Каспийский регион: политика, экономика, культура. 2022. № 4 (73). С. 81–86.
THE CASPIAN REGION: Politics, Economics, Culture. 2022. Vol. 4 (73). P. 81–86.

Научная статья
УДК 316.4
doi: 10.54398/1818510X_2022_4_81

ЭЛЕКТОРАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ: КОНЦЕПТУАЛИЗАЦИЯ ПОНЯТИЯ И ЕГО МЕЖДУНАРОДНО-ПОЛИТИЧЕСКОЕ ИЗМЕРЕНИЕ

Артеев Сергей Павлович[1], Кардава Николай Вахтангович[2]
[1,2] Национальный исследовательский институт мировой экономики и международных отношений имени Е. М. Примакова РАН, Москва, Россия
[1]artsp7@yandex.ru, https://orcid.org/0000-0003-4335-2850
[2]kardava98@mail.ru, https://orcid.org/0000-0002-2609-9809

Аннотация. Цифровизация трансформирует электоральные процессы, в связи с этим актуализируется проблема электоральной кибербезопасности как новой проблемной зоны на стыке IT и политики. Возникает соответствующий вопрос: «Что такое «электоральная кибербезопасность» и в чём заключается её внутриполитическое и международно-политическое значение?» В исследовании используется информация из прессы, официальные документы и научные публикации по кибербезопасности. Компаративный метод применяется как основной. Внутриполитический аспект электоральной кибербезопасности связан с возникновением и усилением в результате выборов социально-политических разделений в обществе и с дестабилизацией политической системы государства. Такое происходит по всему миру. Примерами могут служить Франция, Великобритания, Белоруссия, Украина, Венесуэла, ЮАР. В статье концептуализируется понятие электоральной кибербезопасности и анализируются выборные кейсы США, Германии и России. Электоральная кибербезопасность понимается как способность государства защититься от негативного воздействия и обеспечить устойчивое функционирование информационно-коммуникационной инфраструктуры, задействованной в предвыборной кампании, процессе голосования и подведения его итогов, с целью обеспечения легитимности вновь сформированных выборных органов власти и устойчивости политической системы. С точки зрения национальных интересов России, проблема ЭКБ является стимулом для создания и распространения эффективной защищённой системы электронного голосования отечественной разработки. Необходимо сфокусироваться не столько на бесплодной дискуссии с Западом о нарушениях на выборах или их отсутствии, сколько на продвижении российских наработок в сфере электоральной кибербезопасности на постсоветском пространстве и по линии БРИКС.

Ключевые слова: электоральная кибербезопасность, информационная безопасность, США, Германия, Россия, выборы, легитимность, разделённые общества

Для цитирования: Артеев С. П., Кардава Н. В. Электоральная кибербезопасность: концептуализация понятия и его международно-политическое измерение // Каспийский регион: политика, экономика, культура. 2022. № 4 (73). С. 81–86. https://doi.org/10.54398/1818510X_2022_4_81.

ELECTORAL CYBERSECURITY AS A CONCEPT AND ITS INTERNATIONAL POLITICAL DIMENSION

Sergey P. Arteev[1], Nikolai V. Kardava[2]
[1,2] National Research Institute of World Economy and International Relations named after E. M. Primakov of the Russian Academy of Sciences, Moscow, Russia
[1] artsp7@yandex.ru, https://orcid.org/0000-0003-4335-2850
[2] kardava98@mail.ru, https://orcid.org/0000-0002-2609-9809

Abstract. Digitalization transforms electoral processes. In this connection, the problem of electoral cybersecurity as a new problem area at the intersection of IT and politics becomes relevant. The relevant question arises: What is "electoral cybersecurity" and what is its domestic and international political significance? The study uses information from the press, official documents, and academic publications on cybersecurity. The comparative method is used as the main method. The domestic political aspect of electoral cybersecurity is related to the emergence and intensification of socio-political divisions in society and the destabilization of the state's political system as a result of elections. This happens all over the world. Examples include France, Great Britain, Belarus, Ukraine, Venezuela and South Africa. The article conceptualizes the concept of electoral cybersecurity and analyzes the electoral cases of the United States, Germany and Russia. Electoral cybersecurity is understood as a state's ability to protect itself from the negative impact and ensure sustainable functioning of information and communication infrastructure involved in the pre-election campaign, voting process and summarizing its results, in order to ensure the legitimacy of the newly formed elected authorities and sustainability of the political system. From the point of view of the national interests of Russia, the problem of electoral cybersecurity is an incentive for the creation and distribution of an effective secure electronic voting system of domestic development. It is necessary to focus not so much on the fruitless discussion with the West about election violations or their absence, as on the promotion of Russian developments in the sphere of electoral cybersecurity in the post-Soviet space and through BRICS.

Keywords: electoral cybersecurity, information security, USA, Germany, Russia, elections, legitimacy, divided societies

For citation: Arteev S. P., Kardava N. V. Electoral cybersecurity as a concept and its international political dimension. *Kaspiyskiy region: politika, ekonomika, kultura* [The Caspian Region: Politics, Economics, Culture]. 2022, no. 4 (72), pp. 81–86. https://doi.org/10.54398/1818510X_2022_4_81.

