное программное обеспечение, которое активируется ответом на какое-либо событие, например, на запуск пользователем того или иного приложения, посещение целевого веб-сайта, или наступлением определенной даты (и времени).

³⁰ Конвенция о преступности в сфере компьютерной информации ETS № 185. Будапешт, 23 ноября 2001 г. Статья 32. Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным. URL: <http://base.garant.ru/4089723/b3975f01ce8b0eb0c9b11526d9b4c7bf> (дата обращения 10.04.2021).

³¹ Ford C.A. Op. cit. P. 4–5.

³² Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. – М.: ИМЭМО РАН, 2020. С. 91; VI Московская конференция по международной безопасности. С. 93; Толстухина А. Ракета в ответ на кибератаку? // Международная жизнь. 30.01.2017. URL: <https://interaffairs.ru/news/show/16811> (дата обращения: 13.09.2021); Шариков П.А. Информационные угрозы и контроль над вооружениями: возможен ли диалог между Россией и США? Международный дискуссионный клуб «Валдай»: Мнения экспертов. 20 ноября 2020. URL: <https://ru.valdaiclub.com/a/highlights/informatsionnye-ugrozy-i-kontrol-nad-vooruzheniyami> (дата обращения 12.04.2021); Nye J.S. Deterrence and dissuasion in cyberspace. P. 61; Nye J.S. The world needs an arms control treaty for cybersecurity // The Washington Post. 1 October 2015; Futter A. What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk. European Leadership Network (ELN) Global Security Brief. June 2020. – London: ELN, 2020. P. 5, 7. URL: <https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/06/Cyber-arms-control.pdf> (accessed 13.04.2021); Ford C.A. The trouble with cyber arms control // The New Atlantis. 2010. № 29. P. 52–67; Giles M. We need a cyber arms control treaty to keep hospitals and power grids safe from hackers // MIT Technology Review. 01.10.2018. URL: <https://www.technologyreview.com/2018/10/01/139955/we-need-a-cyber-arms-control-treaty-to-keep-hospitals-and-power-grids-safe-from-hackers> (accessed 13.04.2021).

³³ Уязвимость нулевого дня – программная уязвимость, обнаруженная злоумышленниками до того, как о ней узнали производители компьютерной программы.

³⁴ Nye J.S. The world needs an arms control treaty for cybersecurity.

БИБЛИОГРАФИЯ

- Бартош А.А. Защита от неизвестного супостата // Независимое военное обозрение. 8 июля 2021.
- Демидов О.В., Черненко Е.В. Грозный ум на страже кибербезопасности // Индекс безопасности. 2014. Т. 20. № 3 (110). С. 153–158. URL: <http://www.pircenter.org/media/content/files/12/14116651340.pdf> (дата обращения 21.09.2021).
- Дылевский И.Н., Запихахин В.О., Комов С.А., Коротков С.В., Петрунин А.Н. Международный режим нераспространения информационного оружия: утопия или реальность? // Военная мысль. 2014. № 10. С. 3–12.
- Карасев П.А. США наращивают киберсилы. Российский совет по международным делам: аналитика и комментарии. 2 августа 2017. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/ssha-narashchivayut-kibersily> (дата обращения 21.09.2021).

