



МЕЖПАРЛАМЕНТСКАЯ АССАМБЛЕЯ
ГОСУДАРСТВ – УЧАСТНИКОВ
СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

ДЕМОКРАТИЯ, ВЫБОРЫ, ПАРЛАМЕНТАРИЗМ

Безопасность избирательного процесса



МЕЖПАРЛАМЕНТСКАЯ АССАМБЛЕЯ
ГОСУДАРСТВ – УЧАСТНИКОВ
СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

ДЕМОКРАТИЯ, ВЫБОРЫ, ПАРЛАМЕНТАРИЗМ

БЕЗОПАСНОСТЬ ИЗБИРАТЕЛЬНОГО ПРОЦЕССА

Санкт-Петербург
2023

УДК 324
ББК 67.400.8
Б40

Серия основана в 2021 году

Руководитель издательского проекта «Демократия, выборы, парламентаризм»:
Генеральный секретарь — руководитель Секретариата Совета МПА СНГ
Д. А. Кобицкий

Авторы:

А. С. Бояшов, И. И. Мушкет, О. Н. Лешенюк, Р. А. Амбурцев,
С. Г. Караваев, А. Н. Ксендзов

Рецензенты:

С. С. Молдабаев — доктор юридических наук, профессор, руководитель
общественного объединения «Центр устойчивого развития Ochaq»;
И. А. Краснов — кандидат исторических наук, начальник редакционно-
издательского отдела информационно-издательского управления Секретариата
Совета МПА СНГ.

Безопасность избирательного процесса / А. С. Бояшов,
Б40 И. И. Мушкет, О. Н. Лешенюк [и др.]. — Санкт-Петербург : Секретариат Совета МПА СНГ, 2023. — 96 с. — (Демократия, выборы, парламентаризм).

ISBN 978-5-86857-045-2

Монография посвящена актуальным проблемам обеспечения безопасности электоральных процессов в странах Содружества Независимых Государств. Авторы рассматривают различные формы иностранного вмешательства в выборы, анализируют новые вызовы, связанные с развитием информационно-коммуникационных технологий. В книге также дана высокая оценка роли Конвенции о стандартах демократических выборов, избирательных прав и свобод в государствах — участниках Содружества Независимых Государств (принята в 2002 г.) в совершенствовании избирательных систем.

УДК 324
ББК 67.400.8

ISBN 978-5-86857-045-2

© Секретариат Совета МПА СНГ, 2023
© Авторский коллектив, 2023

Введение

В чем состоит особенность обеспечения безопасности избирательного процесса? Авторы этой книги исследуют безопасность избирательного процесса как электоральную безопасность, то есть состояние защищенности личности, общества и государства от угроз в ходе организации, подготовки и проведения итогов выборов и референдумов¹. Избирательные процессы — определяющий фактор развития. В условиях мира выборы и референдумы выполняют функцию воспроизводства политико-правовых систем. В условиях войны избирательные процессы — ключевой этап эскалации либо завершения конфликта. В мире протекают как минимум 65 крупных военных конфликтов, и каждый из них связан с избирательными процессами. Растет доля политических электоральных технологий в проецировании военной силы: сегодня лишь 20% всех мер, используемых для достижения военных целей, являются военными². Проецирование «мягкой силы» с целью влияния на развитие — неотъемлемый элемент современных международных отношений. Но проецирование «мягкой силы» в отношении избирательных процессов становится грубым вмешательством с целью контроля за развитием. Развитие социальных техно-

¹ Лешенюк О. Н. Укрепление электоральной безопасности через синхронизацию межпарламентского компонента Союзного государства, ОДКБ, СНГ // Региональная политика, политическая география и геополитика. История и современность: материалы международной научной конференции, посвященной 20-летию кафедры региональной политики и политической географии СПбГУ / под ред. Н. М. Михеевой, Н. В. Каледина. — Санкт-Петербург: Издательство ВВМ, 2022. — С. 719–725; Бояшов А. С. Президент в Послании неслучайно обратил внимание на электоральную безопасность // СБ. Беларусь сегодня. — 2023. — 24 мая. URL: <https://www.sb.by/articles/prezident-v-poslanii-nesluchayno-obratil-vnimanie-na-elektoralnuyu-bezopasnost-ekspert-iz-bgu.html>.

² Герасимов В. В. Основные тенденции развития форм и способов применения ВС, актуальные задачи военной науки по их совершенствованию: доклад на общем собрании Академии военных наук, 2013. URL: <https://vpk-news.ru/articles/14632>.

логий вмешательства позволяет конструировать электоральные противоречия внутри государств. По этим причинам электоральная безопасность требует особого концептуального осмысления.

Обеспечение электоральной безопасности не сводится к противодействию иностранному вмешательству. Во-первых, вмешательство в избирательные процессы может исходить от внутренних источников угроз. Во-вторых, внешнее вмешательство, как правило, «паразитирует» на внутренних проблемах, внутренние и внешние источники угроз — звенья одной цепи. В-третьих, самое опасное, что повестка иностранного вмешательства — это «троянский конь» для электоральных процессов. Вмешательство само по себе (например, кража личных данных зарегистрированных избирателей) не является конечной целью внешних субъектов. Настоящая цель состоит в том, чтобы тиражирование иностранного вмешательства стало *системой координат* внутренней политической борьбы. В таких условиях в основе политической конкуренции лежит апелляция к внешнему вмешательству, а не внутреннее развитие. Кандидаты в парламент, во всенародное собрание или на пост президента апеллируют к внешнему вмешательству, косвенно признавая, что система уязвима. Это снижает доверие населения к государственным институтам, ведь именно государственные институты обязаны обеспечить безопасность волеизъявления граждан. Как следствие отсутствия доверия снижается участие граждан в государственных делах, только в этот момент государство действительно становится уязвимым для внешнего вмешательства.

Актуальность разработки концепции электоральной безопасности обусловлена развитием сложных сетевых форм иностранного вмешательства в выборы и референдумы, в том числе с участием международных организаций³. Современное вмешательство больше не осуществляется в день выборов, его все сложнее отличить от международного сотрудничества. Избирательные процессы усложняются: появляются такие формы свободного волеизъявления и признания выборов, как всенародные собрания, национальные курултай. Вмешательство в элек-

³ Boyashov A. Network Governance of the UN Human Rights Council. Diplomatic, Institutional, and Organizational Actors. — New York: Routledge, 2022. — 180 p.

торальный суверенитет, в свою очередь, представляется лишь крайней формой подрыва электоральной безопасности, базирующейся на внешних угрозах. В этом случае вмешательство в электоральный суверенитет необходимо трактовать как акт агрессии со всеми вытекающими последствиями.

Ускорение передачи информации «расширяет» процесс обеспечения безопасности избирательного процесса по времени, участникам и объектам. Во-первых, безопасность избирательного процесса предполагает обеспечение состояния защищенности не только во время подготовки и организации голосования на избирательных участках, но и сразу после подведения итогов, а также во время электорального «затишья». Во-вторых, под обеспечением электоральной безопасности подразумевается защита не только граждан и организаторов избирательных процессов, но и иных вовлеченных лиц, включая наблюдателей, СМИ, а также лиц, участвующих в повышении квалификации членов избирательных комиссий. В-третьих, состояние электоральной защищенности обеспечено в полном объеме лишь тогда, когда обеспечена безопасность электоральной инфраструктуры, включая информационные ресурсы, критическую инфраструктуру и личные данные граждан.