Введение

Цифровизация превратилась в ключевой тренд современности. Экспансия цифровых технологий приобретает всеобщий характер. Такая «онлайнизация» всё большего количества сфер резко повышает значимость кибербезопасности, пренебрежение которой наносит существенный ущерб и способствует возникновению международно-политических осложнений и кризисов. Однако внедрение электронного голосования на выборах в ряде государств [14] и стремительное превращение Интернета в ключевую политическую площадку, существенно влияющую на электоральные предпочтения, ставят новые задачи не только перед IT-отраслью, экономический и политический вес которой растёт опережающими темпами много лет подряд (например фигуры Билла Гейтса [1] и Павла Дурова [24] сегодня воспринимаются уже не только через призму бизнеса, они приобретают политический капитал), но и перед академическим политологическим сообществом. Общий тренд таков, что с каждым выборным циклом возрастает влияние фактора Сети на итоги голосования. В связи с этим возникает соответствующий вопрос: «Что такое «электоральная кибербезопасность» и в чём заключается её внутриполитическое и международно-политическое значение?»

Внутриполитический аспект электоральной кибербезопасности связан с возникновением и усилением в результате выборов социально-политических разделений в обществе и с дестабилизацией политической системы государства. Такое происходит по всему миру. Примерами могут служить Франция, Великобритания, Белоруссия, Украина, Венесуэла, ЮАР.

Однако в наиболее явной и острой форме это произошло в США. Именно там президентские выборы в 2016 и 2020 гг. привели к существенному углублению существующих общественно-политических разломов. Сформировалась и актуализировалась устойчивая протестная повестка. Происходящая социальная трансформация сопровождается ревизией традиционных американских ценностей, что выражается в появлении движения BLM и др.

Сопряжение международных и внутриполитических факторов в условиях цифровизации электоральных процессов происходит быстрее и создаёт дополнительные риски. Социально-политические разделения в современных обществах получают дополнительный импульс в ходе выборов. И это главный вызов для демократических режимов, не имеющий простых решений.

Основная часть

Электоральная кибербезопасность в общественно-политическом и научном дискурсе

Проекты и инициативы по обеспечению международной кибербезопасности и шире – регулирования киберпространства – активно обсуждаются в экспертном и политическом сообществе со второй половины 1990-х гг. [3; 20]. Однако о каких-то общеобязательных правилах не удавалось договориться и в условиях относительно стабильной международной обстановки 2000-х гг., поэтому ожидать прорыва в условиях текущей фактически развернувшейся полицентричной холодной войны (Китай, Россия, Запад, другие центры силы) не приходится. Кибербезопасность как международный институт (практика) не работает. Наоборот, существует устойчивая тенденция к милитаризации киберпространства со стороны государств. США выделили Кибернетическое командование в качестве отдельной структуры в 2018 г., в Германии кибервойска появились в 2017 г., в России – в 2014 г. Последние события на Украине, как видно, уже способствуют этому.

На этом фоне происходит цифровизация электоральных процессов, осуществляемая в двух основных форматах – кооперативном (сотрудничество) и конфронтационном (противоборство). Существуют кейсы успешной электоральной цифровизации, которые интересны преимущественно своей технологической составляющей, и их изучают в политико-практическом и академическом плане в рамках передачи опыта. Именно такая модель электронных выборов сформировалась в Эстонии [18; 31] и Норвегии [28], т. е. в этом случае электоральная цифровизация интернационализирована и имеет кооперативный характер. Однако секьюритизация темы выборов в демократических государствах на фоне обострившихся международно-политических противоречий становится всё более распространенной.

Проблематика электоральной кибербезопасности базируется на стыке двух пластов политологического дискурса: первое направление – это информационная и кибербезопасность на национальном и международном уровнях [8; 13; 17; 31; 35; 37], второе – электронное голосование как часть цифровой демократии [23, 30; 34].

По нашему мнению, электоральная кибербезопасность (ЭКБ) – способность государства защититься от негативного внутреннего и внешнего воздействия и обеспечить устойчивое функционирование своей информационно-коммуникационной инфраструктуры, задействованной в предвыборной кампании, процессе голосования и подведения его итогов, с целью обеспечения легитимности вновь сформированных выборных органов власти и устойчивости политической системы.

ЭКБ обладает двухконтурной структурой – внутренний контур (политический) и внешний (технологический). Политический контур включает в себя проблематику электоральных процессов, международной безопасности, в том числе вопросы научно-технологического развития. Технологический контур ЭКБ основан на IT и смежных областях, что составляет его материальную основу.

Политическая значимость ЭКБ обусловлена жёсткой причинно-следственной связью с легитимностью. Отсутствие легитимности или слабая / неполная легитимность приводят к глубокому расколу в обществе между сторонниками разных политических платформ и резко сужают внутри- и внешнеполитические возможности для власти, что неизбежно приводит к экономическим трудностям и ухудшению социальной ситуации.

ЭКБ и кейс-стади

США, Германия и Россия в текущий период в международно-политическом плане представляют собой ярко выраженные конфронтационные кейсы. Эти страны были выбраны для анализа ЭКБ по нескольким причинам. Во-первых, именно эти государства, несмотря на существенные различия их политических систем и разные траектории развития технологий электронного голосования в исторической ретроспективе, сегодня являются мировыми лидерами в сфере внедрения цифровых технологий в электоральные процессы. Во-вторых, электоральные процессы в этих государствах как крупнейших политических субъектах являются интернационализированными, т. е. привлекают повышенное внимание международного сообщества. И длительное конфликтное российско-американское и российско-германское взаимодействие, когда каждая из сторон на официальном уровне позиционирует себя как демократия и подвергает жёсткой критике оппонента за пренебрежение к демократическим нормам и ценностям, резонансно проявляется и в теме выборов. Интернационализация выборных процессов в США, Германии и России по сравнению с другими государствами, в которых электоральные процессы цифровизированы, находится на более высоком уровне и отличается секьюритизированным характером.

