РУСОФОБИЯ КАК СТРАТЕГИЯ СЕКЬЮРИТИЗАЦИИ КИБЕРПРОСТРАНСТВА США

Аннотация

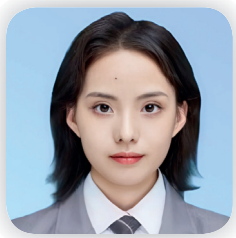
Субъекты секьюритизации рассматривают определенную проблему как экзистенциальную угрозу, используя свою дискурсивную власть для интеграции этой проблемы в стратегический национальный фреймворк безопасности. На этой основе правительство принимает чрезвычайные меры для ответа на эту угрозу и стремится убедить аудиторию в их необходимости. США неоднократно подчеркивали, что Россия осуществляла атаки через Сеть на американское правительство и обвиняли Россию в манипуляции американскими выборами, заставляя элиту и население поверить, что Россия представляет угрозу национальной безопасности США в киберпространстве, что далее легитимизирует и осуществляет нестандартные меры сдерживания России. Рассматривая Россию как основную угрозу, США дополнительно укрепляют свои полномочия в киберпространстве, продвигают процесс милитаризации киберпространства.

Ключевые слова: секьюритизация, киберпространство, США, Россия, дискурсивная манипуляция.

Автор

Ван Юэ

Аспирантка кафедры сравнительной политологии
Российского университета дружбы народов
им. Патриса Лумумбы
Москва, Россия



Теория секьюритизации была впервые предложена и развита Копенгагенской школой. Она заключается в том, что действующие субъекты маркируют определенные вопросы или объекты как экзистенциальную угрозу и через речевые действия добиваются признания этих угроз аудиторией, чтобы оправдать свои действия по данному вопросу [8]. В теории секьюритизации Копенгагенской школы безопасность выходит за рамки обычной политики, она, по сути, переводит вопросы общеполитической сферы в сферу безопасности, чтобы получить преимущество в принятии срочных мер. Поэтому Копенгагенская школа считает, что безопасность носит идейный характер, а секьюритизация является дискурсивным процессом. Важно, как политическая элита выбирает и определяет угрозы [17]. Секьюритизация представляет собой процесс взаимодействия субъектов безопасности, референтных объектов и аудитории, в ходе которого формируется коллективная реакция и общее восприятие определенной угрозы.

В России секьюритизация чаще анализируется через призму связки «безопасность — развитие», обращая внимание на взаимосвязь между развитием и безопасностью в процессе секьюритизации. В этом контексте некоторые ученые придают особое значение роли дискурса. Например, В.И. Бартенев изучает секьюритизацию сферы содействия международному развитию, показывая, как международное сообщество посредством политического дискурса превращает проблемы развития в категорию угроз безопасности [1]. Н.В. Юдин указывает, что секьюритизация не является про-

стым взаимопроникновением и расширением сфер безопасности и развития, а требует акцента на ее сути как особой дискурсивной практики [7, с. 20]. В другой своей статье он исходит из «узкого, постмодернистского понимания теории секьюритизации» и анализирует секьюритизацию дискурса «мягкой силы» [6, с. 60].

Несмотря на то, что в российских и зарубежных исследованиях секьюритизации дискурсивные практики занимают важное место, большинство работ предоставляют лишь общий макрорамочный подход, а объяснение функционирования дискурса зачастую остается слишком обобщенным. Кроме того, угрозы в киберпространстве обычно обладают виртуальностью и анонимностью, а также часто пересекают границы, их нельзя напрямую приписать определенным действующим субъектам. Это приводит к тому, что государства в сфере секьюритизации киберпространства более склонны использовать речевые действия для конструирования угроз.

В методологической части данной статьи используется теоретическая рамка манипуляции дискурсом китайского ученого Ай Сижуна, дискурсивные практики в процессе секьюритизации конкретизируются в три переменные: салиентность дискурса (salience), фреймирование дискурса (framing) и позиционирование дискурса (positioning) [26], с некоторыми незначительными изменениями, как показано на рисунке.