-
- Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. – М.: ИМЭМО РАН, 2020. 98 с.
- Себекин С.А. Женевская кибероттепель: надейся на лучшее – готовься к худшему // Россия в глобальной политике: Мнения. 30 июня 2021. URL: <https://globalaffairs.ru/articles/zhenevskaya-kiberottepel> (дата обращения 25.09.2021).
- Толстухина А. Ракета в ответ на кибератаку? // Международная жизнь. 30.01.2017. URL: <https://interaffairs.ru/news/show/16811> (дата обращения: 13.09.2021).
- Шариков П.А. Информационное сдерживание: трансформация парадигмы стратегической стабильности // Российский совет по международным делам (РСМД): Аналитика и комментарии. 5 сентября 2013. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnoe-sderzhivanie-transformatsiya-paradigmy-strat> (дата обращения 07.04.2021).
- Шариков П.А. Информационные угрозы и контроль над вооружениями: возможен ли диалог между Россией и США? Международный дискуссионный клуб «Валдай»: Мнения экспертов. 20 ноября 2020. URL: <https://ru.valdaiclub.com/a/highlights/informatsionnye-ugrozy-i-kontrol-nad-vooruzheniyami> (дата обращения 12.04.2021).
- VI Московская конференция по международной безопасности. Материалы конференции. 26–27 апреля 2017. – М: Министерство обороны Российской Федерации. 2017. 178 с. URL: <http://www.pircenter.org/media/content/files/14/15106557720.pdf> (дата обращения 05.04.2021).
- Arbatov A. New Era of Arms Control: Myths, Realities and Options. Carnegie Moscow Center Commentary. 24 October 2019. URL: <https://carnegie.ru/commentary/80172> (accessed 07.04.2021).
- Blank S. Can information warfare be deterred? // Information Age Anthology. V. III: The Information Age Military. Eds. D.S.Alberts and D.S.Papp. – Washington D.C.: Command and Control Research Program, 2001. P. 125–157.
- Boulanin V. Arms Production Goes Cyber: A Challenge for Arms Control. Stockholm International Peace Research Institute (SIPRI) Commentary. 30 May 2013. URL: <https://www.sipri.org/node/361> (accessed 18.09.2021).
- Ford C.A. International Security in Cyberspace: New Models for Reducing Risk. Arms Control and International Security Papers. V. 1. № 20. 2020. 8 p. URL: <https://www.state.gov/wp-content/uploads/2020/10/T-paper-series-Cybersecurity-Format-508.pdf> (accessed 09.04.2021).
- Ford C.A. The trouble with cyber arms control // The New Atlantis. 2010. № 29. P. 52–67.
- Futter A. What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk. European Leadership Network (ELN) Global Security Brief. June 2020. – London: ELN, 2020. 10 p. URL: <https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/06/Cyber-arms-control.pdf> (accessed 13.04.2021).
- Geers K. The challenge of cyber attack deterrence // Computer Law & Security Review. 2010. № 26. P. 298–303. DOI: 10.1016/j.clsr.2010.03.003.
- Goodman W. Cyber deterrence: tougher in theory than in practice? // Strategic Studies Quarterly. 2010. V. 4. № 3. P. 102–135.
- Nye J.S. Deterrence and dissuasion in cyberspace // International Security. Winter 2016/2017. V. 41. № 34. P. 44–71. DOI: 10.1162/ISEC_a_00266.
- Nye J.S. Nuclear lessons for cyber security // Strategic Studies Quarterly. 2011. V. 5. № 4. P. 18–38.
- Sokov N. The U.S. withdrawal from the Open Skies Treaty // Pathways to Peace and Security. 2021. № 1(60). P. 133–150. DOI: 10.20542/2307-1494-2021-1-133-150
- Stern E. Retaliatory deterrence in cyberspace // Strategic Studies Quarterly. V. 5. № 1. 2011. P. 62–80.
- U.S. Cyberspace Solarium Commission Report. March 2020. Washington D.C.: U.S. Congress, 2020. 182 p. URL: https://drive.google.com/file/d/1ryMCIL_dZ30QyJFqFkkf10MxIXJGT4yv/view (accessed 09.04.2021).