Оптика анализа рассматриваемых кейсов будет отличаться, потому что факторы ЭКБ (внутриполитический конкурентный расклад между разными политическими силами, реагирование государственных институтов на вмешательство, законодательные превентивные инициативы) по-разному срабатывают в разных странах. Несмотря на то, что и США, и Германия относятся к государствам с высокой легалистской культурой, в первом случае (США после выборов 2016 и 2020 гг.) на международную и внутриполитическую обстановку в большей мере повлияло прокурорское расследование, во втором (ФРГ) – совокупная реакция государственных институтов. В случае с Россией на первый план выходит идентитарный вопрос (как часть внутриполитической борьбы за общественную поддержку и попытка привлечь на свою сторону не-западные страны), ЭКБ выступает в качестве одного из преломлений обретения РФ своей идентичности.

Таким образом, технологическая и международно-политическая составляющие делают именно эти государства наиболее репрезентативным для анализа темы ЭКБ. Ведь если механизм дистанционного голосования подвергается массированной критике со стороны общественности, то возникает вопрос о легитимности выбранных кандидатов и их способности воплощать в реальность свою политическую программу.

Кейс США

США являются глобальным лидером по ряду направлений, в том числе и в сфере высоких технологий. Именно поэтому они одними из первых создали обширную разветвлённую систему противодействия информационным и кибератакам [9; 25]. Однако это не уберегло их от электорально-кибернетических кризисов, как показали выборы президента США 2016 и 2020 гг., а также регулярные скандалы на выборах других уровней [19].

Выборы президента США 2016 г., на которых победу одержал кандидат от Республиканской партии Д. Трамп, вошли в число наиболее скандальных за всю историю Америки. Проигравшая сторона – Демократическая партия и сторонники её кандидата – обвинила во вмешательстве Россию. Суть Russiagate заключается в якобы компрометации кандидата от демократов Х. Клинтон с помощью взлома серверов [36] и обнародования конфиденциальной информации о её здоровье и якобы имевшем место аморальном поведении людей из её окружения, которые в случае победы демократов стали бы частью новой администрации 45-го президента США. В результате хакерской атаки и массированной негативной информационной кампании репутации Х. Клинтон мог быть нанесён существенный ущерб, и она проиграла выборы. В 2017–2019 гг. своё расследование Russiagate проводил специальный прокурор Р. Мюллер, который пришёл к выводу, что факт вмешательства российских властей в американские выборы достоверно установлен, однако информационная атака не оказала существенного влияниях на результаты выборов в ноябре, а сам избранный 45-й президент США или сотрудники его штаба не вступали в сговор с российскими властями [33].

«Дело о вмешательстве» постоянно находилось в актуальной политической повестке, создавая серьёзные сложности для реализации курса администрации 45-го президента. Пожалуй, впервые в истории Америки значительная часть общества стала подозревать президента в лоббировании интересов иностранного государства. По данным социологических исследований, американское общество оказалось разделённым по этому вопросу [32]. В результате, несмотря на очевидную межличностную симпатию Трампа и Путина, санкционное давление на РФ только усилилось.

Весь четырёхлетний президентский срок Д. Трампа оказался в тени возможного кризиса легитимности. Далее, в результате отказа Трампа признавать поражение на президентских выборах 2020 г. и затянувшегося разбирательства по поводу инцидентов при подсчёте результатов электронного голосования в ряде штатов [5] случился штурм Капитолия 6 января 2021 г. Электоральный раскол между сторонниками Байдена и Трампа приобрёл остро конфронтационный характер и наряду с другими кливажами создал угрозу делегитимации избранного 46-го президента Дж. Байдена. Американская политическая система выстояла, но также стало ясно, что демократические институты уязвимы для угроз нового типа – электоральных кибер- и информационных атак как на стадии предвыборной кампании, так и при подсчёте голосов и передаче властных полномочий.

Международно-политические последствия Russiagate ознаменовались упущенной возможностью предотвратить дальнейшую деградацию российско-американских отношений, прервать обоюдную санкционную спираль, возобновить полноценный диалог по стратегической стабильности. Между тем Россия последовательно отвергала все обвинения во вмешательстве в американские выборы.

Кейс Германии

Вопросы обеспечения кибербезопасности в политической сфере являются актуальными и для ФРГ. В преддверии выборов в Бундестаг 2021 г. Генпрокуратура Германии начала расследование кибератак хакерской группировки Ghostwriter на немецких политиков, за которой, по утверждению властей Германии, якобы стояла Россия [2]. По версии следствия ФРГ, группировка пыталась посредством рассылки фишинговых сообщений получить доступ к личным данным депутатов Бундестага и ландтагов (земельных парламентов), прежде всего от блока Христианско-демократического и Христианско-социального союзов (ХДС/ХСС) и Социал-демократической партии Германии (СДПГ).