Конструкция и салиентность ситуации угрозы — секьюритизация киберпространства США и американо-российская конкуренция

С развитием информационных и коммуникационных технологий киберпространство стало не только средством обмена и распространения информации, но и важной областью национальной безопасности и международного управления. Поскольку киберпространство не подчиняется традиционным концепциям суверенитета, его функционирование и безопасность трудно контролировать напрямую через единое государственное учреждение, что ведет к сложности регулирования [5]. Этот недостаток регулирования способствует увеличению угроз, таких как киберпреступность, кибершпионаж и распространение фальшивой информации, из-за чего многие страны ускорили процесс секьюритизации киберпространства. В этом процессе кибербезопасность была поднята до уровня ключевого аспекта национальной безопасности и стала центральной темой в формулировке политики безопасности. В то же время конфронтация между государствами постепенно расширилась с традиционной военной сферы на киберпространство, где власть

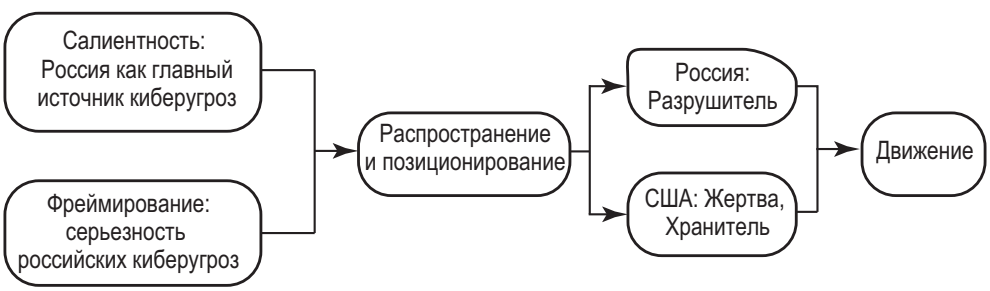


Рисунок 1. Процесс дискурсивной манипуляции США в рамках секьюритизации. Составлено автором

и влияние стали предметом борьбы между странами.

Еще в начале 1990-х годов США начали переход от обычной политизации вопросов кибербезопасности к ее секьюритизации. Событие с «червем Морриса» в 1988 году вызвало широкую обеспокоенность правительства и общества США по вопросам кибербезопасности, после чего была создана Команда компьютерного реагирования на чрезвычайные ситуации (CERT), но тогда угрозы описывались только на техническом уровне. Последующий ряд хакерских атак побудил США включить вопросы кибербезопасности в повестку дня правительства, что способствовало разработке ранних мер защиты и реагирования в Сети. Война в Персидском заливе в 1991 году заставила США осознать важность информационной войны и способности доминировать в информационном пространстве, и угрозы начали рассматриваться в контексте национальной безопасности. Чиновник Министерства обороны США Ричард Кларк ввел концепцию «цифрового Перл-Харбора», связывая кибератаки иностранных хакеров с потенциально катастрофическими последствиями. После терактов 11 сентября 2001 г. США включили киберпространство в свою военную стратегию, подчеркнув, что «информационное преимущество» является ключом к победе в современной войне [11].

В последние годы США все чаще рассматривают определенные государства как источник киберугроз. В 2016 году американское правительство впервые официально обвинило Россию в кибератаках на организации Демократической партии перед президентскими выборами 8 ноября [21]. В этом контексте США приняли закон о противодействии иностранной пропаганде и дезинформации, который предусматривает разработку «общегосударственной» стратегии борьбы с иностранной дезинформацией [4]. Был создан Глобальный центр взаимодействия (GEC), в котором были сформированы рабочие группы для противодействия угрозам от России, Китая, Ирана и терроризма. В 2017 и 2020 годах Консультативная комиссия США по публичной дипломатии опубликовала доклады о цифровой дипломатии. В сравнении с докладом 2017 года в версии 2020 года слово «угроза» упоминается значительно чаще, причем угроза, конфликты или дезинформация все чаще связываются с Россией. В данном докладе Россия упоминается 104 раза, тогда как Китай — лишь 11 [3]. Эти документы отражают усиление идей США о противостоянии в киберпространстве, особенно выделяя Россию как главный объект борьбы.

