Как изучать политику безопасности в области ИКТ: возможности и ограничения критического дискурс-анализа

И. Т. Стадник

Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7–9

Для цитирования: *Стадник И. Т.* Как изучать политику безопасности в области ИКТ: возможности и ограничения критического дискурс-анализа // Вестник Санкт-Петербургского университета. Международные отношения. 2024. Т. 17. Вып. 2. С. 183–200.
https://doi.org/10.21638/spbu06.2024.205

В статье рассматривается метод критического дискурс-анализа (КДА) на примере отношений США и России в области ИКТ-безопасности, а также в контексте переговоров на уровне ООН в этой же сфере, где обе страны имеют существенное влияние на процессы. КДА можно использовать для изучения политики безопасности в области информационно-коммуникационных технологий (ИКТ), чтобы понять, как различные акторы используют язык для обсуждения проблем: какие термины и концепции используются, а также как они могут влиять на общественное восприятие проблемы. Также КДА может использоваться для изучения динамики взаимодействия между различными акторами: какие интересы они преследуют и на какие компромиссы они готовы пойти для достижения общих целей. Метод соединен с теоретической рамкой А. Хольцшайтер, которая выделяет уровни анализа (микроагенты и макроструктуры), а также типы реализации власти/влияния в дискурсе (совещательный и продуктивный). В качестве демонстрации метода автором проделан краткий анализ дискурсов ИКТ-угроз США и России на основе стратегических документов государств. Он вписан в структуры двусторонних отношений и международных переговоров, представленных в виде событий на временной шкале. В зависимости от уровня анализа или отправной точки исследования — агентов или структур — мы получаем совершенно разные объяснения причинно-следственных связей возможных объяснений изменения политики через дискурс (продуктивный или совещательный). Исследование ИКТ-безопасности усложняется еще и тем, что мы обязаны держать в фокусе и двусторонний, и международный уровень взаимодействия, так как эти процессы тесно взаимосвязаны. В заключение описываются важные ограничения метода, в том числе слабый объяснительный потенциал причин изменения политики в области ИКТ-безопасности.

Ключевые слова: критический дискурс-анализ, кибербезопасность, информационная безопасность, проблема структуры и агента, США, Россия.

Введение

Исследования политики безопасности в области информационно-коммуникационных технологий (ИКТ) как на национальном, так и на глобальном уровне в большинстве своем концентрируются либо на анализе действий государств и негосударственных акторов в киберпространстве, либо на изучении стратеги-

ческих документов и описании приоритетов стран, рисках и угрозах, исходящих из использования ИКТ, а также описании организационного и административного обеспечения кибербезопасности. Однако этот спектр исследований остается неполным, если мы будем рассматривать безопасность в области ИКТ не только с позиций традиционных теорий международных отношений, но и вооружимся конструктивистской логикой в построении методологии. Безопасность в области ИКТ как объект исследования нельзя увидеть или потрогать, поэтому знания об этой области постоянно конструируются как самими исследователями, так и теми, кто непосредственно вовлечен в процессы, связанные с политикой кибербезопасности. И здесь на первый план выходит понятие дискурса и его значение для формулирования политики безопасности.

Согласно концепции, разработанной Э. Лакло и Ш. Муфф, дискурс можно представить как способ понимания социального мира путем интерпретации и реинтерпретации значений, которые коммуникативные акторы присваивают объектам окружающего мира. При этом дискурсы постоянно находятся в динамике и конкурируют между собой за право зафиксировать определенные ими значения в языке [1, с. 26]. В конце 90-х годов прошлого века популярность получил критический дискурс-анализ (КДА), в основе которого лежит функционалистский подход, который выступает за анализ текстов как «используемого языка». Его цель состоит в том, чтобы «связать лингвистический анализ с социальным анализом» [2]. Предметом критического дискурс-анализа становятся социальные проблемы, властные отношения, а также исследования текстов, их интерпретации, восприятие и социальные последствия [3].

КДА может применяться для изучения политики безопасности в области ИКТ в нескольких направлениях. Во-первых, для того, чтобы понять, как различные акторы, включая государства и частный сектор, используют язык для обсуждения проблем ИКТ-безопасности: какие термины и концепции используются, а также как они могут влиять на общественное восприятие проблемы. Во-вторых, КДА может использоваться для изучения динамики взаимодействия между различными акторами в контексте ИКТ-безопасности. Это может помочь понять, как разные стороны взаимодействуют друг с другом, какие интересы они преследуют и на какие компромиссы они готовы пойти для достижения общих целей.

О каких же дискурсах в данном случае может идти речь? Для начала воспользуемся еще теорией секьюритизации, предложенной представителями копенгагенской школы О. Уивером и Б. Бузаном [4]. Через призму этой теории киберпространство стало референтным объектом, пройдя через этапы секьюритизации: озвучивание угроз и формулирование политики для достижения безопасности. Угрозы для/из киберпространства определяют шаги, которые необходимо предпринять в комплексе мер для защиты уязвимых слоев общества и/или поддержания национальной безопасности с учетом повсеместной цифровизации всех аспектов жизни. Восприятие угроз в киберпространстве приводит к определенному выбору политики безопасности — как внутри страны, так и на международном уровне. Для наглядности в этой статье мы будем анализировать дискурсы угроз на примере США и России. Обе страны имеют значительный опыт в формировании и реализации политики безопасности в области ИКТ на национальном уровне и на международном, являясь локомотивами переговорных процессов по глобальной кибербезопасности. При этом подходы этих стран значительно отличаются: в США, где акцент идет на защите

компьютерных сетей и содержащейся в них информации, а также критической инфраструктуры страны, распространен термин «кибербезопасность» (cyber security); в то же время в России, где фокус с сетей и инфраструктуры смещается в сторону информационных (контентных) угроз обществу и государству, используется термин «информационная безопасность». Важно подчеркнуть, что эти подходы не являются противоречащими друг другу. Понятие информационной безопасности является более широким и включает в себя составляющие кибербезопасности [5].

Цель данной статьи — выявить потенциал и ограничения КДА для изучения политики безопасности в области ИКТ. В качестве демонстрации метода автором проделан краткий анализ дискурсов ИКТ-угроз США и России на основе стратегических документов государств. Он вписан в структуры двусторонних отношений и международных переговоров, представленных в виде событий на временной шкале. Далее, отталкиваясь от общей гипотезы, автор формулирует два исследовательских вопроса для каждого уровня анализа или отправной точки исследования (агенты или структуры), чтобы выяснить возможные объяснения изменений политики через дискурс (продуктивные или совещательные).