Данные обвинения в адрес России, конечно, получили быструю реакцию в российском правительстве и других ведомствах. Например официальный представитель МИД РФ Мария Захарова заявила, что выдвигаемые Берлином обвинения в причастности России к хакерским атакам на депутатов федерального и земельных парламентов ФРГ бездоказательны и имеют явную внешнеполитическую подоплёку. По словам представителя МИДа, несмотря на неоднократные обращения России по дипломатическим каналам, Германия так и не предоставила никаких доказательств причастности РФ к этим атакам [2]. Ещё в 2017 г., когда аналогичным образом проходили выборы в Бундестаг, Председатель комитета Совета Федерации РФ по международным делам Константин Косачёв заявлял в ответ на обвинения немецких властей, что тезис о вмешательстве русских в выборы Германии сошёл на нет за несколько месяцев до дня голосования, поскольку исход волеизъявления граждан стал известен заблаговременно.

13 мая 2021 г. канцлер Германии Ангела Меркель заявляла, что в 2015 г. Россия проводила кибератаку на Бундестаг, в результате которой якобы были украдены документы из офиса канцлера в парламенте [4]. В сентябре 2021 г. за несколько дней до начала выборов в Бундестаг (выборы состоялись 26 сентября 2021 г.) представители МВД Германии заявили, что была проведена кибератака на один из серверов Интернет-сайта федерального ведомства статистики Германии Destatis [12]. Федеральное ведомство статистики Destatis занимается в том числе выборами и проводит подсчёт голосов. По информации МВД, «указаний на манипуляции с данными или их утечкой нет». Что касается инициаторов атаки, то они не были установлены.

Германия борется за электоральную кибербезопасность на нескольких взаимопересекающихся направлениях: повышение IT-компетенций депутатов и чиновников, создание институционального кордона, принятие и внедрение в практику соответствующих законодательных инициатив.

Все 43 партии, допущенные к выборам, были приглашены на консультации [10]. Однако это не решает проблему фейков. Так, ложная информация постоянно циркулировала в “Telegram”, “YouTube”, “Facebook” и “Twitter”.

ФРГ предпринимает значительные усилия для обеспечения кибербезопасности в различных сферах. В Германии создана целая сеть государственных ведомств и компаний, которые занимаются вопросами обеспечения кибербезопасности и регулирования киберпространства. В частности, ФРГ, так же как США и Великобритания, использует комбинирование кибероперациий с радиоэлектронной разведкой [6].

В 2009 г. Германия утвердила Закон об укреплении безопасности в сфере информационных технологий Федерации. В начале 2011 г. была принята «Стратегия кибербезопасности для Германии», которая обновляется каждые пять лет (2016, 2021) [38].

Кейс Германии свидетельствует о росте напряжённости в международном общении между Западом и не-Западом. С точки зрения российско-германских отношений обвинения приводят к взаимному отчуждению и снижению контактов на самых разных уровнях, что препятствует обмену опытом в сфере ЭКБ.

Кейс России

Вопрос о вмешательстве в выборы в РФ актуализировался в 2010-е гг., и его значимость в официальном политическом дискурсе росла параллельного иностранного влияния постепенно стал постоянным пунктом официальной российской политической повестки. Борьба с таким воздействием проявляется в нескольких формах, наиболее заметные из которых:

- доклады МИД РФ о правах человека, издающиеся с 2011 г. [15] (сравни: ежегодные доклады Госдепа США Country Reports on Human Rights Practices [39], выходят с 1977 г.);
- деятельность Временной комиссии Совета Федерации [16];
- «Закон об иноагентах» [21];
- законодательство о нежелательных организациях [22].

Непосредственно по электоральному аспекту Россия обвиняет Запад во вмешательстве в выборы президента страны 2018 г. [11] и выборах в Государственную думу 2021 г. [7]. Однако в отличие от США и Германии обращает на себя внимание иной способ

реагирования. Российские правоохранительные органы и специальные службы слабо представлены в медийном поле, не обнародуются развернутые технические данные о вмешательстве, не детализируются механизмы вмешательства. Экспертный уровень именно по ЭКБ с точки зрения публичности также представлен слабо.

Российский электоральный кейс отличает реактивность по отношению к Западу. Конфронтация с Западом является одним из путей, благодаря которому формируется собственная российская модель развития, хотя конкретизированный, эмпирически сформулированный и понятный большинству населения образ будущего по-прежнему отсутствует. Электоральная кибербезопасность в российском случае выполняет прежде всего идентитарную функцию, является своеобразным маркером деления на «своих» и «чужих». Тем не менее, нельзя не признать и успехи в цифровизации электоральных процессов РФ, которые могут рассматриваться и как внешнеполитический ресурс.

Выводы

Электоральная кибербезопасность – это политический фактор, который через легитимность выборов влияет на международную ситуацию и обстановку внутри государства существенным образом. Очевидно, что магистральная линия на «интернетизацию» политических процессов, в том числе выборов, будет нарастать с каждым годом. Это поднимает множество вопросов, которые могут быть успешно решены, если будут задействованы сразу несколько уровней: персональный (компетентность в сфере цифровых технологий как новая грамотность), национальный (понятные, контролируемые независимыми инстанциями способы верификации подсчёта электронных голосов), международный (определение на межгосударственном уровне принципов взаимодействия и ненападения на критическую IT-инфраструктуру), глобальный (создание международного режима информационной и кибербезопасности через подписание обязывающих международных конвенций в сфере кибербезопасности, наделение институций наподобие Международного союза электросвязи ООН директивными наднациональными полномочиями).