Игра между США и Россией также расширилась с традиционного геополитического соперничества до сферы кибербезопасности, причем информационное пространство стало основной ареной для проведения Штатами «гибридной войны» против России, а информационная война в киберпространстве между США и Россией усиливается. Кроме того, установление международного порядка в процессе секьюритизации киберпространства также является одним из ключевых моментов в игре между США и Россией. Во главе с США НАТО продвигает в ООН международные нормы для киберпространства, которые подчеркивают применимость международного права в области прав человека и законодательства об использовании вооруженной силы в киберпространстве, а также выступают против «сетевого суверенитета», предложенного Россией и Китаем [24].

Фреймирование и распространение дискурса кибербезопасности США.

Согласно теории секьюритизации субъекты секьюритизации обладают высоким уровнем авторитета и власти, обычно это государственные лидеры

и политическая элита. Именно эти группы могут использовать свое положение для максимального воздействия на аудиторию и в конечном итоге реализации мер секьюритизации. Аудитория играет ключевую роль, для успешной секьюритизации определенной темы необходимо, чтобы она была принята аудиторией, между ней и субъектом было достигнуто согласие относительно угрозы и поддержаны нестандартные меры, направленные на решение этой проблемы.

В процессе секьюритизации, чтобы лучше убедить аудиторию, субъекты используют в своем дискурсе выборочное выделение некоторых аспектов угрозы, влияя тем самым на понимание и восприятие аудиторией данной проблемы безопасности для достижения более высокого уровня секьюритизации. Этот процесс называется «фреймирование дискурса». В когнитивной лингвистике фреймы — это психологические структуры, формирующие когнитивное поведение и действия людей. Когда люди слышат определенное слово, в их мозгу активируется соответствующий фрейм. В политическом дискурсе фреймы представляют проблему с определенной (выгодной) точки зрения, чтобы направлять понимание аудиторией событий, политики или вопросов.

В процессе пропаганды угрозы от России американские политики и СМИ активно используют следующие дискурсивные фреймы для воздействия на когнитивные карты аудитории:

Явно связывают российское государство и государственные учреждения с «хакерскими группами». Несмотря на отсутствие конкретных доказательств, в официальных сообщениях США используются утвердительные формулировки для обвинения России. Агентство по кибербезопасности и защите инфраструктуры (CISA) рассматривает Россию как «государство-противник», описывая российское правительство как «участвующее в злонамеренной киберактивности с целью проведения широкомасштабного кибершпионажа, подавления определенной социальной и политической активности, кражи интеллектуальной собственности и нанесения ущерба региональным и международным противникам» [13]. В другом отчете утверждается, что многие российские государственные департаменты поддерживают кибератакующих, подразумевая, что Россия «злонамеренно планирует» или «организует запланированные атаки». Целью таких заявлений является конкретизация угрозы и придание ей целенаправленного характера [16].

Связывание киберугроз с вмешательством в американские выборы и внутреннюю политику, делая из России главного врага демократическим ценностям. Например, во время американских выборов 2016 года американские СМИ использовали сильные выражения, такие как «манипуляция голосами», «подрыв общественного мнения», «разрушение демократической системы», создавая чувство кризиса и подчеркивая эрозию демократии. Бывший заместитель советника по национальной безопасности Хуан С. Зарате (Juan C. Zarate) заявил: «Россияне провели организованную кампанию с целью подорвать американскую демократию и ослабить доверие людей к демократическому процессу и системе» [18]. В 2021 году США снова заявили, что Россия распространяет через Интернет ложную информацию для подрыва американских выборов 2022 года, действующий президент США Байден заявил: «Это является наглым нарушением нашего суверенитета» [14].