Безопасность избирательного процесса является необходимым условием обеспечения электорального суверенитета государства: чем выше степень защищенности граждан, организаторов и инфраструктуры в рамках электоральной безопасности, тем ниже эффективность внешнего вмешательства в избирательные процессы. При этом сами понятия электорального суверенитета и внешнего вмешательства нуждаются в проработке. Каким образом отличить вмешательство от влияния? Стоит ли делить суверенитет на «народный», «государственный», «электоральный» или «цифровой»? Является ли вмешательство в избирательные процессы актом агрессии? Покрывает ли электоральный суверенитет внутренние угрозы электоральной безопасности?

Особенность обеспечения именно электоральной безопасности (по сравнению, например, с военной, экономической или экологической) заключается в периодичности выборов, ставшей уже международным демократическим стандартом. За редким исключением выборы и референдумы планируются заблаговременно,

участникам и организаторам избирательных процессов необходимо время для принятия взвешенных решений. Стандарт периодичности выборов зафиксирован в статье 6 Конвенции о стандартах демократических выборов, избирательных прав и свобод в государствах — участниках Содружества Независимых Государств (принята 7 октября 2002 г., далее — Конвенция СНГ). Периодичность выборов обеспечивает сменяемость власти, подразумевает ограничение срока полномочий избираемых кандидатов. В случае референдумов периодичность обеспечивает обратную связь государства с населением, предсказуемость действий государства, запланированную «сверку часов» с гражданами при принятии решений.

Одновременно со всеми плюсами периодичность выборов неминуемо сужает восприятие безопасности избирательного процесса. Узкое понимание безопасности избирательного процесса сосредоточено лишь на периодичном обеспечении безопасности на избирательном участке, например в единый день голосования. Действительно, проведение всех выборов в единый день голосования экономит средства, но также и позволяет внешним субъектам, нацеленным на вмешательство, сосредоточить усилия.

Практика многих государств показывает, что радикализация протестов, давление на граждан, провокации организаторов, утечки личных данных возникают, на первый взгляд, в период проведения голосования на избирательных участках. Такое положение дел обусловлено взаимозависимостью избирательных процессов и уровня доверия граждан к основным государственным институтам. Для провокаторов целесообразно сосредоточивать силы на избирательных процессах, так как вмешательство в выборы оборачивается снижением доверия граждан к государственным институтам. Во время выборов и референдумов растет «нагрузка» на структуры жилищно-коммунального хозяйства, общепита, здравоохранения, транспорта. В странах СНГ многие избирательные участки расположены в школах, школа — это институт первичной политической социализации, соответственно провокации становятся «минами замедленного действия» для детей. Вдобавок к этому нагнетание напряженности в период выборов и референдумов связано с политической борьбой и агитацией, на этом «паразитируют» внешние субъек-

екты. Традиционно с вызовами безопасности сопряжена организация голосования на зарубежных участках в горячих точках. Взаимозависимость избирательных процессов и доверия граждан делает справедливым и обратное утверждение: при высокой степени электоральной безопасности выборы и референдумы консолидируют общество, способствуют разрешению внутренних противоречий.

Основная угроза электоральной безопасности заключается в снижении доверия граждан к государственным институтам, в неучастии граждан в государственных делах. Концептуальное переключение внимания на «участие граждан» вместо «доверия граждан» позволяет использовать количественные инструменты мониторинга (на основе явки избирателей, членства в политических партиях, использования онлайн-систем заявлений и др.). Даже при узком понимании безопасности как защищенности в короткий промежуток времени безопасность избирательного процесса затрагивает элементы других подсистем национальной безопасности:

— политической безопасности — в случае препятствий обеспечению избирательных прав и свобод граждан, а также дезорганизации системы государственного управления, создания препятствий функционированию государственных и общественных институтов;

— информационной безопасности — в случае информационных угроз при обработке и хранении личных данных, а также дискредитации информационного обеспечения и сопровождения государственной политики;

— научно-технологической безопасности — в случае взлома систем сбора и подсчета голосов, систем обучения членов избирательных комиссий;

— социальной безопасности — в случае использования участниками избирательного процесса языка вражды или непропорционального апеллирования к национальным, языковым либо этническим идентификационным характеристикам в агитации, а также в случае подкупа голосов и электоральной коррупции;

— военной безопасности — при дискредитации вооруженных сил или нанесении ущерба военной инфраструктуре в ходе электоральной кампании в горячих точках;

- экономической безопасности — при использовании избирательных процессов как инструмента блокирования производств, предприятий, цепочек сбыта, а также при активизации транснациональных криминальных структур во время выборов;
- биологической безопасности — в случае распространения инфекций и возникновения угроз санитарно-эпидемиологическому благополучию населения в ходе электоральных кампаний;
- гидрометеорологической безопасности — при проведении выборов в условиях чрезвычайной ситуации (наводнение, пожар, сильный ветер, землетрясение);
- демографической безопасности — в случае использования субъектами политической борьбы политических технологий, направленных на разрушение института семьи как социального института.

Широкое понимание безопасности избирательного процесса позволяет проанализировать электоральную безопасность комплексно, то есть не только с точки зрения вышеперечисленных угроз безопасности, которые требуют оперативного реагирования, но и с точки зрения вызовов, способствующих возникновению угроз и требующих комплексных программ предотвращения.

Актуальность исследования электоральной безопасности в государствах СНГ вызвана пока еще противоречивым эффектом внедрения цифровых технологий в избирательные процессы. Цифровизация позволяет облегчить процесс голосования в труднодоступных регионах, экономит время, ускоряет получение предварительных итогов голосования. По оценкам специалистов, внедрение цифровых технологий в избирательные процессы приводит к росту явки избирателей, привлечению к голосованию избирателей за рубежом. Вместе с тем со снижением расходов на аренду помещений в ходе цифровизации растут затраты на обучение специалистов комиссий работе с технологиями и техническими средствами. С внедрением цифровых технологий риску подвергается один из основных стандартов демократических выборов — тайна голосования. Та же условная видеочасть на избирательном участке, с одной стороны, обеспечивает прозрачность выборов, а с другой — создает риски нарушения законного права граждан голосовать аноним-

но. Актуализируется проблема возможности взлома информационной инфраструктуры и, как следствие, проблема доверия граждан к результатам выборов.

Благодаря дистанционным технологиям основные угрозы электоральной безопасности приобретают новые формы. Среди примеров: дистанционный шантаж и угрозы в отношении избирателей, членов избирательных комиссий и их семей, псевдоголосование в интернете, имитация звонков государственных органов, минирование избирательных участков посредством IP-телефонии, фальсификация предварительных итогов голосования, локальное отключение мобильной связи, информационное манипулирование СМИ и наблюдателями в социальных сетях. Эти проблемы снова делают актуальной идею «суверенного интернета»: необходимость защиты национального информационного пространства, информационно-коммуникационной инфраструктуры, а также личных данных граждан. Несмотря на развитие цифровых технологий, по сей день происходят террористические акты в отношении избирательных комиссий и их членов. Игнорировать цифровизацию также не получается: в условиях реальной политической борьбы цифровизация (например, подсчет в режиме реального времени) может стать манипулятивным инструментом по дискредитации организаторов выборов и референдумов. В ходе цифровых избирательных процессов конструируется сетевая инфраструктура, аудитория, которая в дальнейшем используется для получения политической или экономической выгоды отдельной группой лиц. С этой точки зрения обеспечение электоральной безопасности не заканчивается с завершением государственной электоральной кампании.

Проблеме обеспечения электоральной безопасности и посвящена данная книга. В ней читатель познакомится с концепциями и механизмами обеспечения электоральной безопасности в государствах — участниках СНГ. Особый акцент сделан на возможностях и рисках цифровизации избирательных процессов. Так или иначе, от простого внедрения цифровых носителей информации до организации дистанционного электронного голосования, каждое государство — участник СНГ вовлечено в процесс цифровизации избирательной системы.