Исследовательская проблема

Когда мы говорим об обеспечении глобальной ИКТ-безопасности, прежде всего мы подразумеваем особый международный режим, который должен быть сформирован, чтобы установить общие для всех государств рамки возможных действий в киберпространстве, а также механизмы для контроля за их соблюдением. Однако несмотря на более чем двадцатилетнюю историю дипломатических усилий на уровне ООН, договориться о правилах и создать универсальные механизмы защиты от ИКТ-угроз государствам не удалось. Важно уточнить, что речь идет о правилах, нормах и механизмах, которые могли бы иметь юридическую силу, так как некоторый прогресс в переговорах все же был достигнут и в распоряжении государств есть список норм, принципов, мер доверия и наращивания потенциала в ИКТ-сфере, закрепленный в докладах Группы правительственных экспертов (ГПЭ) и Рабочей группы открытого состава (РГОС) ООН и получивший одобрение в резолюциях ГА ООН [6]. Однако наличие такого списка норм «ответственного поведения государств в киберпространстве» и их добровольный характер не способствуют укреплению международной кибербезопасности: число атак на информационные системы и объекты гражданской и военной инфраструктуры растет с каждым годом, также происходит всплеск хакерской активности во время вооруженных конфликтов и столкновений. Ситуацию усугубляет также сложность в атрибуции совершенных кибератак той или иной стране, чтобы иметь возможность использовать ответные меры, вплоть до применения военной силы и даже ядерных вооружений, как манифестируется прямо или косвенно в стратегических документах некоторых стран, в том числе США и России [7; 8]. Однако не стоит воспринимать киберпространство как «Дикий Запад», где отсутствуют законы и есть только право сильнейшего. Существует большое количество региональных и двусторонних соглашений по сотрудничеству в области кибербезопасности, договоров о взаимной правовой помощи, контактные сети CERTов — групп, непосредственно реагирующих на инциденты и обменивающихся технической информацией о киберата-

ках [9]. Но этого, как показывает практика, оказывается недостаточно. Кибератаки продолжаются, государства обвиняют друг друга в их организации и проведении, особенно это заметно проявляется там, где отношения между государствами напряжены, а киберинциденты только снижают уровень доверия друг другу или же вообще являются причиной резкого ухудшения и прекращения полноценного диалога. Российско-американские отношения являются здесь ярким примером.

Гипотеза

Прогресс в переговорах по кибербезопасности (как на двустороннем, так и на международном уровне) будет достигнут, **как только дискурсы участников будут согласованы, так что восприятие киберугроз станет схожим.** Прогрессом в данном случае будет считаться заключение юридически значимого соглашения либо реализуемые на практике инициативы. В интересах любого государства (агента в терминах КДА) быть первым и навязать свой дискурс киберугроз, убеждая других в том, что он правильно отражает реальность. Когда ценности в обеспечении безопасности и восприятие киберугроз совпадают, легче идти на уступки и вырабатывать совместные решения для политики кибербезопасности.

Теоретическая рамка А. Хольцшайтер

Прежде чем перейти от нашей проблемы к формулированию исследовательских вопросов, стоит обратиться к проблеме, которую сформулировала А. Хольцшайтер при анализе различных исследований международной политики, где использовался КДА как один из методов исследования. «Вместо того чтобы просто исследовать использование языка в международной политике, исследование дискурса требует изучения социальных и политических эффектов, которые возникают в результате использования определенной лексики, с одной стороны, и продуктивного воздействия определенных конструкций реальности на активность и идентичность индивидов и групп» [10].

Хольцшайтер изучала, как борьба за смыслы проявляется в дипломатической практике или международных переговорах, и пришла к выводу, что исследования, использующие дискурс-анализ, можно сгруппировать и распределить вдоль шкалы, где с одной стороны отправной точкой исследования будут агенты (производящие тексты или речевые акты), а с другой — структуры (контекст, внутри которого происходит взаимодействие). Эта шкала позволяет обозначить дискурсивные подходы к исследованиям либо как преимущественно макроструктурные, либо как микроинтерактивные (см. табл. 1).

При этом, как пишет Хольцшайтер, это не означает, что подходы к дискурсу, ориентированному на агентов, пренебрегают структурами, внутри которых происходит коммуникация, или что подходы к дискурсу, ориентированному на структуры, игнорируют отдельные речевые акты агентов. Однако «самая фундаментальная дилемма заключается в желании объединить конструктивистскую онтологию, основанную на совместном конструировании смыслов и значений между агентами и структурами, с одной стороны, и позитивистскую эпистемологию, которая стремится идентифицировать причинно-следственные связи — с другой. Это затруднительное положение

Таблица 1. **Онтологические различия**

	Микроинтерактивный подход	**Макроструктурный подход**
Определение дискурса	Дискурс как текст в контексте, но акцент на дискурсе как коммуникативном обмене	Дискурс как текст в контексте, но с акцентом на исторически сложившиеся структуры значения
Преобладающий уровень анализа	Агенты/индивидуальный — «Субъекты придают смысл»	Структура/Холистичный — «Смысл создает субъектов»
Текст/Контекст	Текст: Небольшие примеры повседневной коммуникации Контекст: Институциональная среда для коммуникативного обмена	Текст: Тексты как агрегированные свидетельства больших смысловых структур Контекст: Широкий исторический или социально-политический контекст

Источник: [10].

Таблица 2. **Уровни анализа и отношения между дискурсом и властью**

	Уровень — Агент	**Уровень — Структура**
Делиберативный	Дискурс как коммуникативная рациональность — дискурс как место, где проявляется «сила лучшего аргумента».	Делиберативный дизайн международных институтов позволяет устранять асимметрию власти в глобальной политике посредством дискурса
Продуктивный	Дискурс как связь знания и власти: акторы стремятся навязать другим свой взгляд на реальность в дискурсе	Дискурсы как институционализированные смысловые структуры неизбежно порождают и увековечивают асимметрию власти

Источник: [10].

проявляется как в практической реализации власти посредством дискурса, так и в желании объяснить истоки изменений в международной политике через нормы и идентичности» [10].

В отношении «практической реализации власти посредством дискурса» пишет Хольцшайтер также выделяет два типа — продуктивный и делиберативный (совещательный), опираясь на идеи М. Фуко и Ю. Хабермаса соответственно. В табл. 2 приведены их особенности.

Таким образом мы получаем теоретическую рамку для использования КДА в исследовании международной политики. В нем есть уровни анализа (микроагенты и макроструктуры), а также типы реализации власти/влияния в дискурсе (совещательный и продуктивный). Отметим, что получившаяся матрица из четырех составляющих может быть применена как к анализу определенного предмета (например, можно рассматривать проблемы борьбы с киберпреступностью, фокусируясь на агентах либо структурах), так и собственно к агентам и структурам, при этом следует помнить о базовой предпосылке социального конструктивизма, где и агенты, и структуры взаимно влияют и определяют друг друга [11].

Теперь, используя эту рамку, сформулируем исследовательские вопросы по нашему примеру: российско-американские отношения в сфере ИКТ-безопасности.