Описание того, как российские кибератаки могут повлиять на жизнь граждан, делая угрозу более ощутимой для населения. США обвиняют Россию в распространении ложной информации через социальные и медиаплатформы для влияния на восприятие американцев. В отчете Центра глобального взаимодействия

утверждается, что Россия использует официальные коммуникации, государственно финансируемые СМИ, сайты-посредники, а также множество фальшивых аккаунтов на основных социальных платформах для создания и усиления ложных нарративов, сбивая с толку американскую общественность и поощряя ее сомневаться в силе и законности американского правительства [10]. США также обвиняют российское правительство в использовании фишинговых атак для кражи информации американских граждан. В 2024 году Министерство юстиции США заявило, что смогло предотвратить хакерскую атаку России на правительственные учреждения, заместитель генерального прокурора Лиза Монако (Lisa Monaco) сказала: «Российское правительство осуществило этот план с целью украсть информацию американцев» [22].

Описание России как противника с передовыми кибернетическими способностями, особенно подчеркивая непредсказуемость и сложность предотвращения ее кибератак, и тем самым формируя ощущение технологической тревоги. В американских СМИ и официальных отчетах (например, GEC), атаки, якобы исходящие из России, обычно называют APT, то есть «продвинутая постоянная угроза» (advanced persistent threat), считая, что эти атаки осуществляются организациями хакеров с высоким уровнем технической компетенции, поддерживаемыми государством, имеющими долгосрочные цели и стратегическое планирование.

Подчеркивание того, что кибератаки России представляют прямую угрозу национальной безопасности, экономике и ключевым областям инфраструктуры. В информационном бюллетене, выпущенном администрацией Обамы в 2016 году под названием «Противодействие вредоносной кибердеятельности России», указывается, что киберугрозы представляют собой одну из самых серьезных экономических и национальных проблем безопасности, с которыми сталкиваются Соединенные Штаты сегодня [9]. В 2020 году в докладе «О международной безопасности в киберпространстве: новые модели для снижения рисков» Госдепартамента США отмечалось, что Россия и другие страны осуществляют через Сеть «разрушительные атаки на нашу критическую инфраструктуру», и такие действия рассматриваются как «значительная неядерная стратегическая атака» [2].

Описание так называемых кибератак из России как «имеющих глобальное воздействие», угрожающих мировому демократическому порядку. После масштабной кибератаки в Грузии в 2019 году госсекретарь США Майк Помпео заявил: «Это действие противоречит утверждениям России о том, что она является ответственным участником в киберпространстве и показывает, что российское ГРУ продолжает проводить безрассудные кибероперации против множества стран. Эти действия направлены на создание разделения, небезопасности и подрыв демократических институтов <…> Мы будем продолжать работать с международным сообществом для поддержания международной рамки ответственного поведения государств в киберпространстве» [19]. Интересно, что несмотря на обвинения России в качестве инициатора со стороны Грузии, США и многих других стран, ни одна из стран не предоставила прямых, общедоступных и поддающихся проверке материальных доказательств [15]. Это согласуется с предыдущими обвинениями США в адрес России. С помощью такого дискурса США представляются как защитники демократических учреждений, а Россия изображается как «злодей», подрывающий мировой демократический порядок. Эта двоичная противопоставляющая нарративная модель предназначена для того, чтобы вдохновлять общественную поддержку «справедливости» и враждебность к «угрозам».

Можно видеть, что процесс конструирования «киберугрозы из России» в США больше зависит от воображения, а не от оценки реальности, основываясь в целом на речевых действиях, которые связывают эту угрозу с национальным суверенитетом, социально-экономическим благополучием, демократическим порядком и другими областями, что отражает попытку США «гиперсекьюритизировать» киберпространство. Гиперсекьюритизация означает расширение за пределы обычных рисков и угроз, ее типичной особенностью является способность вызывать каскадные эффекты в других сферах [12].

На международном уровне США с помощью дискурсивного воздействия стремятся получить поддержку стран НАТО и Евросоюза, формируя международную коалицию для сдерживания России, а также направляют нейтральные страны к отказу от сотрудничества с Россией в области кибербезопасности, ослабляя таким образом ее международное влияние. США вместе с союзниками публично обвиняют Россию в кибератаках, например, в инцидентах с SolarWinds и NotPetya, пытаясь сформировать международное восприятие поведения России в выгодном для Штатов свете [23]. В этом аспекте США используют личный опыт европейских стран (например, атаку на украинскую электросеть), чтобы усилить резонанс с американским секьюритизационным нарративом.