В главе 1 «Электоральная безопасность государства» содержится концептуальный анализ электоральной безопасности. Исследованы основные подходы к электоральной безопасности, изложенные в политико-прикладной и научной литературе. Вниманию читателя предложена составленная на основе анализа имеющихся подходов оценка тенденций разработки концепции электоральной безопасности, определяющей основные интересы государства и источники угроз в электоральной сфере.

В главе 2 «Цифровые технологии в избирательном процессе» проанализирован опыт внедрения цифровых технологий в избирательные процессы в мире. Сделан обзор экспертных мнений по поводу внедрения цифровых технологий в организацию выборов и референдумов. Рассмотрены новые технологии голосования, цифровые технологии администрирования избирательных процессов. Из-за рисков использования цифровых технологий в ненадлежащих целях также приведены типовые способы цифрового вмешательства в организацию выборов и референдумов в странах СНГ.

Глава 3 «Безопасность избирательного процесса» содержит исследование подходов государств — участников СНГ к обеспечению электоральной безопасности. В главе сопоставлены основные национальные интересы государств — участников СНГ, а также проведен сравнительный анализ электорального элемента концепций национальной безопасности стран Содружества. Рассмотрены основные региональные механизмы СНГ, содействующие государствам в обеспечении безопасности избирательного процесса: координация государств-участников, модельное законодательство, документы, принципы, механизмы СНГ в области электоральной безопасности.

В заключении изложены концептуальные выводы и практические рекомендации относительно укрепления электоральной безопасности государств Содружества в условиях цифровизации избирательных систем.

Электоральная безопасность государства

Электоральная безопасность государства представляет собой состояние защищенности личности, общества и государства от угроз в ходе организации, подготовки и подведения итогов выборов и референдумов. В научно-аналитической литературе данный феномен пока не получил должного системного рассмотрения. В зависимости от методологических или политических предпочтений авторов понятие «электоральная безопасность» употребляется в качестве синонима таких понятий, как «электоральный суверенитет», «электоральная неприкосновенность» (англ. electoral integrity) или «информационная безопасность». Литература в области электоральной безопасности затрагивает вопросы, связанные с вмешательством в выборы, обеспечением защиты информации, электоральной помощью (англ. electoral assistance), а также с электоральной дипломатией и особой группой составов преступлений, имеющих отношение к избирательным процессам. Часто электоральная безопасность фактически понимается как безопасность электоральной инфраструктуры, преступления против которой, наряду с преступлениями против экономической или военной инфраструктуры, влекут ответственность и взыскание ущерба. Задача этой главы состоит в системном представлении электоральной безопасности государства как состояния защищенности национальных интересов, определении основных национальных интересов и источников угроз электоральной безопасности. Для этого в главе проведен анализ прикладных и академических исследований в области электоральной безопасности.

1.1. Электоральная безопасность государства в ходе проведения выборов и референдумов

Электоральная безопасность государства — состояние защищенности национальных интересов государства в ходе проведения выборов и референдумов. Электоральная безопасность государства шире, чем охрана избирательных участков во время проведения голосования или защита личных данных участников и организаторов. Электоральные процессы всегда сопряжены с политической борьбой, ввиду этого вмешательство в организацию выборов и референдумов — неизбежный элемент избирательных кампаний. С этой точки зрения обеспечение электоральной безопасности предполагает поддержание достаточной степени устойчивости государства к вмешательству в выборы, другими словами, поддержание существующих норм, правил и инструментов подготовки, проведения и подведения итогов выборов и референдумов⁴.

Вмешательство в выборы представляет собой инструмент отдельных государств (как правило, США и стран коллективного Запада) по дестабилизации внутривнутриполитической обстановки в том или ином государстве. Средствами дестабилизации общественно-политической ситуации часто выступают генерирование протестного потенциала в обществе и создание политической сингулярности (в процессе принятия решения участвует каждый гражданин, а существующая конструкция с политическими партиями и выборами становится ненужной), что приводит к дискредитации государственной системы. После прохождения точки политической сингулярности государство должно либо качественно измениться, либо быть уничтожено. При этом используются кибератаки с высоким уровнем социального инжиниринга и применением комбинированных систем, включающих в себя возможности искус-

⁴ Евстифеев Р. В. Иностранное вмешательство в национальные выборы в цифровую эпоху: постановка проблемы и перспективы исследований // Вестник РГГУ. Серия: Политология. История. Международные отношения. — 2022. — № 3. — С. 10–27.

ственного интеллекта и различные роботизированные устройства (боты)⁵.

Распространение вмешательства в выборы на международной арене обусловлено тем, что кратчайший путь к установлению контроля над тем или иным государством лежит через влияние на избирательный процесс. Электоральное влияние квалифицируется как косвенная форма вмешательства — противоправное скрытое воздействие на выборы с использованием информационно-коммуникационных технологий (ИКТ), финансирования, работы с общественным мнением, тогда как прямая форма вмешательства представляет собой противоправное воздействие на систему установления итогов выборов⁶. Обеспечение электоральной безопасности включает в себя необходимость устранения прямого воздействия на системы регистрации граждан, хранения их личных данных, технологии голосования.

Наряду со СМИ и ресурсами интернета, оказывающими коммуникационное влияние, распространение получают формы силового вмешательства через фальсификацию результатов, взлом электоральной инфраструктуры, прямое принуждение граждан голосовать определенным образом⁷. Электоральное вмешательство на практике не имеет правовых последствий для субъекта вмешательства. Наиболее распространенные в мире формы вмешательства представлены принуждением избирателя к голосованию за определенных кандидатов (то есть лишением его свободы выбора) либо фальсификацией (подтасовкой) итогов электоральной кампа-

⁵ Прогнозируемые вызовы и угрозы национальной безопасности Российской Федерации и направления их нейтрализации / под общей редакцией А. С. Коржевского; редакционная коллегия: В. В. Толстых, И. А. Копылов. — Москва: РГГУ, 2021. — С. 42–48.

⁶ Борисов И. Б. Вмешательство в национальные выборы как сопутствующий фактор демократических процессов в глобальном мире // Гражданин. Выборы. Власть. — 2021. — № 3 (21). — С. 122.

⁷ Фельдман П. Я., Федякин А. В., Ежов Д. А. Технологии вмешательства в выборы: научное осмысление в поисках семантической определенности // Вестник Томского государственного университета. Философия. Социология. Политология. — 2019. — № 50. — С. 210–218.

нии⁸. К вмешательству относятся кибератаки на политические организации, публичное обнародование данных о гражданах и организаторах выборов и референдумов, попытки взлома систем хранения и передачи данных, а также использование СМИ и социальных сетей в целях агитации за отдельных кандидатов. Противодействие таким формам вмешательства нуждается в широком толковании электоральной безопасности как защищенности всех стадий организации выборов, в том числе информационной коммуникации.

Электоральная безопасность необязательно тождественна национальной, так как включает в себя элементы личной безопасности: безопасности избирателей и членов избирательных комиссий, а также лиц, которые в силу должностного положения участвуют в обеспечении избирательного процесса в ходе выборных кампаний. Электоральная безопасность — это состояние сложной системы защищенности, включающей следующие элементы: 1) защищенность голосующих и организаторов; 2) минимизация последствий потенциальных и реальных негативных явлений социального, информационного и техногенного характера в ходе избирательного процесса; 3) реализация волеизъявления избирателей; 4) устранение рисков дестабилизации общества, противодействие внутренним и внешним угрозам конституционным устоям государства и национальной безопасности страны в целом.