Исследовательские вопросы

Для начала рассмотрим нашу тему с одного конца спектра: как структура влияет на агентов? Для этого поставим следующий вопрос (**RQ1**): влияет ли взаимодействие между США и Россией в киберпространстве на формулирование их дискурсов киберугроз? Иными словами, пересмотрит ли агент свой дискурс и в конечном счете политику кибербезопасности под влиянием двусторонних отношений? Опираясь на теоретическую рамку, этот вопрос мы будем анализировать на уровне *макроструктуры*, т. е. исследовать, как динамика двусторонних отношений (структуры) в киберпространстве может повлиять на восприятие угроз и в конечном итоге изменить дискурс у государств. Чтобы определить тип реализации власти в дискурсе, нужно выбрать индикатор-событие. Например, обвинения России во вмешательстве в президентские выборы в США 2016 г., которое заключалось во взломе серверов Национального комитета демократической партии, избирательной инфраструктуры и информационных кампаниях в социальных сетях для манипулирования общественным мнением [12]. После этого можно увидеть следы изменения дискурса в США и его миграции в сторону информационной безопасности с появлением тезиса о «взломанных выборах, подрывающих американскую демократию» [13]. Здесь мы можем предположить *продуктивный тип реализации*, так как, согласно Фуко, дискурсы закреплены в структурах и воспроизводят неравенство во власти. Иными словами, атакующая сторона определяет модель киберугроз и впоследствии навязывает свой дискурс, заставляя воспринять объект угрозы (институт выборов) как референтный и заслуживающий секьюритизации. Если агент не может навязать дискурс с помощью речевых актов (используя лучший аргумент), тогда он действует через контекст (двустороннее взаимодействие в киберпространстве, зачастую негативное). Анализ американского дискурса будет приведен далее в статье.

Теперь возьмем другой конец спектра (**RQ2:**): как агенты влияют на структуру? Как дискурсы киберугроз США и России влияют на результаты международных переговоров по кибербезопасности? Различия в степени «чувствительности» и первостепенности угроз для обоих государств в конечном счете препятствуют глобальному консенсусу по кибербезопасности. Теперь мы перемещаемся на *микроуровень агентов*, но взаимодействуют они на переговорах по ИКТ в контексте международной безопасности в Первом комитете ООН (а именно ГПЭ и РГОС). Используя речевые акты на этапе переговоров и сформулированные письменно позиции, агенты пытаются убедить остальных участников переговоров в том, что их дискурс киберугроз «правильнее» отражает реальность. Агенты могут использовать структуру для усиления веса своего дискурса, например через количество ко-спонсоров резолюций ООН, касающихся ИКТ в контексте международного мира и безопасности. Индикатором для реализации власти/влияния может служить факт согласования консенсусного доклада по итогам очередного переговорного раунда. Здесь мы предполагаем *совещательный тип реализации,* так как площадка ООН и мандаты обоих переговорных форматов обязывают участников находить консенсус и искать компромисс, поэтому «сила лучшего аргумента» может играть определяющую роль. Однако в RQ2 мы близко сталкиваемся с проблемой «ко-влияния» агентов и структуры. За время существования повестки в Первом комитете структура претерпела

существенные изменения: изначальный формат ГПЭ насчитывал около 20 стран-участниц, при этом заседания группы были закрытыми. С 2018 г. появился параллельный формат РГОС, который допускал участие всех стран — членов ООН, и даже негосударственных акторов в неформальных сессиях, при этом заседания проходят открыто для всех желающих, так же как и документооборот. Такие метаморфозы структуры могут свидетельствовать о стремлении агентов менять правила и процедуры в свою пользу или добиваться большего признания и легитимности своего дискурса киберугроз, расширяя количество участников процесса.

Изучение дискурса угроз в США и России

Для наглядного отображения дискурсов в обеих странах возьмем стратегические документы: доктрины, стратегии национальной безопасности, обороны, внешней политики, концепции и планы действий, посвященные конкретно вопросам кибербезопасности или информационной безопасности на национальном и международном уровнях. Всего было отобрано 16 российских [14–29] и 20 американских документов и [30–49]. Каждый документ изучался на предмет упоминания каких-либо угроз, связанных с использованием ИКТ. По итогам анализа каждой уникальной по смыслу угрозе был присвоен соответствующий тег. Всего было выделено 25 уникальных тегов для российских документов и 27 — для американских. На общем уровне их можно разделить на четыре широкие группы: угрозы, относящиеся к информационной безопасности, к кибербезопасности, к вопросам войны и мира, а также к технологической зависимости (на рис.[1] они отмечены красным, синим, зеленым и желтым соответственно).

В российском дискурсе угроз можно определить все четыре составляющие, при этом акцент идет преимущественно на информационной безопасности, к которой можно отнести сюжеты, связанные с дезинформацией, ограничением работы российских СМИ за рубежом, внешним информационным вмешательством, распространением экстремизма и терроризма в сети, обеспечением общественной безопасности и защитой государственного суверенитета в сети. При этом в документах отмечаются защита критической инфраструктуры, кибершпионаж, уязвимости в ПО и оборудовании, а также наращивание военного потенциала в киберпространстве другими странами, угроза миру и стабильности вследствие возможной кибервойны.

В американском дискурсе преобладает кибербезопасность: уязвимости критической инфраструктуры, ПО и оборудования, ботнеты, кибершпионаж, кража данных, интеллектуальной собственности, низкая осведомленность персонала о киберугрозах, экономические потери вследствие кибератак. Отдельно упоминается защита электоральной инфраструктуры. Однако в общей картине также присутствуют и вопросы информационной безопасности — кибертерроризм (по времени появления совпадает с борьбой США против терроризма на Ближнем Востоке), а также дезинформация и внешнее информационное вмешательство (появляются в документах с 2016 г.). Следующие теги, отнесенные к информационной безопасности — сохранение открытого и свободного интернета и противодействие цензуре, — уже имеют другое смысловое значение — угрозы не *от* использования ИКТ,

[1] См. рисунок в приложении к настоящей статье на сайте: https://doi.org/10.21638/spbu06.2024.205

а *для* ИКТ. Угроза войны также встречается в американском дискурсе, но ей не уделяется много внимания, в отличие от российского.

Стоит отметить, что в документах обеих стран выделялись угрозы, относящиеся к компьютерным преступлениям (киберпреступности), и, с одной стороны, эта часть дискурса у обеих стран совпадает, однако с другой — США придают большое значение к трансграничным атакам на инфраструктуру с использованием вирусов-вымогателей (ransomware), что имело последствия для двусторонних переговоров с Россией в 2021–2022 г.

Уровни анализа

Теперь, когда мы представляем, из чего складываются дискурсы обеих стран, необходимо добавить структуру, а именно поместить эту дискурсивную ретроспективу в контекст двусторонних отношений в области кибербезопасности, а также международных переговоров на уровне ООН[2].