Кейсы США, Германии и России демонстрируют, что ЭКБ становится одним из основных факторов риска в двустороннем межгосударственном взаимодействии. Окно возможностей для решения проблемы на международном уровне сохранялось, несмотря на накопленный груз взаимных претензий. Однако мощная конфронтация между Россией и Западом после начала реализации силового сценария на Украине в конце февраля 2022 г., похоже, отодвигает этот процесс на неопределённый срок.

С точки зрения национальных интересов России, проблема ЭКБ является стимулом для создания и распространения эффективной защищённой системы электронного голосования отечественной разработки. Необходимо сфокусироваться не столько на бесплодной дискуссии с Западом о нарушениях на выборах или их отсутствии, сколько на продвижении российских наработок в сфере ЭКБ на постсоветском пространстве и по линии БРИКС. Внедрение общих платформ для электронного голосования взаимно укрепит легитимность политических систем множества незападных стран и сделает политические процессы более стабильными, предсказуемыми, ослабит социально-политические размежевания.

Список литературы

1. Билл Гейтс назвал поводом для беспокойства недоверие к правительствам. – 25.12.2021. – URL: https://quote.rbc.ru/news/short_article/61c741e09a7947cce011bfa9 (дата обращения: 20.06.2022).
2. Власти Германии начали расследование кибератак в преддверии выборов в Бундестаг. (Spiegel). – URL: https://tass.ru/mezhdunarodnaya-panorama/12344247 (дата обращения: 20.06.2022).
3. Верхелст, Э. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС / Э. Верхелст, Я. Ваутерс // Вестник международных организаций. – 2020. – Т. 15, № 2. – С. 141–172. doi: 10.17323/1996-7845-2020-02-07.
4. Германия расследует новую хакерскую атаку со стороны России перед выборами в бундестаг. – 09.09.2021. – URL: https://theins.ru/news/244924 (дата обращения: 20.06.2022).
5. Если Трамп не сдается, его уничтожат. – 22.12.2020. – URL: https://www.kommersant.ru/doc/4626711 (дата обращения: 20.06.2022).
6. Ждан, О. Е. Современная киберстратегия Европейского союза: цели, задачи, потенциальные противники / О. Е. Ждан. – 2017. – URL: https://isca.kz/ru/analytics-ru/1990 (дата обращения: 24.12.2021).
7. Захарова заявила о вмешательстве в выборы в РФ со стороны других стран. – 16.09.2021. – URL: https://rg.ru/2021/09/16/zaharova-zaiavila-o-vmeshatelstve-v-vybory-v-rf-so-storony-drugih-stran.html (дата обращения: 20.06.2022).
8. Зиновьева, Е. С. Международная информационная безопасность / Е. С. Зиновьева. – Москва : МГИМО-Университет, 2013. – 194 с.
9. Карасев, П. Новые стратегии США в области кибербезопасности / П. Карасев. – 15.11.2018. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/novye-strategii-ssha-v-oblasti-kiberbezopasnosti/ (дата обращения: 20.06.2022).
10. К выборам в бундестаг допущены 44 малые партии. – 09.07.2021. – URL: https://www.dw.com/ru/k-vyboram-v-bundestag-dopushheny-44-malyh-partii/a-58222572 (дата обращения: 20.06.2022).
11. Комиссии известно о мышиной возне агентов влияния. – 05.03.2018. – URL: https://www.kommersant.ru/doc/3566544 (дата обращения: 20.06.2022),
12. МВД ФРГ подтвердил кибератаку на сайт ведомства статистики, пока неизвестно, кто ее организовал. – URL: https://www.swissinfo.ch/rus/46975328 (дата обращения: 20.06.2022).
13. Овчинский, В. С. Россия и вызовы цифровой среды: рабочая тетрадь / В. С. Овчинский, Е. С. Ларина, С. А. Кулик. – Москва : Спецкнига, 2014. – 40 с.
14. Опыт проведения электронного голосования в мире. – 25.06.2020. – URL: https://ria.ru/20200625/1573357895.html (дата обращения: 20.06.2022).
15. О ситуации с правами человека в отдельных странах. Доклад МИД РФ. – 08.07.2021. – URL: https://mid.ru/ru/foreign_policy/humanitarian_cooperation/1426290/ (дата обращения: 20.06.2022).
16. Постановление № 172-СФ от 14.06.2017 «О создании Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации». – URL: http://council.gov.ru/activity/documents/81373/ (дата обращения: 20.06.2022).
17. Ромашкина, Н. П. Проблема международной информационной безопасности в ООН / Н. П. Ромашкина // Мировая экономика и международные отношения. – 2020. – № 12. – С. 25–32. doi: 10.20542/0131-2227-2020-64-12-25-32.
18. Ручкин, А. В. Электронное голосование на выборах в органы государственной власти и местного самоуправления: опыт Эстонии / А. В. Ручкин, А. А. Чижов // Вопросы управления. – 2018. – № 5. – С. 54–60.
19. Системы голосования Dominion: канадская компания в центре заявлений о мошенничестве на выборах в США. – 09.11.2020. – URL: https://ru.technocracy.news/729666671 (дата обращения: 20.06.2022).
20. Угроза фрагментации: добьется ли мировое сообщество безопасности Сети. – 19.11.2018. – URL: https://www.rbc.ru/opinions/technology_and_media/19/11/2018/5bf12c579a79477c7ba79152 (дата обращения: 20.06.2022).
21. Федеральный закон от 20.07.2012 г. № 121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента». – URL: http://www.kremlin.ru/acts/bank/35748 (дата обращения: 27.12.2021).