Противодействие внешним угрозам электоральной безопасности — залог обеспечения электорального суверенитета государства, то есть государственного суверенитета в избирательных процессах⁹. Электоральный суверенитет определяется как полнота и свобода усмотрения государства при организации и проведении выборов и референдумов; как национальная модель построения избирательной системы и организации избирательного процесса¹⁰. Право на национальную модель развития частично пе-

⁸ Фельдман П. Я. Концептуализация понятия «электоральное вмешательство» в эпоху «гибридных войн» // Известия Тульского государственного университета. Гуманитарные науки. — 2018. — № 4. — С. 3-12.

⁹ Борисов И. Б. Электоральный суверенитет. — Москва: РОИИП, 2010. — 94 с.

¹⁰ Борисов И. Б. Трансформация избирательных систем под воздействием неблагоприятных факторов // Гражданин. Выборы. Власть. — 2022. — № 2 (24). — С. 43.

рекликается с правом на развитие и правом на самоопределение. В таком случае под электоральной безопасностью следует понимать состояние защищенности национальной модели развития.

Для вмешательства в выборы концептуально разработаны манипулятивные политические технологии «демократического строительства», «смены режимов», «демократического транзита»¹¹, «переходного правосудия»¹², продвижения демократии и прав человека¹³.

Даже сама проблематика электоральной безопасности может выступать инструментом вмешательства, если избирательная система государства находится под внешним управлением. Так, в США проблематика вмешательства в выборы активно разрабатывалась с 2016 г. с целями расширения антироссийских санкций и блокирования «Северного потока — 2»¹⁴. После 2016 г. тематика вмешательства в выборы была инструментализирована во внутренней политической борьбе против Д. Трампа во время президентских выборов в 2020 г. На тему вмешательства в выборы США была подготовлена серия докладов («Гризлигейт», «Crossfire Hurricane» «Доклад Мюллера», «Кремлевский доклад»). Хотя доклады носят политический характер и состоят из непроверенной информации, в подготовительных материалах имеются наблюдения концептуального характера. В серии докладов комитета по разведке Сената США содержится интересный вывод относительно того, что продвижение дискурса об иностранном вмешательстве создает впечатление уязвимости самих выборов, а это подрывает доверие избирателей¹⁵.

¹¹ Miller M. Shock to the System // Coups, Elections, and War on the Road to Democratization. — New Jersey: Princeton University Press, 2021. — 348 p.

¹² Willard-Foster M. Toppling Foreign Governments: The Logic of Regime Change. — Philadelphia: University of Pennsylvania Press, 2018. — 344 p.

¹³ Boyashov A. Network Governance of the UN Human Rights Council. Diplomatic, Institutional and Organizational Actors. — New York: Routledge, 2022. — 180 p.

¹⁴ В новых санкциях США против России обнаружилась лазейка для Трампа // РБК. — 2017. — 2 августа. URL: <https://www.rbc.ru/economics/02/08/2017/5980a5289a794754fb147bc2>.

¹⁵ Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security // U. S. Senate Select Committee on Intelligence. — 2018. — May 8. URL: <https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated>.

В 2021 г. был опубликован доклад Национального совета по разведке США об иностранных угрозах президентским выборам 2020 г. Доклад оперирует понятием «влияние на безопасность или неприкосновенность выборов» (англ. *impact on security or integrity of elections*). Ключевую методологическую особенность этого доклада представляет объединение понятий «электоральное вмешательство» и «электоральное влияние». В докладе разведывательное сообщество США понимает под электоральным влиянием «...открытые и тайные усилия иностранных правительств или субъектов, действующих в качестве агентов иностранных правительств или от их имени, направленные на прямое или косвенное воздействие на выборы в США, включая кандидатов, политические партии, избирателей или их предпочтения, или политические процессы»¹⁶. Электоральное вмешательство, в свою очередь, трактуется как «...совокупность методов влияния на выборы, нацеленная на технические аспекты выборов, включая регистрацию избирателей, голосование и подсчет голосов, подведение итогов»¹⁷. Хотя в докладе вмешательство понимается как совокупность методов влияния, всё же, по мнению авторов доклада, вмешательство происходит тогда, когда влияние нацелено на технические аспекты выборов. Такой подход кардинально отличается от подхода, в котором влияние и вмешательство разграничены через отношение к национальному законодательству: влияние — правомерные действия, вмешательство — неправомерные.

Феномен электорального вмешательства может быть объяснен последствиями колониальной политики западных государств. В колониальной политике выборы, партийное строительство, референдумы, сама структура государства и все избирательные процессы выстраивались не с целью развития территории, а под сбор налогов с местного населения и выкачивание дешевых ресурсов, включая сырье и рабов¹⁸. Примечательна точка зрения,

¹⁶ National Intelligence Council. Foreign Threats to the 2020 US Federal Elections // Office of the Director of National Intelligence. URL: <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf>.

¹⁷ Ibid.

¹⁸ Zanden J.L. van. Colonial State Formation and Patterns of Economic Development in Java, 1800–1913 // *Economic History of Developing Regions*. — 2010. — № 2 (25). — P. 155–176.

в соответствии с которой электоральное правосудие предполагает предотвращение не только внешнего вмешательства в выборы, но и электоральных преступлений вообще, в том числе обусловленных внутренними угрозами электоральной безопасности¹⁹.

Электоральная безопасность тесно переплетена с информационной. В результате взаимных обвинений во вмешательстве раскручивается спираль гонки вооружений в области ИКТ. В последнее время обсуждается предложение о принятии международного кодекса поведения, который разграничил бы проблемы хакерских атак, влияния СМИ, социальных сетей, а также зафиксировал бы существующие договоренности в области невмешательства²⁰. Практика показывает, что до сегодняшнего дня договоренности в области невмешательства не выполнялись в полной мере. Но можно ли вывести из вмешательства электоральную безопасность? Таким образом, чтобы идеологическое противоборство не затрагивало избирательные процессы?

Идеологическое противоборство обуславливает вмешательство в избирательные процессы не только во время организации выборов и референдумов, но и в период «затишья». Современные политические технологии вмешательства предусматривают два основных способа: оказание внешней поддержки тем или иным политическим акторам и так называемое стимулирование демократических процессов²¹. При этом для вмешательства в электоральные процессы характерен эффект отсроченного действия: вне зависимости от мотивации иностранного субъекта вмешательство одного государства в избирательные процессы другого государства значительно повышает шансы дестабилизации государства-объекта в течение пяти

¹⁹ Elections, Violence and Transitional Justice in Africa / ed. by Opongo E., Murithi T. — New York: Routledge, 2022. — 202 p.

²⁰ Тимофеев И. Н., Чарап С. Кодекс невмешательства. Российский совет по международным делам. — 2019. — 14 июня. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/kodeks-nevmeshatelstva/>.

²¹ Corstange D., Marinov N. Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention // American Journal of Political Science. — 2012. — № 3. — P. 655–670.

лет²². Среди основных эффектов электорального вмешательства выделяется «информационное влияние» — целенаправленное вмешательство иностранных государств во внутренние дела других государств для создания климата недоверия между государством и его гражданами через использование восприимчивости уязвимых сторон общества²³. При этом электоральное вмешательство предпочтительнее военного ввиду отсутствия людских потерь и предпочтительнее переговоров в том случае, если переговоры влекут большие финансовые затраты.