Действия США по секьюритизации в киберпространстве в ответ на «российскую угрозу»

США через дискурс создали «российскую угрозу» как основной вызов киберпространства, сформировав комплекс нарративов о кибербезопасности в отношении России, который широко распространяется через правительственные и официальные заявления, отчеты специализированных агентств, СМИ, и таким образом получает широкое признание внутри страны и среди западных союзников, способствуя установлению соответствующих норм.

Используя российские кибератаки в качестве предлога, США продвинули законодательство по кибербезопасности, увеличили военный бюджет и инвестиции в технологическое развитие этой сферы, а также ввели санкции против России. Среди наиболее значимых можно выделить следующие: в 2017 году был принят «Закон о противодействии американским врагам через санкции» (CAATSA); в 2021 году президент Байден подписал исполнительный указ о санкциях против России, который предоставлял полномочия для наложения санкций на лиц, участвующих в деятельности, связанной с вмешательством в выборы, кибератаками и коррупцией; 1 марта 2022 года Сенат США единогласно принял «Акт об укреплении кибербезопасности США»; в проекте оборонного бюджета США на 2025 финансовый год инвестиции в киберпространственные операции составят 14,5 миллиарда долларов.

На международном уровне США различными способами объединяют союзников в области кибербезопасности против России, одновременно продвигая глобальные правила управления киберпространством и укрепляя кибербезопасность себя и своих союзников. США добились включения киберзащиты в коллективные оборонительные статьи НАТО, и в 2021 году НАТО опубликовало новую стратегию усиления киберзащиты, в которой ясно определены коллективные ответы на кибератаки России [20]. В сентябре 2019 года США и еще 27 стран подписали «Соглашение об ответственном поведении государств в киберпространстве» (Joint Statement on Advancing Responsible State Behavior in Cyberspace), в котором выражено стремление к совместным действиям

для «защиты свободного, открытого и безопасного киберпространства» и обеспечения того, чтобы «страны, поступающие противоположно, несли последствия за недобросовестное поведение в киберпространстве». Это заявление исключило Россию и было направлено на создание кибер-«НАТО», которое не только легитимизирует проведение агрессивных военных операций в киберпространстве, но и стремится объединить усилия различных сторон для осады и подавления стратегических соперников, включая Россию [25].

Заключение

В процессе секьюритизации киберпространства США сконструировали образ России как главной угрозы, чрезмерно преувеличивая масштабы и глубину киберугрозы, и использовали это для акцентирования права на применение силы и действия военных законов, что объективно способствовало милитаризации киберпространства и усилению гонки кибервооружений, углубляя уровень гиперсекьюритизации киберпространства. Российское правительство решительно отвергает необоснованные обвинения со стороны США и их союзников, неоднократно подчеркивая важность продвижения сотрудничества в области безопасности киберпространства. В этом контексте России следует укрепить построение цифрового суверенитета, чтобы обеспечить национальный автономный контроль и информационную безопасность в цифровом пространстве, а также совместно с такими странами, как Китай, способствовать созданию справедливой и равноправной системы развития и безопасности информационного киберпространства.