График охватывает период с 2000 по 2024 г. На первых двух шкалах отмечены документы, используемые для анализа дискурсов, а также периоды президентских администраций в обеих странах. На третьей шкале отмечены важные точки двустороннего взаимодействия в области кибербезопасности (например, соглашение о мерах доверия в киберпространстве от 2013 г. [50] или «киберразрядка», наступившая после саммита Путин — Байден в 2021 г. [51]), включающие также механизмы сотрудничества в виде рабочих групп. Кроме продуктивных примеров взаимодействия, на шкале также есть красные точки, свидетельствующие о негативных событиях, заморозивших двустороннее сотрудничество. Примечательно, что в обоих случаях сворачивания рабочих групп (в 2014 и 2022 гг.) катализатором становилось обострение украинского кризиса и резкое ухудшение российско-американских отношений как его следствие. В 2016 г. США обвинили Россию во вмешательстве в президентские выборы, а впоследствии неоднократно заявляли о риске повторения ситуации с выборами в конгресс. Эти обвинения также повлияли на срыв переговоров по кибербезопасности в Женеве в 2018 г. [52]. В 2020 г. со стороны России была предпринята попытка возобновить диалог в рамках двустороннего механизма, предоставить взаимные гарантии невмешательства во внутренние дела, включая выборы [53], но предложение было отвергнуто американской стороной, несмотря на то, что даже в Национальной стратегии по кибербезопасности 2018 г. упоминаются угрозы информационной безопасности: кибератаки как политические инструменты, вмешательство в электоральные процессы и операции информационного влияния на население. Только в 2021 г. диалог возобновится, но с очень ограниченным фокусом на защите критической инфраструктуры, а также на расследовании кибератак с использованием вирусов-вымогателей на американские предприятия, включая Colonial Pipeline и JBS. Российская сторона осталась недовольна таким узким подходом к решению двусторонних проблем в области кибербезопасности [54].

На последней, четвертой шкале отмечены периоды работы переговорных треков: ГПЭ (фиолетовый) и РГОС (оранжевый), а также принятые или непринятые

[2] См. график «График событий на двустороннем и международном уровне в области кибербезопасности» в приложении к настоящей статье на сайте: https://doi.org/10.21638/spbu06.2024.205

консенсусные доклады по итогам работы. Первый провал ГПЭ произошел сразу после первого же созыва в 2004–2005 гг. Тогда причиной стало то, что участники группы не смогли договориться о предмете переговоров и как раз тогда проявились различия в подходах к безопасности между США и Россией. Лишь ко второму созыву в 2009 г. была выработана компромиссная формулировка «безопасное использование ИКТ в контексте международной безопасности», которая позволила продолжить работу и принять первый консенсусный доклад. В 2017 г. причиной отсутствия консенсуса стал вопрос применимости международного гуманитарного права к киберпространству. США и их союзники продвигали позицию, что милитаризация пространства уже происходит, поэтому неизбежно страны придут к тому, чтобы выработать «правила ведения кибервойны», используя свод уже имеющихся норм для конвенциональных войн. Россия и ее союзники отрицали такой подход, настаивая на исключительно мирном использовании ИКТ и сохранении международной стратегической стабильности. Текущий переговорный процесс в рамках РГОС должен завершиться в 2025 г.

Если рассматривать упомянутые угрозы и вызовы в докладах ГПЭ и РГОС, можно заметить, что их список претерпевал изменения с течением времени с точки зрения дискурса: в 2021 г. появились уточняющие положения, характерные для дискурса информационной безопасности. Краткое отображение дискурса можно увидеть в табл. 3.

Продуктивный и делиберативный типы реализации влияния через дискурсы

Напомним, что при формулировании исследовательских вопросов мы предположили типы реализации влияния через дискурсы. Для RQ1 это продуктивный тип, когда агент может изменить политику вынужденно, подчиняясь динамике структуры (на нашем макроструктурном уровне речь идет о двусторонних отношениях). Для RQ2 это совещательный тип, когда агенты используют силу наилучшего аргумента, чтобы прийти к консенсусу (этот вопрос рассматривается на уровне микроагентов, но в контексте переговорных площадок в ООН со своими правилами). Также вернемся к изначальной гипотезе, что прогресс в переговорах по кибербезопасности будет достигнут, когда дискурсы агентов по угрозам будут совпадать. Поэтому нам важно следить за динамикой развития дискурсов обоих агентов и отмечать факторы, влияющие на их изменения.

Оценивая ретроспективно российско-американские отношения в сфере ИКТ-безопасности, мы видим, что разница в дискурсах, т. е. в приоритетах угроз, существенна, но позитивное взаимодействие происходило как раз в рамках кибербезопасности — меры укрепления доверия, выработка подходов к защите критической инфраструктуры. Однако попытки российской стороны привнести элементы информационной безопасности, в том числе политические аспекты ИКТ-угроз, встречали сопротивление. В этом контексте, если предположить, что Россия действительно могла[3] организовать вмешательство в американские выборы [60] и таким образом добавить новый референтный объект в рамках секьюритизации, мы

[3] Официально российские власти отрицают какое-либо вмешательство.

Таблица 3. **Дискурс угроз по документам**

Виды угроз	ГПЭ 2010	ГПЭ 2013	ГПЭ 2015	ГПЭ 2021	РГОС 2021
киберпреступность	+	+	+	+	+
проблема атрибуции совершенных кибератак		+	+	+	
использование ИКТ в террористических целях	+		+	+	+
проблема кибернаемников (посредников для осуществления кибератак)	+				
нападения на объекты критической инфраструктуры	+	+	+	+ (медицинские объекты и здравоохранение)	+ (в том числе информационной, а также подрывающие доверие к политическим и избирательным процессам и государственным институтам или оказывающие влияние на общедоступность и целостность интернета)
наращивание государствами военного потенциала в сфере ИКТ	+		+	+	+
использование ИКТ в политических целях	+	+		+ (скрытые информационные кампани с применением ИКТ для влияния на процессы, системы и общую стабильность другого государства)	
проблема доверия к производимому ПО и оборудованию (не задекларированные вредоносные функции)		+			
использование уязвимостей в сетях и продуктах/сервисах для совершения атак		+		+	
разный потенциал государств в обеспечении безопасности в области ИКТ	+		+	+	+
отсутствие норм приемлемого использования ИКТ для государств	+	+			

Источники: [55–59].

могли бы говорить о продуктивном типе реализации влияния на уровне макроструктуры, поскольку дальнейшие стратегические документы США фиксируют составные части дискурса информационной безопасности после 2016 г. Однако наивно полагать, что такой шаг мог быть спланирован только для изменения дискурса, скорее это стало побочным эффектом в рамках более сложного политического взаимодействия двух стран с богатой историей конфронтации друг с другом.