Обеспечение электоральной безопасности — сугубо государственная функция. Электоральная безопасность выступает основным условием демократического развития, а не наоборот. Международные организации, передающие техническую помощь в области развития от иностранных субъектов, как правило, методологически ставят безопасность избирательного процесса в зависимость от так называемого уровня демократического развития. Между тем уровень демократического развития может быть определен только на основе национальных особенностей того или иного государства, а для развития государству необходима безопасность. Исследования так называемой электоральной помощи (технической помощи в области избирательных процессов) указывают на неоднозначное целеполагание иностранных государств при направлении технической помощи в рамках международных организаций²⁴.

Несмотря на то что обеспечение электоральной безопасности входит в функции государства, региональные организации могут

²² Levin D. Should We Worry about Partisan Electoral Interventions? The Nature, History, and Known Effects of Foreign Interference in Elections // *Defending Democracies Combating Foreign Election Interference in a Digital Age* / ed. by Hollis D. B., Ohlin J. D. — New York: Oxford University Press, 2021. — P. 32.

²³ Fjällhed A., Pamment J., Bay S. A Swedish Perspective on Foreign Election Interference // *Defending Democracies Combating Foreign Election Interference in a Digital Age* / ed. by Hollis D. B., Ohlin J. D. — New York: Oxford University Press, 2021. — P. 141.

²⁴ Антюшин Н. А. Избирательная поддержка в эпоху дискурса «внешнего вмешательства» // *Российская государственность на пути в будущее: традиции и траектории политико-правовых реформ: материалы IX научно-практической конференции по исследованию российской государственности* (Владимир, 15 октября 2021 г.). — Владимир: Владимирский филиал РАНХиГС, 2021. — С. 139–145.

содействовать координации государств в области электоральной безопасности. Такое положение дел объясняется ростом транснационального элемента организации выборов из-за переноса части электоральных процессов в цифровое пространство. В этом случае региональные организации не могут претендовать на функции «институтов международной электоральной юстиции» для расследования вмешательств в электоральные процессы и реагирования на них. Неравенство в технологическом и экономическом развитии будет программировать подобные организации на воспроизводство вмешательства отдельной группы государств.

Обеспечение электоральной безопасности государства сопряжено в первую очередь с эффективной внутренней политикой. Внешние субъекты вмешательства обычно лишь «паразитируют» на внутренних недочетах, политизируя их и превращая в элемент внутривнутриполитической борьбы. Как правило, государство устойчиво к внешнему вмешательству в том случае, если проводит эффективную внутреннюю политику²⁵.

1.2. Национальные интересы государства и источники угроз электоральной безопасности

Электоральная безопасность государства предусматривает защиту от внешних и внутренних угроз в электоральной сфере. Вмешательство в электоральные процессы представляет собой основную угрозу национальной безопасности. Субъекты вмешательства принимают сложную сетевую форму, вовлекая в свою деятельность СМИ, рейтинговые агентства, благотворительные организации, фонды и некоммерческие организации. Западные международные наблюдатели при этом выполняют операцию по «легализации вбрасываемой информации». Объектом иностранного электорального вмешательства вместо конкретных политических участников становится организация системы избирательных процессов в целом²⁶. Иностранное вмешательство

²⁵ Willard-Foster M. *Toppling Foreign Governments*. — 2018. — 256 p.

²⁶ Манойло А. В., Авдеева Н. В., Лавринов Б. Б. Внешнее вмешательство в выборы как угроза безопасности Российской Федерации // Гражданин. Выборы. Власть. — 2018. — № 3. — С. 58–91.

основано на управлении восприятием рисков с целью размывания «легитимности» избирательных процессов. Другими словами, реальная электоральная безопасность в большей степени зависит от внутренних факторов, чем от внешних юридических институтов, механизмов и процессов²⁷.

Национальные интересы государства в ходе проведения выборов и референдумов включают: 1) обеспечение гражданам права избирать и быть избранными; 2) функционирование институтов бесперебойного прямого волеизъявления; 3) сохранение устойчивости избирательной системы; 4) обеспечение сбалансированности интересов и недискриминации общественных групп, организаций и государственных органов; 5) обеспечение права государства на развитие; 6) устойчивый рост явки и поступательное развитие правовой культуры граждан; 7) обеспечение защиты прав граждан в ходе цифровизации избирательных систем.

Основными индикаторами состояния защищенности государственных интересов в области электоральной безопасности могут выступать: 1) участие граждан в электоральных процессах (например, через анализ явки, ротацию членов местных избирательных комиссий по районам, подключение к работе избирательных комиссий молодежи); 2) бесперебойная работа организаторов избирательных процессов (например, через работу с обращениями граждан, повышение квалификации, разъяснение методологии организации выборов и референдумов). Изменение доверия граждан к государственным службам может свидетельствовать о состоянии защищенности, на наш взгляд, лишь косвенно, хотя лонгитюдные социологические опросы граждан дают важную информацию о динамике настроений в обществе. Причины тому — тайна голосования, а также сугубо индивидуальное определение гражданами государственных институтов.

Одним из основных внешних источников угроз электоральной безопасности выступает неравенство в социально-экономическом развитии. Источниками внешних угроз электоральному суверенитету являются субъекты иностранного вмешательства:

²⁷ Евстафьев Д. Г. Информационные манипуляции и государственный суверенитет: риски для России // Гражданин. Выборы. Власть. — 2019. — № 2 (12). — С. 98–110.

иностранное государство, группа иностранных государств, международная организация, международная неправительственная организация, иностранный гражданин, лицо без гражданства, иностранная организация (юридическое лицо) либо группа иностранных граждан, лиц без гражданства, иностранных организаций (юридических лиц), включая иностранное средство массовой информации, а также физические и юридические лица, действующие в их интересах. Среди предложенных направлений противодействия три основных: на законодательном уровне, на правоприменительном уровне, а также информационное направление. Среди типов инструментов вмешательства авторы выделяют финансовые рычаги, организационно-политические механизмы, коммуникативные приемы и киберинструменты²⁸.

Необходимость предотвращения циклического вмешательства в выборы и референдумы требует выделения электоральной преступности²⁹. Электоральная преступность как подвид политической преступности — «негативное социальное явление, выражаемое совокупностью общественно опасных деяний, совершаемых в период и в связи с проведением избирательной кампании или кампании референдума, причиняющих или создающих угрозу причинения вреда конституционным правам и свободам граждан, а также подрывающих основы конституционного строя в стране»³⁰.

Если посмотреть на мировые тренды, вмешательство в выборы все чаще квалифицируется в качестве основной угрозы национальной безопасности (феномен так называемой секьюритизации). Феномен секьюритизации вызван различием государственных подходов к обеспечению невмешательства во внутренние дела. Например, США смотрят на проблему вмешательства с точки зрения избирательных процессов, а Российская Феде-

²⁸ Евстифеев Р. В. Иностранное вмешательство в национальные выборы в цифровую эпоху: постановка проблемы и перспективы исследований // Вестник РГГУ. Серия: Политология. История. Международные отношения. — 2022. — № 3. — С. 10–27.

²⁹ Кочетова П. О., Тепляшин П. В. Криминологические аспекты электоральной преступности: понятие, структура и формы // Актуальные вопросы юридической науки. — 2019. — № 4 (4). — С. 89–97.

³⁰ Там же. — С. 91.

рация — с точки зрения информационной безопасности и риска дестабилизации внутренней ситуации³¹. Секьюритизация выражается в повышении требований к внешним субъектам, желающим прямо или косвенно выступить участниками избирательного процесса, ужесточении ответственности за действия или бездействие, результатом которых становится подрыв доверия к электоральному процессу, обеспечении правового регулирования областей, через которые могут быть созданы угрозы избирательным процессам³².