Литература

1. *Бартенев В.И.* Секьюритизация сферы содействия международному развитию: анализ политического дискурса // Вестник международных организаций: образование, наука, новая экономика. — 2011. — № 3. — С. 37–50.
2. *Зиновьева Е.С. Яникеева И.О.* Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе // Вестник Санкт-Петербургского университета. Международные отношения. — 2022. — № 2. — С. 158–173.
3. *Павлюченко А.А.* Цифровая дипломатия США сквозь призму теории секьюритизации в современной информационной экосистеме // Медиа в современном мире. 62-е Петербургские чтения: Сборник материалов ежегодного 62-го Международного научного форума. — СПб.: ООО «Медиапапир», 2023. — С. 249–251.
4. *Павлюченко А.А.* К вопросу о периодизации цифровой дипломатии США // Русская политология. — 2023. — № 3. — С. 69–81.
5. *Рамич М.С., Пискунов Д.А.* Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник РУДН. Серия: Международные отношения. — 2022. — № 2. — С. 238–255.
6. *Юдин Н.В.* Секьюритизация дискурса «мягкой силы» в российских международно-политических исследованиях // Коммуникации. Медиа. Дизайн. — 2019. — № 2. — С. 56–72.
7. *Юдин Н.В.* Связка «безопасность–развитие»: проблемы и перспективы инструментализации. Мировая экономика и международные отношения. — 2017. — № 9. — С. 16–23.
8. *Buzan B., Wæver O., De Wilde J.* Security: A new framework for analysis. Lynne Rienner Publishers, 1998.
9. FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment // The White House. — [Электронный ресурс]. — Режим доступа: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and (дата обращения: 11.10.2024).
10. GEC Special Report: Russia's Pillars of Disinformation and Propaganda // GEC. — [Электронный ресурс]. — Режим доступа: https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/ (дата обращения: 11.10.2024).

11. *Górka M.* Conceptualising securitisation in the field of cyber security policy // Journal of Modern Science. — 2023. — № 4. — P. 263–290.
12. *Lobato L.C., Kenkel K.M.* Discourses of cyberspace securitization in Brazil and in the United States // Revista Brasileira de Política Internacional. — 2015. — № 2. — P. 23–43.
13. Nation-State Cyber Actors // CISA. — [Электронный ресурс]. — Режим доступа: https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (дата обращения: 10.10.2024).
14. Remarks by President Biden at the Office of the Director of National Intelligence // The White House. — [Электронный ресурс]. — Режим доступа: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/27/ (дата обращения: 10.10.2024).
15. *Roguski P.* Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace — [Электронный ресурс]. — Режим доступа: https://www.justsecurity.org/69019/ (дата обращения: 30.10.2024).
16. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure // CISA. — [Электронный ресурс]. — Режим доступа: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a (дата обращения: 10.10.2024).
17. *Taureck R.* Securitization theory and securitization studies // Journal of International relations and Development. — 2006. — № 9. — С. 53–61.
18. The Cyber Attacks on Democracy// The Catalyst. — [Электронный ресурс]. — Режим доступа: https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy (дата обращения: 10.10.2024).
19. The United States Condemns Russian Cyber Attack Against the Country of Georgia // U.S. Department of State. — [Электронный ресурс]. — Режим доступа: https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (дата обращения: 12.10.2024).
20. The Cyber Defence // NATO. — [Электронный ресурс]. Режим доступа: https://www.nato.int/cps/de/natohq/topics_78170.htm (дата обращения: 30.10.2024).
21. U.S. formally accuses Russian hackers of political cyber-attacks // Reuters. — [Электронный ресурс]. — Режим доступа: https://www.reuters.com/article/idUSKCN12729B/ (дата обращения: 02.10.2024).
22. US says it disrupted Russian efforts to hack government agencies // Reuters. — [Электронный ресурс]. — Режим доступа: https://www.reuters.com/world/us/us-says-it-has-disrupted-russian-efforts-commit-computer-fraud-2024-10-03/ (дата обращения: 11.10.2024).
23. US, allied nations accuse Russia of cyberattacks against Ukraine and NATO // POLITICO. — [Электронный ресурс]. — Режим доступа: https://www.politico.com/news/2024/09/05/us-allied-nations-russia-cyberattacks-ukraine-nato-00177542 (дата обращения: 30.10.2024).
24. 张新宝, 许可. 网络空间主权的治理模式及其制度构建 // 中国社会科学. — 2016. — № 8. — С. 139–158.
25. 方兴东,钟祥铭. 算法认知战：俄乌冲突下舆论战的新范式 // 传媒观察. — 2022. — № 4. — С. 5–15.
26. 艾喜荣. 话语操控与安全化:一个理论分析框架 // 国际安全研究. — 2017. — № 3. — С. 57–78.