22. Федеральный закон от 28.12.2012 № 272-ФЗ (ред. от 14.03.2022) «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» (с изм. и доп., вступ. в силу с 15.03.2022). – URL: https://legalacts.ru/doc/federalnyi-zakon-ot-28122012-n-272-fz-o/ (дата обращения: 20.06.2022).

23. Федоров, В. И. Эволюция электронного голосования в России: проблемы классификации и периодизации / В. И. Федоров, Д. А. Ежов // Вестник Московского государственного областного университета. – 2021. – № 1. – С. 146–162. doi: 10.18384/2224-0209-2021-1-1055.

24. Человек с харизмой: может ли Павел Дуров стать политическим лидером. – 03.05.2018. – URL: https://www.forbes.ru/milliardery/360967-chelovek-s-harizmoy-mozhet-li-pavel-durov-stat-politicheskim-liderom (дата обращения: 20.06.2022).

25. Шариков, П. А. Информационный суверенитет и вмешательство во внутренние дела в российско-американских отношениях / П. А. Шариков // Международные процессы. – 2018. – Т. 16, № 3. – С. 170–188. doi: 10.17994/IT.2018.16.3.54.10.

26. Buzan, B. Security: A New Framework for Analysis / B. Buzan, O. Waever, J. de Wilde. – London : Lynne Rienner, 1998. – 239 p.

27. Electronic voting. – Britannica. – URL: https://www.britannica.com/topic/electronic-voting (дата обращения: 27.12.2021).

28. Electronic voting – challenges and opportunities : report / Norway's Ministry of Local Government and Regional Development. – Oslo, 2006. – 153 p.

29. Finnemore, M. Constructing Norms for Global Cybersecurity / M. Finnemore, D. Hollis // American Journal of International Law. – 2016. – №. 110 (3). – P. 425–479. doi: 10.1017/S0002930000016894.

30. Goldsmith, B. Implementing and Overseeing Electronic Voting and Counting Technologies / B. Goldsmith, H. Ruthrauff. – Washington, D.C. : The National Democratic Institute, 2013. – 310 p. – New Delhi: Veta Boos, 2010. – 230 p.

31. Krivonosova, I. The forgotten election administrator of internet voting: lessons from Estonia / I. Krivonosova // Policy Studies. – July 2021. doi: 10.1080/01442872.2021.1958179.

32. On Russia's Election Meddling, Americans Are Divided. – 20.12.2016. – U.S. News and World Report. – URL: https://www.usnews.com/news/politics/articles/2016-12-20/americans-divided-on-russian-interference-in-election (дата обращения: 24.12.2021).

33. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Special Counsel Robert S. Mueller : in 3 vol. – Washington, D.C., March 2019. – Vol. 3. – P. 4–10, 157.

34. Ronchi, A. e-Democracy: Toward a New Model of (Inter)active Society / A. Ronchi. – Berlin : Springer; 2019. – 242 p. doi: 10.1007/978-3-030-01596-1.

35. Routledge Handbook of International Cybersecurity / ed. by E. Tikk, M. Kerttunen. – New York : Routledge, 2020. – 416 p.

36. Russian government hackers penetrated DNC, stole opposition research on Trump. – June 14 2016. – Washington Post. – URL: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html (дата обращения: 27.12.2021).

37. The Oxford Handbook of Cyber Security / ed. by P. Cornish. – Oxford : Oxford University Press, 2021. – 880 p.

38. Cybersicherheitsstrategie für Deutschland. August 2021. – Bundesministerium des Innern und für Heimat. – URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=0D14C65A47A8BD384B0E965F1B2C7510.1_cid364?__blob=publicationFile&v=1 (дата обращения: 20.05.2022).

39. 2020 Country Reports on Human Rights Practices. – March 30, 2021. – U. S. Department of State. – URL: https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/ (дата обращения: 27.12.2021).

References

1. *Bill Geyts nazval povodom dlya bespokoystva nedoverie k pravitelstvam*, 25.12.2021 [Bill Gates called distrust of governments a cause for concern]. Available at: https://mid.ru/ru/foreign_policy/humanitarian_cooperation/1426290/ (accessed: 20.05.2022).

2. *Vlasti Germanii nachali rassledovanie kiberatak v preddverii vyborov v Bundestag (Spiegel)* [German authorities have launched an investigation into cyberattacks ahead of Bundestag elections]. Available at: https://tass.ru/mezhdunarodnaya-panorama/12344247 (accessed: 20.05.2022)

3. Verhelst, Ye., Vauters, Ya. Globalnoe upravlenie v sfere kiberbezopasnosti: vzglyad s pozitsii mezhdunarodnogo prava i prava ES [Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives]. *Vestnik mezhdunarodnykh organizatsiy* [International Organisations Research Journal]. 2020, vol. 15, no. 2, pp. 141–172. doi: 10.17323/1996-7845-2020-02-07.

4. *Germaniya rassleduet novuyu khakerskuyu ataku so storony Rossii pered vyborami v bundestag, 09.09.2021* [Germany investigates new hacker attack by Russia ahead of Bundestag elections]. Available at: https://theins.ru/news/244924 (accessed: 20.05.2022).

5. *Esli Tramp ne sdaetsya, ego unichtozhat, 22.12.2020* [If Trump does not surrender, he is destroyed]. Available at: https://www.kommersant.ru/doc/4626711 (accessed: 20.05.2022).