С практической точки зрения иностранное вмешательство в выборы выступает реальной угрозой государственному суверенитету и демократическому развитию государств³³. Исследования электоральной безопасности, носящие прикладной характер, как правило, нацелены на определение конкретных форм иностранного вмешательства в избирательные процессы. Такая постановка вопроса обусловлена необходимостью противодействия конкретным формам вмешательства.

В отдельных случаях для концептуального изучения феномена иностранного вмешательства используется понятие «электоральный суверенитет». В докладе 2017–2018 гг. о защите государственного суверенитета и предотвращении вмешательства во внутренние дела Российской Федерации понятие «электоральный суверенитет» не отделяется от понятия «государственный суверенитет» и используется для определения вмешательства во внутренние дела как не основанной на общепризнанных принципах международного права и международных договорах Российской Федерации деятельности со стороны иностранных государств, юридических и физических лиц, их объединений, имеющей целью изменение основ конституционного

³¹ Зиновьева Е. С. Проблема «цифрового вмешательства» в российско-американских отношениях // Российский совет по международным делам. — 2020. — 23 октября. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/problema-tsifrovogo-vmeshatelstva-v-rossiysko-amerikanskikh-otnosheniyakh/>.

³² Buzan B., Wæver O., Wilde J. de. Security: A New Framework for Analysis. — London: Lynne Rienner, 1998. — 239 p.

³³ Мушкет И. И., Амбурцев Р. А., Ксендзов А. Н. Противодействие иностранному вмешательству в электоральные процессы: опыт государств — участников Межпарламентской Ассамблеи СНГ // Право. Безопасность. Чрезвычайные ситуации. — 2022. — № 2 (55). — С. 52–62.

строю, территориальной целостности Российской Федерации, ее внутренней и внешней политики, состава и структуры органов государственной и муниципальной власти³⁴. Фактически понятие «электоральный суверенитет» разработано с целью определения основных видов иностранного вмешательства. В указанном докладе их десять: 1) проведение социологических исследований в интересах зарубежных государственных структур в преддверии выборов за счет иностранного финансирования; 2) противоправное и публичное навязывание извне (иностранными правительственными, межправительственными и официальными парламентскими структурами) конкретных кандидатов; 3) ведение из-за рубежа на национальных языках целенаправленной систематической и массовой пропаганды за счет иностранного государственного финансирования в течение всего периода, включая «день тишины» и день голосования; 4) прямое противоправное воспрепятствование голосованию избирателей на зарубежных участках; 5) проведение кибератак из-за рубежа на ресурсы центральных избирательных комиссий; 6) финансирование из-за рубежа деятельности так называемых гражданских активистов, принимавших непосредственное участие в предвыборной агитации, включая агитацию за бойкот выборов, и «контроле за выборами»; 7) оказание из-за рубежа на безвозмездной основе адресной помощи по политическому признаку отдельным участникам избирательных процессов, включая информационно-консультационное обслуживание, организационную и иную поддержку; 8) публичное непризнание результатов выборов, включая непризнание самого права на участие в выборах граждан по политическому и региональному признакам; 9) публичное, целенаправленное и систематическое распространение диффамации, а также дискредитация в отношении действующих институтов власти, системы организации и проведения выборов; 10) стимулирование раскола внутри российского общества, общественного недовольства, дестабилизация

³⁴ Специальный доклад по итогам президентских выборов в Российской Федерации (2018 г.) с точки зрения покушений на российский электоральный суверенитет // Совет Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/structure/commissions/iccf_def/plans/92958.

ции государства и общества путем внешнего экономического, дипломатического, информационного и иного давления.

В дополнение к указанным формам вмешательства существуют сложные формы, например иностранное вмешательство под видом международного наблюдения за выборами (путем предвзятых политических оценок в заключениях о выборах)³⁵. Каким образом отличить иностранное вмешательство от международного наблюдения? Носителем суверенитета государств является народ, а потому право на признание выборов принадлежит народу. Ни одно современное государство не установило в качестве субъекта оценки выборов ни одну международную организацию. Государства не делегируют какой бы то ни было организации право на признание или непризнание выборов и референдумов. Соответственно, международный наблюдатель будет сопровождать электоральные процессы, выполняя вспомогательную по отношению к организаторам выборов функцию³⁶.

Активное развитие концепция электоральной безопасности получила на этапе обсуждения новой редакции Концепции национальной безопасности Республики Беларусь в 2022–2023 гг. Согласно заявлению Государственного секретаря Совета Безопасности Республики Беларусь А. Г. Вольфовича, в новой редакции Концепции зафиксирован термин «электоральный суверенитет» как неотъемлемое право независимого, суверенного государства самостоятельно, без вмешательства извне проводить выборы и референдумы³⁷.

Если рассматривать электоральную безопасность в широком смысле, то ее обеспечение требует комплексной защиты государственного суверенитета, а не исключительно электорального

³⁵ Борисов И. Б. Иностранцы (международные) организации на выборах в Российской Федерации: правовая «халатность» или вынужденная необходимость // Гражданин. Выборы. Власть. — 2018. — № 3. — С. 40–57.

³⁶ Международное наблюдение за выборами / А. С. Бояшов, И. И. Мушкет, С. Г. Караваев [и др.]. — Санкт-Петербург: Секретариат Совета МПА СНГ, 2021. — 84 с. — (Демократия, выборы, парламентаризм).

³⁷ Проект Концепции нацбезопасности будет вынесен на общественное обсуждение. В чем суть изменений // БЕЛТА. — 2023. — 20 февр. URL: <https://www.belta.by/society/view/proekt-kontseptsii-natsbezopasnosti-budet-vynesen-na-obshchestvennoe-obsuzhdenie-v-chem-sut-izmenenij-551270-2023/>.

компонента. Государственный суверенитет — это возможность и способность высшей государственной власти самостоятельно организовывать и реализовывать полноту своих компетенций³⁸. В числе показателей, свидетельствующих о подрыве или ослаблении государственного суверенитета, следует отметить: 1) ограничение юрисдикции государства иностранными органами управления; 2) ограничение монополии государства на применение насилия при законных основаниях; 3) активность международных и иностранных организаций в политической деятельности государства. Таким образом, государственный суверенитет фактически зиждется на монополии государства организовывать выборы.

Достоинство методологического выделения электорального элемента суверенитета заключается в определении той грани, которая отделяет субъектов избирательного процесса от посторонних организаций. В этом случае международный наблюдатель, направленный на выборы или референдум от международной организации, кардинально отличается от национальных наблюдателей (партий, волонтеров, общественных объединений), которые являются участниками избирательного процесса в широком смысле.

В то же время выделение именно электорального суверенитета имеет свои методологические недостатки. Во-первых, при использовании понятия «электоральный суверенитет» внимание замыкается на внешних угрозах электоральной безопасности. Во-вторых, отличительной характеристикой суверенитета является его неделимость. Ограниченное употребление термина «электоральный суверенитет» в академической литературе связано с риском политтехнологического разделения суверенитета на «народный», «режимный», «цифровой» и т. д. Неделимость суверенитета была обоснована еще в классическом произведении Ж. Бодена «Шесть книг о республике», хотя сам Ж. Боден употреблял понятия «государственный суверенитет»

³⁸ Ватгиль В. Н. Защита государственного суверенитета в Республике Беларусь: противодействие деструктивным угрозам в политической сфере // Вестник Гродненского государственного университета имени Янки Купалы. Серия 1: История и археология. Философия. Политология. — 2023. — № 1. — С. 123–128.