Если мы рассматриваем взаимодействие США и России как двух основных двигателей переговорного процесса в Первом комитете, то видим, что странам (и их союзникам) приходилось искать компромиссы, что отчетливо видно по тому, какие доклады состоялись, а какие нет. Конечно, круг обсуждаемых вопросов на ГПЭ и РГОС был существенно шире, чем обсуждение ИКТ-угроз. Проблемы применения международного права к киберпространству, а также возможность создания юридически обязывающих норм играли гораздо большую роль для успешного завершения очередного мандата групп. Но в рамках нашего исследования угроз мы видим, что даже здесь есть динамика в общем дискурсе докладов, а значит, государства, принимавшие участие в обсуждениях, нашли способы отразить волнующие их угрозы, с которыми согласились все члены сначала переговорной группы, а затем и государства — члены ООН, поскольку каждый доклад был одобрен соответствующей резолюцией ГА ООН. При этом важно сделать оговорку, что необходимо также более подробно изучить «речевые акты» и США, и России во время сессий РГОС[4], чтобы составить более полную картину дискурсов обеих стран в контексте взаимодействия на переговорной площадке, так как на текущем этапе мы проанализировали только консенсусные документы, в составлении которых принимали участие и другие страны.

Поэтому на уровне микроагентов мы можем говорить о совещательном типе реализации влияния в рамках нашего исследовательского вопроса. Примечательно, что если рассматривать этот же вопрос на макроструктурном уровне, как это делает М. Раймонд, объясняя постепенный прогресс в разработке кибернорм, несмотря на глубокие политические разногласия участников, необходимостью следовать процедурным правилам переговорной площадки [61], то тогда можно говорить о продуктивном типе реализации влияния, но уже структуры на агентов. Здесь проблема ко-влияния структуры и агентов в конструктивистской эпистемологии проявляется как никогда наглядно.

Ограничения метода и выводы

Использование КДА в анализе политики кибербезопасности выглядит довольно интересным и наглядным подходом, но остается вопрос, насколько изучение дискурса приблизит нас к пониманию причин изменения политики? А. Хольцшайтер справедливо замечает, что совершенно не ясно, являются ли изменения дискурса следствием изменения политики или причиной самой по себе. Как мы можем увидеть из рассуждения выше, в зависимости от уровня анализа, а точнее того, что

[4] Все субстантивные сессии РГОС имеют видеозапись и изучение выступлений стран технически реализуемо. В то же время заседания ГПЭ были закрытыми, поэтому материала для анализа, кроме итоговых докладов, нет.

мы делаем отправной точкой в исследовании — агентов или структуру, — мы получаем совершенно разные объяснения причинно-следственных связей.

Исследование ИКТ-безопасности усложняется еще и тем, что мы обязаны держать в фокусе и двусторонний, и международный уровень взаимодействия, так как эти процессы тесно взаимосвязаны. Изучать политику ИКТ-безопасности любой страны изолированно на одном из уровней представляется непродуктивным.

Также важно держать в уме, что иногда киберповестка становится частью более широкой повестки стратегической стабильности, включая обычные и ядерные вооружения, и часто оказывается «разменной монетой» для маневра на переговорах. В паре США — Россия это проявляется очень отчетливо.

Тем не менее применение КДА позволяет выявить значимые нюансы политики кибербезопасности / информационной безопасности государства, однако ввиду совместного влияния на формирование политики как агентов процесса, так и структур в которых они взаимодействуют, невозможно выделить конкретные факторы, объясняющие смену акцентов политики. Понимание дискурсов и их сопоставление позволяет объяснить, почему, несмотря на всеми признанную важность проблемы, не удается достичь значительного прогресса в формировании глобального режима по кибербезопасности. Страны-локомотивы этого процесса, а именно США и Россия, значительно отличаются друг от друга в приоритезации угроз, исходящих из использования ИКТ. В таком случае гипотеза, выдвинутая в начале статьи, пока не опровергнута.

Литература

1. Йоргенсен, М. и Филлипс, Л. Дж. (2008), *Дискурс-анализ. Теория и метод*, пер. с англ., 2-е изд., испр., Харьков: Гуманитарный центр.

2. Fairclough, N. and Wodak, R. (1997), Critical Discourse Analysis, in: van Dijk, T. (ed.), *Discourse Studies: A Multidisciplinary Introduction,* vol. 2. London: Sage, pp. 258–284.

3. Titscher, S., Meyer, M., Wodak, R. and Vetter, E. (2000), *Methods of Text and Discourse Analysis*, London: Sage Publications Ltd. Sage Knowledge. https://doi.org/10.4135/9780857024480

4. Buzan, B. and Waever, O. (1998), *Security: A New Framework for Analysis*, Boulder: Lynne Rienner Publishers.

5. Пучков, О. А. (2019), Разграничение понятий «информационная безопасность» и «кибербезопасность» в законодательстве Российской Федерации, доктрине и юридической практике, *Право и государство: теория и практика,* № 5 (173), с. 66–69.

6. Developments in the field of information and telecommunications in the context of international security, *UNODA*. URL: https://disarmament.unoda.org/ict-security/ (дата обращения: 26.11.2023).

7. *Основы государственной политики Российской Федерации в области ядерного сдерживания* (2020). URL: https://www.mid.ru/ru/foreign_policy/international_safety/disarmament/1434131/ (дата обращения: 26.11.2023).

8. *Nuclear Posture Review, Department of Defense* (2018). URL: https://media.defense.gov/2018/Feb/02/2001872877/-1/-1/1/EXECUTIVE-SUMMARY.PDF (дата обращения: 26.11.2023).

9. Mačák, K. (2017), From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers, *Social Science Research Network*. SSRN Scholarly Paper ID 2961821. URL: https://papers.ssrn.com/abstract=2961821 (дата обращения: 26.11.2023).

10. Holzscheiter, A. (2013), Between Communicative Interaction and Structures of Signification: Discourse Theory and Analysis in International Relations, *International Studies Perspectives*, vol. 15, iss. 2. https://doi.org/10.1111/insp.12005

11. Wendt, A. E. (1987). The Agent-Structure Problem in International Relations Theory, *International Organization*, vol. 41, no. 3, pp. 335–370.

12. Шариков, П. (2018) Информационный суверенитет и вмешательство во внутренние дела в Российско-американских отношениях, *Международные процессы,* т. 16, № 3 (54), с. 170–188.

13. *National Cyber Strategy of the United States of America* (2018). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 26.11.2023).

14. *Доктрина информационной безопасности Российской Федерации* (2000). URL: https://base.garant.ru/182535/ (дата обращения: 26.11.2023).

15. *Стратегия национальной безопасности Российской Федерации* (2000). URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения: 26.11.2023).

16. *Концепция внешней политики Российской Федерации* (2000). URL: https://docs.cntd.ru/document/901764263 (дата обращения: 26.11.2023).