6. Zhdan, O. E. *Sovremennaya kiberstrategiya Evropeyskogo soyuza: tseli, zadachi, potentsialnye protivniki*. 2017. Available at: https://isca.kz/ru/analytics-ru/1990 (accessed: 24.12.2021).

7. *Zakharova zayavila o vmeshatelstve v vybory v RF so storony drugikh stran*, 16.09.2021 [Zakharova announced interference in the elections in the Russian Federation by other countries]. Available at: https://rg.ru/2021/09/16/zaharova-zaiavila-o-vmeshatelstve-v-vybory-v-rf-so-storony-drugih-stran.html (accessed: 20.05.2022).

8. Zinoveva, E. S. *Mezhdunarodnaya informatsionnaya bezopasnost* [International information security]. Moscow: MGIMO-Universitet; 2013, 194 p.

9. Karasev, P. *Novye strategii SSHA v oblasti kiberbezopasnosti*, 15.11.2018 [New US Cybersecurity Strategies]. Available at: https://russiancouncil.ru/analytics-and-comments/analytics/novye-strategii-ssha-v-oblasti-kiberbezopasnosti/ (accessed: 20.05.2022).

10. *K vyboram v bundestag dopushcheny 44 malye partii*, 09.07.2021 [44 small parties admitted to elections to the Bundestag]. Available at: https://www.dw.com/ru/k-vyboram-v-bundestag-dopushheny-44-malyh-partii/a-58222572 (accessed: 20.05.2022).

11. *"Komissii izvestno o myshinoy vozne agentov vliyaniya"*, 05.03.2018 ["The commission is aware of the mouse fuss of agents of influence"]. Available at: https://www.kommersant.ru/doc/3566544 (accessed: 20.05.2022).

12. *MVD FRG podtverdil kiberataku na sayt vedomstva statistiki, poka neizvestno, kto ee organizoval*, 2021 g. [The Ministry of Internal Affairs of Germany confirmed a cyber attack on the website of the statistics department, it is still unknown who organized it, 2021]. Available at: https://www.swissinfo.ch/rus/46975328 (accessed: 20.05.2022).

13. Ovchinsky, V. S., Larina, E. S., Kulik, S. A. *Rossiya i vyzovy tsifrovoy sredy: rabochaya tetrad* [Russia and the Challenges of the Digital Environment: Workbook]. Moscow: Special Book; 2014, 40 p.

14. *Opyt provedeniya elektronnogo golosovaniya v mire*, 25.06.2020 [Experience of electronic voting in the world]. Available at: https://ria.ru/20200625/1573357895.html (accessed: 20.05.2022).

15. Situacii s pravami cheloveka v otdelnykh stranah. Doklad MID RF, 08.07.2021 [On the human rights situation in individual countries. Report of the Ministry of Foreign Affairs of the Russian Federation]. Available at: https://mid.ru/ru/foreign_policy/humanitarian_cooperation/1426290/ (accessed: 20.05.2022).

16. *Postanovlenie № 172-SF ot 14.06.2017 "O sozdanii Vremennoy komissii Soveta Federatsii po zashchite gosudarstvennogo suvereniteta i predotvrashcheniyu vmeshatelstva vo vnutrennie dela Rossiyskoy Federatsii"* [Decree No. 172-SF dated June 14, 2017 "On the establishment of an Interim Commission of the Federation Council for the protection of state sovereignty and the prevention of interference in the internal affairs of the Russian Federation"]. Available at: http://council.gov.ru/activity/documents/81373/ (accessed: 20.05.2022).

17. Romashkina, N. P. Problema mezhdunarodnoy informatsionnoy bezopasnosti v OON [The problem of international information security in the UN]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya* [World Economy and International Relations]. 2020, no. 12, pp. 25–32. doi: 10.20542/0131-2227-2020-64-12-25-32.

18. Ruchkin, A. V., Chizhov, A. A. Elektronnoe golosovanie na vyborakh v organy gosudarstvennoy vlasti i mestnogo samoupravleniya: opyt Estonii [E-Voting in Elections to State Authorities and Local Self-Government: Estonian Experience]. *Voprosy upravleniya* [Management Issues]. 2018, no. 5, pp. 54–60.

19. *Sistemy golosovaniya Dominion: kanadskaya kompaniya v tsentre zayavleniy o moshennichestve na vyborakh v SSHA*, 09.11.2020 [Dominion Voting Systems: Canadian company at the center of US election fraud allegations]. Available at: https://ru.technocracy.news/729666671 (accessed: 20.05.2022).

20. *Ugroza fragmentatsii: dobetsya li mirovoe soobshchestvo bezopasnosti Seti*, 19.11.2018 [The Threat of Fragmentation: Will the Global Community Achieve Network Security?]. Available at: https://www.rbc.ru/opinions/technology_and_media/19/11/2018/5bf12c579a79477c7ba79152 (accessed: 20.05.2022).

21. *Federalnyy zakon ot 20.07.2012 g. № 121-FZ "O vnesenii izmeneniy v otdelnye zakonodatelnye akty Rossiyskoy Federatsii v chasti regulirovaniya deyatelnosti nekommercheskikh organizatsiy, vypolnyayushchikh funktsii inostrannogo agenta"* [Federal Law No. 121-FZ of July 20, 2012 "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of the Activities of Non-Commercial Organizations Performing the Functions of a Foreign Agent"]. Available at: http://www.kremlin.ru/acts/bank/35748 (accessed: 27.12.2021).