и «народный суверенитет» как равнозначные³⁹. Современные международно-правовые инструменты не позволяют отделить электоральное вмешательство от влияния, так как в результате вмешательства в выборы наносится не физический или территориальный, а политический урон. Здесь надо отметить, что через нанесение политического урона государство вполне может решать территориальные вопросы. Само же вмешательство в выборы сопряжено с нарушением принципов невмешательства, суверенитета и самоопределения, что уже зафиксировано в Уставе ООН (соответственно, можно «заново» разрабатывать концепции электорального невмешательства, электорального суверенитета, электорального самоопределения)⁴⁰.

Методологически электоральный суверенитет представляет собой элемент электоральной безопасности. Причем разработка концепции электоральной безопасности на региональном уровне может помочь конкретизировать позиции стран СНГ в области невмешательства. Разработка концепции электоральной безопасности необходима в связи со следующим.

Во-первых, в научной и аналитической литературе пока нет системного понимания фактора безопасности в ходе выборов и референдумов. Ключевой водораздел мировых подходов проходит по той же линии, что и сравнительные политические исследования демократического развития: по линии «права человека — экономическое развитие»⁴¹. В первом случае во главу электоральной безопасности ставятся права на свободу мирных собраний и свободного волеизъявления, а во втором — право государств на развитие. В первом случае выдвигается суждение о том, что соблюдение прав человека, не относящихся к избирательным (хотя и перекликающихся с ними!), обеспечивает безопасность. Во втором случае предполагается, что безопасность обеспечивает реализацию прав человека, а абсолютизация

³⁹ Гугняк В. Я. Жан Боден (1530–1596) как представитель раннего меркантилизма // Вопросы экономики и права. — 2015. — № 5. — С. 80–85.

⁴⁰ Keitner Ch. Foreign Election Interference and International Law // *Defending Democracies: Combating Foreign Election Interference in a Digital Age* / ed. by Hollis D. B., Ohlin J. D. — New York: Oxford University Press, 2021. — P. 188.

⁴¹ Гольяев А. О. Соотношение прав человека и развития: новые веяния в Совете ООН по правам человека // Современное право. — 2017. — № 11. — С. 119–121.

отдельных прав, типа права на собрания и волеизъявление, может происходить в ущерб реализации избирательных прав граждан и безопасности избирательного процесса. В первом случае наблюдатели признаются правозащитниками, а во втором — «сопроводителями» избирательных процессов. Надо отметить, что западноевропейская группа стран придерживается первого подхода лишь в отношениях с развивающимися государствами, тогда как в их внутренних делах безопасность определяет права человека, а не наоборот.

Во-вторых, концептуальное исследование электоральной безопасности необходимо по причине усложнения политических систем государств. Сказывается цифровизация и транснациональный доступ к элементам информации. Размытие грани между субъектами избирательных процессов и внешними заинтересованными сторонами приводит к появлению сложных сетей международного вмешательства. Отличить внешнее вмешательство во внутренние дела от внутреннего вмешательства в выборы становится все труднее.

С целью предотвращения вмешательства развиваются сложные сети в области электоральной безопасности, которые позволяют странам делиться опытом в области электоральных процессов, а зарубежным диаспорам — быть вовлеченными в развитие своей родины. В странах СНГ защита избирательных процессов концептуально оформлена в качестве обеспечения государственных национальных интересов в политической сфере. Политическая подсистема национальной безопасности уже включает защиту конституционного строя и внутривнутриполитических процессов, связанных с выборами и референдумами. Электоральная подсистема, как правило, концептуально не отделяется от политической. Соответственно, на первый взгляд подходы к нейтрализации источников угроз национальной безопасности в политической и электоральной сферах будут идентичными.

Структура политических подсистем государств также усложняется: наряду с организаторами выборов и референдумов в электоральной сфере действуют партии, общественные объединения, СМИ, индивиды. Функции наблюдателей уже давно связаны не только с политическими партиями: в электоральном мониторинге участвуют и организаторы выборов, и между-

народные организации, и волонтеры. Усложняются формы финансирования и информационного сообщения. На пространстве СНГ закономерно возникают новые формы прямого народовластия: всенародные собрания, национальные курултай и общественные советы. Усложнение политических подсистем неминуемо ведет к выделению электоральной сферы. Это связано с отличием иностранного вмешательства в избирательные процессы от других форм вмешательства. При этом оформление безопасности электоральной сферы через понятие электорального суверенитета затрагивает лишь внешние источники угроз национальной безопасности.

В-третьих, выделение элементов электоральной безопасности актуально по причине крайне высокой степени политизации этой темы. От того, что считается безопасным, в конечном счете зависит и то, насколько независимыми будут выборы. Сама система координат, методология выделения элементов безопасности, нередко представляет собой уже готовую концепцию отдельных стран. В то же время избирательные процессы развиваются с учетом национальных и исторических особенностей того или иного государства. Для государств СНГ электоральная безопасность — залог суверенного развития. Соответственно, чрезвычайно важно выделить составляющие электоральной безопасности в Содружестве объективно и беспристрастно, не отдавая предпочтение какой бы то ни было избирательной системе. Особенно актуальным представляется выделение тех ключевых организаций, которые способствуют укреплению электоральной безопасности и деполитизации этой повестки.

Вместе с тем в истории государств из всех регионов мира имеются примеры использования аргумента безопасности в качестве политической технологии консолидации сторонников. Разработка элементов электоральной безопасности позволяет отделить объективные характеристики состояния защищенности от политических технологий: формирования образа врага, инструмента переговорного процесса и политического давления, мобилизации широких слоев населения.

Особая актуальность изучения электоральной безопасности связана с необходимостью определения границ между вмешательством и влиянием извне. Формы внешнего вмешательства

в выборы становятся все сложнее: в него вовлечены ИТ-компании, международные организации и некоммерческие партнерства. Все сложнее становится отличить действительное международное наблюдение от государственного вмешательства под видом международного наблюдения за избирательными процессами. Если с прямым финансированием политических партий из-за рубежа дело обстоит проще, то выявить элемент вмешательства в организации общественных программ или курсов повышения квалификации становится на порядок сложнее.

Анализ прикладных исследований и академической литературы в области электоральной безопасности показывает, что политико-прикладные исследования сосредоточены на изучении иностранного вмешательства в избирательные процессы, в том числе через концепцию защиты государственного суверенитета. Использование термина «электоральный суверенитет» характерно для отдельных прикладных исследований, их достоинство заключается в отделении иностранных субъектов вмешательства от внутренних, например иностранных СМИ от участников избирательного процесса, в случае дискредитации избирательной системы. Вместе с тем сам термин «электоральный суверенитет» содержит признаки тавтологии, так как суверенитет предполагает, что механизм выборов и референдумов является выражением воли народа выбирать путь развития и форму правления. В таком случае необходимо пересматривать основные положения Устава ООН и разрабатывать концепции электорального невмешательства, электорального самоопределения или электорального сотрудничества.

В академических исследованиях в большей степени безопасность избирательного процесса рассматривается как комплексное состояние защищенности от внешних и внутренних угроз. Электоральная безопасность, понимаемая в контексте национальной безопасности как безопасность в электоральной сфере, представляет собой подсистему национальной безопасности. Электоральная безопасность — это состояние защищенности личности, общества и государства от угроз в ходе организации, подготовки и подведения итогов выборов и референдумов.