17. *Концепция внешней политики Российской Федерации* (2008). URL: https://www.consultant.ru/document/cons_doc_LAW_85021/ (дата обращения: 26.11.2023).

18. *Стратегия национальной безопасности Российской Федерации* (2009). URL: http://www.kremlin.ru/supplement/424 (дата обращения: 26.11.2023).

19. *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве* (2011). URL: https://ens.mil.ru/files/morf/Strategy.doc (дата обращения: 26.11.2023).

20. *Концепция внешней политики Российской Федерации* (2013). URL: https://docs.cntd.ru/document/499003797 (дата обращения: 26.11.2023).

21. *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года* (2013). URL: https://base.garant.ru/70641072/ (дата обращения: 26.11.2023).

22. *Концепция стратегии кибербезопасности Российской Федерации (Проект)* (2013). URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 26.11.2023).

23. *Военная доктрина Российской Федерации* (2014). URL: https://docs.cntd.ru/document/420246589 (дата обращения: 26.11.2023).

24. *Стратегия национальной безопасности Российской Федерации* (2015). URL: https://docs.cntd.ru/document/420327289 64U0IK (дата обращения: 26.11.2023).

25. *Доктрина информационной безопасности Российской Федерации* (2016). URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения: 26.11.2023).

26. *Концепция внешней политики Российской Федерации* (2016). URL: http://static.kremlin.ru/media/acts/files/0001201612010045.pdf (дата обращения: 26.11.2023).

27. *Стратегия национальной безопасности Российской Федерации* (2021). URL: https://docs.cntd.ru/document/607148290 (дата обращения: 26.11.2023).

28. *Основы государственной политики Российской Федерации в области международной информационной безопасности* (2021). URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 26.11.2023).

29. *Концепция внешней политики Российской Федерации* (2023). URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения: 26.11.2023).

30. *US National Security Strategy* (2002). URL: https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ (дата обращения: 26.11.2023).

31. *US National Strategy to Secure Cyberspace* (2003). URL: https://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 26.11.2023).

32. *US National Defense Strategy* (2005). URL: https://nssarchive.us/wp-content/uploads/2020/04/2005_NDS. pdf (дата обращения: 26.11.2023).

33. *US National Security Strategy* (2006). URL: http://nssarchive.us/national-security-strategy-2006/ (дата обращения: 26.11.2023).

34. *US National Defense Strategy* (2008). URL: https://nssarchive.us/wp-content/uploads/2020/04/2008 NationalDefenseStrategy.pdf (дата обращения: 26.11.2023).

35. *US Cyberspace Policy Review* (2009). URL: https://www.cisa.gov/resources-tools/resources/2009-cyberspace-policy-review (дата обращения: 26.11.2023).

36. *US National Security Strategy* (2010). URL: https://nssarchive.us/national-security-strategy-2010/ (дата обращения: 26.11.2023).

37. *US Department of Defense Strategy for operating in cyberspace* (2011). URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата обращения: 26.11.2023).

38. *US Department of Homeland Security Blueprint for a secure cyber future* (2011). URL: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (дата обращения: 26.11.2023).

39. *US International Strategy for Cyberspace* (2011). URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ international_strategy_for_cyberspace.pdf (дата обращения: 26.11.2023).

40. *US National Defense Strategy* (2012). URL: https://nssarchive.us/wp-content/uploads/2020/04/defense_strategic_guidance.pdf (дата обращения: 26.11.2023).

41. *US Department of Defense Cyber Strategy* (2015). URL: https://nsarchive.gwu.edu/document/21384-document-25 (дата обращения: 26.11.2023).

42. *US National Security Strategy* (2015). URL: http://nssarchive.us/national-security-strategy-2015/ (дата обращения: 26.11.2023).

43. *US Department of State International Cyber Strategy* (2016). URL: https://ccdcoe.org/uploads/2018/10/USA_Department-of-State_-International-Cyberspace-Policy-Strategy_2016.pdf (дата обращения: 26.11.2023).

44. *US National Security Strategy* (2017). URL: http://nssarchive.us/national-security-strategy-2017/ (дата обращения: 26.11.2023).

45. *US Department of Homeland Security Cybersecurity Strategy* (2018). URL: https://www.dhs.gov/publication/dhs-cybersecurity-strategy (дата обращения: 26.11.2023).

46. *US National Defense Strategy* (2018). URL: https://nssarchive.us/wp-content/uploads/2020/04/2018_NDS. pdf (дата обращения: 26.11.2023).

47. *US Department of Defense Cyber Strategy* (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL. PDF (дата обращения: 26.11.2023).

48. *US National Cyber Strategy* (2018). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 26.11.2023).

49. *US National Cybersecurity Strategy* (2023). URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата обращения: 26.11.2023).

50. *Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия* (2013). URL: http://www.kremlin.ru/supplement/1479 (дата обращения: 26.11.2023).

51. Cyber detente and the Biden-Putin Summit: What this meant for cyber relations between the USA and Russia, *DigitalWatch*, *Geneva Internet Platform*. URL: https://dig.watch/trends/cyber-detente The-evolution-of-USA-Russia-cyber-relations-over-the-years (дата обращения: 26.11.2023).

52. Вместо встречи изменить уже нельзя (2018), *Коммерсант*, 2 марта. URL: https://www.kommersant.ru/doc/3565613 (дата обращения: 26.11.2023).

53. *Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности* (2020). URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 26.11.2023).

54. Рябков: Россия и США провели уже четыре раунда консультаций по кибербезопасности (2021), *Коммерсант*, 22 июля. URL: https://www.kommersant.ru/doc/4910861 (дата обращения: 26.11.2023).

55. *A/65/201* (2010). URL: https://documents.un.org/doc/undoc/gen/n10/469/59/pdf/n1046959.pdf?token=2cEcal4PB2gMYGXnBh&fe=true (дата обращения: 26.11.2023).

56. *A/68/98* (2013). URL: https://documents.un.org/doc/undoc/gen/n13/371/68/pdf/n1337168.pdf?token=pVN6JLfb6fZY56rvsA&fe=true (дата обращения: 26.11.2023).

57. *A/70/174* (2015). URL: https://documents.un.org/doc/undoc/gen/n15/228/37/pdf/n1522837.pdf?token=HMCYHqBx37Phrx8wSy&fe=true (дата обращения: 26.11.2023).

58. *A/75/816* (2021). URL: https://documents.un.org/doc/undoc/gen/n21/068/74/pdf/n2106874.pdf?token=cSYsigTG8MRKa0xWfn&fe=true (дата обращения: 26.11.2023).

59. *A/76/135* (2021). URL: https://documents.un.org/doc/undoc/gen/n21/075/88/pdf/n2107588.pdf?token=B1RrtH8X98lOfc7F4F&fe=true (дата обращения: 26.11.2023).