BIBLIOGRAPHY

- Arbatov A. (2019). *New Era of Arms Control: Myths, Realities and Options*. Carnegie Moscow Center Commentary. 24 October. URL: <https://carnegie.ru/commentary/80172> (accessed 09.04.2021).
- Bartosh A.A. (2021). Zashchita ot neizvestnogo supostata [Protection from an unknown adversary]. *Nezavisimoe voennoe obozrenie*. July 8.
- Blank S. (2001). Can information warfare be deterred? In: *Information Age Anthology. Volume III: The Information Age Military*. Eds. D.S.Alberts and D.S.Papp. Washington: Command and Control Research Program. P. 125–157.
- Boulanin V. (2013). *Arms Production Goes Cyber: A Challenge for Arms Control*. Stockholm International Peace Research Institute (SIPRI) Commentary. 30 May. URL: <https://www.sipri.org/node/361> (accessed: 18.09.2021).
- Demidov O.V., Chernenko E.V. (2014). Groznyi um na strazhe kiberbezopasnosti [A formidable mind on guard for cybersecurity]. *Indeks bezopasnosti*. V. 20. No. 3 (110). P. 153–158. URL: <http://www.pircenter.org/media/content/files/12/14116651340.pdf> (accessed 21.09.2021).
- Dylevskij I.N., Zapivakhin V.O., Komov S.A., Korotkov S.V., and Petrunin A.N. (2014). Mezhdunarodnyi rezhim nerasprostraneniya informatsionnogo oruzhiya: utopiya ili real'nost'? [International regime for non-proliferation of information weapons: utopia or reality?]. *Voennaya mysl'*. [Military Thought]. No. 10. P. 3–12.
- Ford C.A. (2020). *International Security in Cyberspace: New Models for Reducing Risk*. Arms Control and International Security Papers. V. 1. No. 20. 8 p. URL: <https://www.state.gov/wp-content/uploads/2020/10/T-paper-series-Cybersecurity-Format-508.pdf> (accessed 09.04.2021).
- Ford C.A. (2010). The trouble with cyber arms control. *The New Atlantis*. No. 29. P. 52–67.
- Futter A. (2020). *What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk*. European Leadership Network (ELN) Global Security Brief. June. London: ELN. 10 p. URL: <https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/06/Cyber-arms-control.pdf> (accessed 13.04.2021).
- Geers K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*. No. 26. P. 298–303. DOI: 10.1016/j.clsr.2010.03.003.
- Goodman W. (2010). Cyber Deterrence. Tougher in theory than in practice? *Strategic Studies Quarterly*. V. 4. No. 3. P. 102–135.
- Karasev P.A. (2017). *SShA narashchivayut kibersily* [The U.S. is building up its cyber power]. Russian International Affairs Council: Analytics and Commentaries. August 2. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/ssha-narashchivayut-kibersily/> (accessed 21.09.2021).
- Nye J.S. (2016/2017). Deterrence and dissuasion in cyberspace. *International Security*. V. 41. No. 34. P. 44–71. DOI: 10.1162/ISEC_a_00266.
- Nye J.S. (2011). Nuclear lessons for cyber security. *Strategic Studies Quarterly*. V. 5. No. 4. P. 18–38.
- Romashkina N.P., Markov A.S., and Stefanovich D.V. (2020). Mezhdunarodnaya bezopasnost', strategicheskaya stabil'nost' i informatsionnyie tekhnologii [International security, strategic stability, and information technologies]. Moscow: Institute of World Economy and International Relations, Russian Academy of Sciences (IMEMO RAS). 98 p.
- Sebekin S.A. (2021). *Zhenevskaya kiberottepel': nadeisya na luchshee – gotov'sya k khudshemu* [Geneva cyber thaw: hope for the best – prepare for the worst]. Russia in Global Politics: Opinions. June 30. URL: <https://globalaffairs.ru/articles/zhenevskaya-kiberottepel> (accessed 25.09.2021).
- Sharikov P.A. (2013). *Informatsionnoye sderzhivaniye: transformatsiya paradigmy strategicheskoi stabil'nosti* [Information deterrence: transformation of the strategic stability paradigm]. Russian International Affairs Council: Analytics and Commentaries. September 5. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnoe-sderzhivanie-transformatsiya-paradigmy-strat> (accessed 07.04.2021).
- Sharikov P.A. (2020) *Informatsionnyie ugrozy i kontrol' nad vooruzheniyami: vozmozhen li dialog mezhdu Rossiej i SShA?* [Information threats and arms control: Is the Russia-U.S. dialogue possible?]. Valdai International Discussion Club: Expert Opinions. November 20. URL: <https://ru.valdaiclub.com/a/highlights/informatsionnye-ugrozy-i-kontrol-nad-vooruzheniyami> (accessed 12.04.2021).
- (2017). *VI Moskovskaya konferentsiya po mezhdunarodnoi bezopasnosti* [VI Moscow Conference on International Security: Conference materials]. 26–27 April. Moscow: Ministry of Defense of the

-
- Russian Federation. 178 p. URL: <http://www.pircenter.org/media/content/files/14/15106557720.pdf> (accessed 05.04.2021).
- Sokov N. (2021). The U.S. withdrawal from the Open Skies Treaty. *Pathways to Peace and Security*. No. 1 (60). P. 133–150. DOI: 10.20542/2307-1494-2021-1-133-150.
- Sterner E. (2011). Retaliatory deterrence in cyberspace. *Strategic Studies Quarterly*. V. 5. No. 1. P. 62–80.
- Tolstukhina A. (2017). Raketa v otvet na kiberataku? [A missile in response to a cyberattack?]. *Mezhdunarodnaya zhizn'* [International Affairs]. January 30. URL: <https://interaffairs.ru/news/show/16811> (accessed 13.09.2021).
- (2020). U.S. Cyberspace Solarium Commission Report. March. Washington D.C.: U.S. Congress. 182 p. URL: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (accessed 09.04.2021).