22. *Federalnyy zakon ot 28.12.2012 N 272-FZ (red. ot 14.03.2022) "O merakh vozdeystviya na lits, prichastnykh k narusheniyam osnovopolagayushchikh prav i svobod cheloveka, prav i svobod grazhdan Rossiyskoy Federatsii" (s izm. i dop., vstup. v silu s 15.03.2022)* [Federal Law No. 272-FZ of December 28, 2012 (as amended on March 14, 2022) "On Measures to Influence Persons Involved in Violations of Fundamental Human Rights and Freedoms, Rights and Freedoms of Citizens of the Russian Federation" (as amended and supplemented, entry. in force from 15.03.2022)]. Available at: https://legalacts.ru/doc/federalnyi-zakon-ot-28122012-n-272-fz-o/ (accessed: 30.05.2022).

23. Fedorov, V. I., Ezhov, D. A. Evolyutsiya elektronnogo golosovaniya v Rossii: problemy klassifikatsii i periodizatsii [Evolution of Electronic Voting in Russia: Problems of Classification and Periodization]. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta* [Bulletin of the Moscow State Regional University]. 2021, no. 1, pp. 146–162. doi: 10.18384/2224-0209-2021-1-1055.

24. *Chelovek s kharizmoy: mozhet li Pavel Durov stat politicheskim liderom*, 03.05.2018 [A man with charisma: can Pavel Durov become a political leader]. Available at: https://www.forbes.ru/milliardery/360967-chelovek-s-harizmoy-mozhet-li-pavel-durov-stat-politicheskim-liderom (accessed: 20.05.2022).

25. Sharikov, P. A. Informatsionnyy suverenitet i vmeshatelstvo vo vnutrennie dela v rossiysko-amerikanskikh otnosheniyak. [Information sovereignty and interference in internal affairs in Russian-American relations]. *Mezhdunarodnye protsessy* [International processes]. 2018, vol. 16, no. 3, pp. 170–188. doi: 10.17994/IT.2018.16.3.54.10.

26. Buzan, B., Waever, O., de Wilde, J. *Security: A New Framework for Analysis*. London: Lynne Rienner; 1998, 239 p.

27. *Electronic voting. Britannica*. Available at: https://www.britannica.com/topic/electronic-voting (accessed: 27.12.2021).

28. *Electronic voting – challenges and opportunities: report / Norway's Ministry of Local Government and Regional Development*. Oslo: 2006, 153 p.

29. Finnemore M., Hollis D. Constructing Norms for Global Cybersecurity. *American Journal of International Law*. 2016, no. 110 (3), pp. 425–479. doi: 10.1017/S0002930000016894.

30. Goldsmith, B., Ruthrauff, H. *Implementing and Overseeing Electronic Voting and Counting Technologies*. Washington, D.C.: The National Democratic Institute; 2013, 310 p.; New Delhi: Veta Boos; 2010, 230 p.

31. Krivonosova, I. The forgotten election administrator of internet voting: lessons from Estonia. *Policy Studies*. July 2021. doi: 10.1080/01442872.2021.1958179.

32. On Russia's Election Meddling, Americans Are Divided. 20.12.2016. *U.S. News and World Report*. Available at: https://www.usnews.com/news/politics/articles/2016-12-20/americans-divided-on-russian-interference-in-election (accessed: 24.12.2021).

33. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Special Counsel Robert S. Mueller*. Washington, D.C. March 2019, vol. 3, pp. 4–10, 157.

34. Ronchi, A. *e-Democracy: Toward a New Model of (Inter)active Society*. Berlin: Springer; 2019, 242 p. doi: 10.1007/978-3-030-01596-1.

35. *Routledge Handbook of International Cybersecurity*. Ed. by E. Tikk, M. Kerttunen. New York: Routledge; 2020, 416 p.

36. *Russian government hackers penetrated DNC, stole opposition research on Trump*. June 14 2016. Available at: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html (accessed: 27.12.2021).

37. *The Oxford Handbook of Cyber Security*. Ed. by P. Cornish. Oxford: Oxford University Press; 2021, 880 p.

38. Cybersicherheitsstrategie für Deutschland. August 2021. *Bundesministerium des Innern und für Heimat*. Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=0D14C65A47A8BD384B0E965F1B2C7510.1_cid364?__blob=publicationFile&v=1 (accessed: 20.05.2022).

39. *2020 Country Reports on Human Rights Practices*. March 30, 2021. Available at: https://www.state.gov/reports/2020-country-reports-on-human-rights-practices/ (accessed: 27.12.2021).

Информация об авторах
Артеев С. П. – кандидат политических наук, научный сотрудник;
Кардава Н. В. – младший научный сотрудник.

Information about the authors
Arteev S. P. – Candidate of Political Sciences, Research Fellow;
Kardava N. V. – Junior Research Fellow.

Вклад авторов
Артеев С. П. – общая концепция, кейсы США и России, итоговые выводы;
Кардава Н. В. – кейс Германии, итоговые выводы.

Contribution of the authors
Arteev S. P. – general concept, cases of the USA and Russia, conclusion;
Kardava N. V. – the case of Germany, conclusion.

Статья поступила в редакцию 26.08.2022; одобрена после рецензирования 12.09.2022; принята к публикации 30.09.2022.

The article was submitted 26.08.2022; approved after reviewing 12.09.2022; accepted for publication 30.09.2022.