60. *House Permanent Select Committee on Intelligence. Report on Russia Active Measures* (2018). URL: https://republicansintelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf (дата обращения: 26.11.2023).

61. Raymond, M. (2021), Social Practices of Rule-Making for International Law in the Cyber Domain. *Journal of Global Security Studies*, vol. 6, iss. 2. https://doi.org/10.1093/jogss/ogz065

Статья поступила в редакцию 10 января 2024 г.;
рекомендована к печати 20 февраля 2024 г.

Контактная информация:

Стадник Илона Тарасовна — ассистент; i.stadnik@spbu.ru

How to study ICT-security policy: Opportunities and challenges for critical discourse-analysis

I. T. Stadnik

St. Petersburg State University,
7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation

For citation: Stadnik I. T. How to study ICT-security policy: Opportunities and challenges for critical discourse-analysis. *Vestnik of Saint Petersburg University. International Relations*, 2024, vol. 17, issue 2, pp. 183–200. https://doi.org/10.21638/spbu06.2024.205 (In Russian)

The article examines the method of critical discourse-analysis (CDA) on the example of the relations between the United States and Russia in the field of ICT security, as well as in the context of negotiations at the UN level in the same area, where both countries have a significant influence on the processes. CDA can be used to study ICT security policy in order to understand how different actors use language to discuss problems: what terms and concepts are used, as well as how they can influence public perception of the problem. CDA can also be used to study the dynamics of interaction between different actors: what interests they pursue and what compromises they are willing to make to achieve common goals. The method is connected with the theoretical framework of A. Holzscheiter, which identifies the levels of analysis (micro-agents and macro-structures), as well as the types of power/influence realization in discourse (deliberative and productive). As a demonstration of the method, the author has made a brief analysis of the discourses of ICT threats to the United States and Russia based on strategic documents of the states. It is inscribed in the structures of bilateral relations and international negotiations, presented in the form of events on a timeline. Depending on the level of analysis or the starting point of the study — agents or structures — we get completely different explanations of the causal relationships of possible explanations for policy change through discourse (productive or deliberative). The study of ICT security is further complicated by the fact that we must keep both the bilateral and international levels of interaction in focus, since these processes are closely interrelated. In conclusion, the article describes important limitations of the method, including the weak explanatory potential of the reasons for the change in ICT security policy.

Keywords: critical discourse-analysis, cybersecurity, information security, agent-structure problem, United States, Russia.

References

1. Jorgensen, M. and Phillips, L. J. (2008), *Discourse analysis. Theory and method*, transl. from Eng., 2nd ed., Kharkov: Gumanitarnyi tsentr Publ. (In Russian)

2. Fairclough, N. and Wodak, R. (1997), Critical Discourse Analysis, in: van Dijk, T. (ed.), *Discourse Studies: A Multidisciplinary Introduction,* vol. 2. London: Sage, pp. 258–284.

3. Titscher, S., Meyer, M., Wodak, R. and Vetter, E. (2000), *Methods of Text and Discourse Analysis*, London: Sage Publications Ltd. Sage Knowledge. https://doi.org/10.4135/9780857024480

4. Buzan, B. and Waever, O. (1998), *Security: A New Framework for Analysis*, Boulder: Lynne Rienner Publishers.

5. Puchkov, O. A. (2019), Differentiation of the concepts of "information security" and "cybersecurity" in the legislation of the Russian Federation, doctrine and legal practice, *The Rule of Law State: Theory and Practice*, no. 5(173), pp. 66–69. (In Russian)

6. Developments in the field of information and telecommunications in the context of international security, *UNODA*. Available at: https://disarmament.unoda.org/ict-security/ (accessed: 26.11.2023).

7. *Fundamentals of the state policy of the Russian Federation in the field of nuclear deterrence* (2020). Available at: https://www.mid.ru/ru/foreign_policy/international_safety/disarmament/1434131/ (accessed: 26.11.2023). (In Russian)

8. *Nuclear Posture Review, Department of Defense* (2018). Available at: https://media.defense.gov/2018/Feb/02/2001872877/-1/-1/1/EXECUTIVE-SUMMARY.PDF (accessed: 26.11.2023).

9. Mačák, K. (2017), From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers, *Social Science Research Network*. SSRN Scholarly Paper ID 2961821. Available at: https://papers.ssrn.com/abstract=2961821 (accessed: 26.11.2023).

10. Holzscheiter, A. (2013), Between Communicative Interaction and Structures of Signification: Discourse Theory and Analysis in International Relations, *International Studies Perspectives*, vol. 15, iss. 2. https://doi.org/10.1111/insp.12005

11. Wendt, A. E. (1987). The Agent-Structure Problem in International Relations Theory, *International Organization*, vol. 41, no. 3, pp. 335–370.

12. Sharikov, P. (2018), Information sovereignty and interference in internal affairs in Russian-American relations, *Mezhdunarodnye protsessy*, vol. 16, no. 3(54), pp. 170–188. (In Russian)

13. *National Cyber Strategy of the United States of America* (2018). Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed: 26.11.2023).

14. *Information Security Doctrine of the Russian Federation* (2000). Available at: https://base.garant.ru/182535/ (accessed: 26.11.2023). (In Russian)

15. *National Security Strategy of the Russian Federation* (2000). Available at: http://www.scrf.gov.ru/security/information/document5/ (accessed: 26.11.2023). (In Russian)

16. *Foreign Policy Concept of the Russian Federation* (2000). Available at: https://docs.cntd.ru/document/901764263 (accessed: 26.11.2023). (In Russian)

17. *Foreign Policy Concept of the Russian Federation* (2008). Available at: https://www.consultant.ru/document/cons_doc_LAW_85021/ (accessed: 26.11.2023). (In Russian)

18. *National Security Strategy of the Russian Federation* (2009). Available at: http://www.kremlin.ru/supplement/424 (accessed: 26.11.2023). (In Russian)

19. *Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space* (2011). Available at: https://ens.mil.ru/files/morf/Strategy.doc (accessed: 26.11.2023). (In Russian)

20. *Foreign Policy Concept of the Russian Federation* (2013). Available at: https://docs.cntd.ru/document/499003797 (accessed: 26.11.2023). (In Russian)

21. *Fundamentals of the state policy of the Russian Federation in the field of international information security for the period up to 2020* (2013). Available at: https://base.garant.ru/70641072/ (accessed: 26.11.2023). (In Russian)

22. *The concept of the Cybersecurity Strategy of the Russian Federation (Draft)* (2013). Available at: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (accessed: 26.11.2023). (In Russian)

23. *Military doctrine of the Russian Federation* (2014). Available at: https://docs.cntd.ru/document/420246589 (accessed: 26.11.2023). (In Russian)

24. *National Security Strategy of the Russian Federation* (2015). Available at: https://docs.cntd.ru/document/420327289 64U0IK (accessed: 26.11.2023). (In Russian)

25. *Information Security Doctrine of the Russian Federation* (2016). Available at: http://www.scrf.gov.ru/security/information/document5/ (accessed: 26.11.2023). (In Russian)

26. *Foreign Policy Concept of the Russian Federation* (2016). Available at: http://static.kremlin.ru/media/acts/files/0001201612010045.pdf (accessed: 26.11.2023). (In Russian)

27. *National Security Strategy of the Russian Federation* (2021). Available at: https://docs.cntd.ru/document/607148290 (accessed: 26.11.2023). (In Russian)

28. *Fundamentals of the state policy of the Russian Federation in the field of international information security* (2021). Available at: http://www.scrf.gov.ru/security/information/document114/ (accessed: 26.11.2023). (In Russian)

29. *Foreign Policy Concept of the Russian Federation* (2023). Available at: https://www.mid.ru/ru/detail-material-page/1860586/ (accessed: 26.11.2023). (In Russian)

30. *US National Security Strategy* (2002). Available at: https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ (accessed: 26.11.2023).

31. *US National Strategy to Secure Cyberspace* (2003). Available at: https://georgewbush-whitehouse.archives.gov/pcipb/ (accessed: 26.11.2023).

32. *US National Defense Strategy* (2005). Available at: https://nssarchive.us/wp-content/uploads/2020/04/2005_NDS.pdf (accessed: 26.11.2023).

33. *US National Security Strategy* (2006). Available at: http://nssarchive.us/national-security-strategy-2006/ (accessed: 26.11.2023).

34. *US National Defense Strategy* (2008). Available at: https://nssarchive.us/wp-content/uploads/2020/04/2008NationalDefenseStrategy.pdf (accessed: 26.11.2023).

35. *US Cyberspace Policy Review* (2009). Available at: https://www.cisa.gov/resources-tools/resources/2009-cyberspace-policy-review (accessed: 26.11.2023).

36. *US National Security Strategy* (2010). Available at: https://nssarchive.us/national-security-strategy-2010/ (accessed: 26.11.2023).

37. *US Department of Defense Strategy for operating in cyberspace* (2011). Available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed: 26.11.2023).

38. *US Department of Homeland Security Blueprint for a secure cyber future* (2011). Available at: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (accessed: 26.11.2023).

39. *US International Strategy for Cyberspace* (2011). Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ international_strategy_for_cyberspace.pdf (accessed: 26.11.2023).

40. *US National Defense Strategy* (2012). Available at: https://nssarchive.us/wp-content/uploads/2020/04/defense_strategic_guidance.pdf (accessed: 26.11.2023).

41. *US Department of Defense Cyber Strategy* (2015). Available at: https://nsarchive.gwu.edu/document/21384-document-25 (accessed: 26.11.2023).

42. *US National Security Strategy* (2015). Available at: http://nssarchive.us/national-security-strategy-2015/ (accessed: 26.11.2023).

43. *US Department of State International Cyber Strategy* (2016). Available at: https://ccdcoe.org/uploads/2018/10/USA_Department-of-State_-International-Cyberspace-Policy-Strategy_2016.pdf (accessed: 26.11.2023).

44. *US National Security Strategy* (2017). Available at: http://nssarchive.us/national-security-strategy-2017/ (accessed: 26.11.2023).

45. *US Department of Homeland Security Cybersecurity Strategy* (2018). Available at: https://www.dhs.gov/publication/dhs-cybersecurity-strategy (accessed: 26.11.2023).

46. *US National Defense Strategy* (2018). Available at: https://nssarchive.us/wp-content/uploads/2020/04/2018_NDS.pdf (accessed: 26.11.2023).

47. *US Department of Defense Cyber Strategy* (2018). Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed: 26.11.2023).

48. *US National Cyber Strategy* (2018). Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed: 26.11.2023).

49. *US National Cybersecurity Strategy* (2023). Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed: 26.11.2023).

50. *Joint statement by the Presidents of the Russian Federation and The United States of America on a new area of cooperation in confidence-building* (2013). Available at: http://www.kremlin.ru/supplement/1479 (accessed: 26.11.2023). (In Russian)

51. Cyber detente and the Biden-Putin Summit: What this meant for cyber relations between the USA and Russia, *DigitalWatch*, *Geneva Internet Platform*. Available at: https://dig.watch/trends/cyber-detente The-evolution-of-USA-Russia-cyber-relations-over-the-years (accessed: 26.11.2023).

52. Instead of a meeting, it is no longer possible to change (2018), *Kommersant*, March 2. Available at: https://www.kommersant.ru/doc/3565613 (accessed: 26.11.2023). (In Russian)

53. *Vladimir Putin's statement on a comprehensive program of measures to restore Russian-American cooperation in the field of international information security* (2020). Available at: http://kremlin.ru/events/president/news/64086 (accessed: 26.11.2023). (In Russian)

54. *Ryabkov: Russia and the United States have already held four rounds of consultations on cybersecurity* (2021), *Kommersant* July 22. Available at: https://www.kommersant.ru/doc/4910861 (accessed: 26.11.2023). (In Russian)

55. *A/65/201* (2010). Available at: https://documents.un.org/doc/undoc/gen/n10/469/59/pdf/n1046959.pdf?token=2cEcal4PB2gMYGXnBh&fe=true (accessed: 26.11.2023).

56. *A/68/98* (2013). Available at: https://documents.un.org/doc/undoc/gen/n13/371/68/pdf/n1337168.pdf?token=pVN6JLfb6fZY56rvsA&fe=true (accessed: 26.11.2023).

57. *A/70/174* (2015). Available at: https://documents.un.org/doc/undoc/gen/n15/228/37/pdf/n1522837.pdf?token=HMCYHqBx37Phrx8wSy&fe=true (accessed: 26.11.2023).

58. *A/75/816* (2021). Available at: https://documents.un.org/doc/undoc/gen/n21/068/74/pdf/n2106874.pdf?token=cSYsigTG8MRKa0xWfn&fe=true (accessed: 26.11.2023).

59. *A/76/135* (2021). Available at: https://documents.un.org/doc/undoc/gen/n21/075/88/pdf/n2107588.pdf?token=B1RrtH8X98lOfc7F4F&fe=true (accessed: 26.11.2023).

60. *House Permanent Select Committee on Intelligence. Report on Russia Active Measures* (2018). Available at: https://republicansintelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf (accessed: 26.11.2023).

61. Raymond, M. (2021), Social Practices of Rule-Making for International Law in the Cyber Domain. *Journal of Global Security Studies*, vol. 6, iss. 2. https://doi.org/10.1093/jogss/ogz065

Received: January 10, 2024
Accepted: February 20, 2024

Author's information:

Ilona T. Stadnik — Assistant Lecturer; i.stadnik@spbu.ru