Обеспечение электоральной безопасности сопряжено с пропорциональным ограничением избирательных прав и свобод

граждан. С одной стороны, в мире наблюдается расширение всеобщности избирательного права в виде снижения возрастных цензов, нивелирования ценза гражданства на муниципальных выборах, введения квот для меньшинств. С другой стороны, негативный фактор вмешательства в избирательные процессы заставляет отдельные государства внедрять дополнительные цензы, например ценз оседлости. Как правило, пропорциональное ограничение избирательных свобод связано с введением режима чрезвычайного, военного или осадного положения. Сегодня в академической литературе намечается тенденция к изучению ограничения избирательных прав граждан как следствия иностранного информационного и санкционного давления⁴². На пространстве Содружества в соответствии с частью 2 статьи 18 Конвенции СНГ ограничения для выдвижения кандидатов, списков кандидатов, касающиеся создания и деятельности политических партий (коалиций), избирательных прав и свобод граждан, могут применяться в интересах обеспечения электоральной безопасности, то есть защиты конституционного строя, национальной безопасности, поддержания общественного порядка, защиты общественного благосостояния и морали. Уместно привести в качестве примера обеспечение безопасности во время распространения коронавирусной инфекции: граждане с повышенной температурой не допускались в общие помещения для голосования.

⁴² Борисов И. Б. Трансформация избирательных систем под воздействием неблагоприятных факторов // Гражданин. Выборы. Власть. — 2022. — № 2 (24). — С. 26–46.

Цифровые технологии в избирательном процессе

Внедрение цифровых технологий способствует устойчивому развитию промышленности, политики, гуманитарной сферы. Информация становится более доступной, ускоряются многие форматы анализа больших данных, процессы взаимодействия и коммуникации систем. Под задачи цифровизации оптимизируются технологические процессы в образовании, науке, здравоохранении.

Цифровизация не обошла стороной и электоральные процессы⁴⁵. В теоретическом рассмотрении цифровизация избирательных процессов подразумевает создание целой инфраструктуры: обеспечение техническими средствами избирательных участков, разработка программного обеспечения для проведения электронного голосования и дистанционного электронного голосования. Это и образовательный процесс, требующий технических, временных, а иногда и человеческих затрат для обучения как членов избирательных комиссий, так и самих избирателей.

⁴⁵ Бродовская Е. В., Домбровская А. Ю., Карзубов Д. Н., Синяков А. В. Развитие методологии и методики интеллектуального поиска цифровых маркеров политических процессов в социальных медиа // Мониторинг общественного мнения: экономические и социальные перемены. — 2017. — № 5. — С. 79–104; Бубнов А. Ю., Шаповалов В. Л., Дмитриева О. В. Интенсивность вовлеченности россиян в интернет-коммуникацию // Мониторинг общественного мнения: экономические и социальные перемены. — 2013. — № 3. — С. 19–27; Володенков С. В. Big Data как инструмент воздействия на современный политический процесс: особенности, потенциал и акторы // Журнал политических исследований. — 2019. — № 1. — С. 7–13; Косоруков А. А., Котлярова Т. Ю. Информационно-коммуникационные технологии как фактор трансформации публичной сферы современного общества // Тренды и управление. — 2018. — № 4. — С. 88–96; Грачев М. Н. Электронное голосование «за» и «против» // Известия Тульского государственного университета. — 2011. — № 1. — С. 360–366.

С одной стороны, цифровизация призвана упростить проведение государственных электоральных кампаний. Для организаторов выборов цифровизация обеспечивает сверку зарегистрированных избирателей, защищенную передачу данных, автоматизированный подсчет голосов. Для избирателей открывается возможность участия в политической жизни страны из любой точки мира. С другой стороны, возникают вызовы, преодоление которых требует усилий от государства. Повышается стоимость организации выборов, возникают угрозы безопасности, актуализируются проблемы технического обеспечения избирательных процессов, предупреждения киберпреступности, цифрового неравенства в обществе.

2.1. Опыт внедрения цифровых технологий в избирательные процессы

Цифровизация избирательных процессов диктует изменения в общественных отношениях, становится триггером социальных изменений, так как появление новых инструментов волеизъявления оказывает воздействие на политическое сознание граждан⁴⁴. В этом отношении речь идет как о прямом обеспечении самого процесса голосования, так и о подготовительном этапе, когда информационно-коммуникативное пространство становится инструментом воздействия на волеизъявление народа (официальные и альтернативные СМИ, социальные сети, блогинг и микроблогинг)⁴⁵.

Развитие электронного голосования — задача, поставленная практически во всех странах мира. Всего 10 лет назад под электронным голосованием понимали анализ и обработку результатов, полученных в ходе традиционной процедуры. Так

⁴⁴ Лешенюк О. Н. Укрепление электоральной безопасности через синхронизацию межпарламентского компонента Союзного государства, ОДКБ, СНГ // Региональная политика, политическая география и геополитика. История и современность: материалы международной научной конференции, посвященной 20-летию кафедры региональной политики и политической географии СПбГУ / под ред. Н. М. Михеевой, Н. В. Каледина. — Санкт-Петербург: Издательство ВВМ, 2022. — С. 719–725.

⁴⁵ Пильгун Е. В. Семантика и прагматика кризисного дискурса. — Минск: ИВЦ Минфина, 2020. — 203 с.

называлась процедура использования электронных средств (автоматических машин) в целях обработки избирательных бюллетеней и подсчета голосов избирателей⁴⁶. В этом случае речь шла о сугубо машинной обработке результатов голосования. Электронное голосование понимается также как осуществление волеизъявления с помощью телекоммуникационных средств, например интернета или мобильной связи⁴⁷. В этом случае речь идет о дистанционном электронном голосовании. Использование при голосовании систем удаленного доступа делает факт голосования независимым от места нахождения избирателя. Это позволяет привлечь к электоральному процессу граждан, которые не могут принять непосредственное участие в выборах. В данной главе под термином «электронное голосование» авторы понимают применение технологии получения и подсчета голосов избирателей, а также подведения итогов голосования с помощью любых электронных средств.

Государства находятся в поисках той самой идеальной схемы и технологии проведения электронного голосования. На данный момент опробованы следующие форматы его проведения: с использованием технологии сканирования бюллетеней для подсчета голосов; с прямой записью результатов голосования и автоматическим подсчетом голосов; через интернет с созданием личного кабинета⁴⁸; через интернет непосредственно на избирательном участке; через интернет в специальных киосках, расположенных в публичных местах; дистанционное интернет-голосование (избиратель сам выбирает интернет-устройство и место для голосования)⁴⁹; с использованием перфокарт; на электронном аппарате с буквенно-цифровой клавиатурой, который после окончания голосования передает информацию на центральный компьютер; смешанные формы.

⁴⁶ Алексеев Р. А., Абрамов А. В. Проблемы и перспективы применения электронного голосования и технологии избирательного блокчейна в России и за рубежом // Гражданин. Выборы. Власть. — 2020. — № 1. — С. 9–13.

⁴⁷ Давыдов Д. А. Интернет-голосование как электоральная политическая технология // Вестник Пермского университета. — 2010. — № 1 (9). — С. 59.

⁴⁸ Титовская А. В. Электронное тайное голосование в России и за рубежом: сравнительно-правовой анализ // Юридическая наука. — 2012. — № 4 — С. 106.

⁴⁹ Грачев М. Н. Указ. соч. — С. 360.

Для оптимизации избирательного процесса используются варианты технических средств и программного обеспечения, создаются новые, среди которых: электронная система подведения итогов голосования, машины для подсчета посредством идентификационных карт, подсчет голосов посредством съемки бюллетеней на видеокамеры, магнитный картридер, экран и оптическая ручка, сенсорные мониторы, сервис коротких мобильных сообщений, цифровое телевидение, персональное цифровое вспомогательное устройство, сканирование избирательных бюллетеней, технологии блокчейна и др.

Широкое распространение получили электронные машины для голосования, которые позволяли избирателям с нарушением зрения участвовать в голосовании самостоятельно. Однако машины не раз критиковались, так как не предоставляли возможностей для проверки правильности и учета голоса. Сканирование бюллетеней позволяет сохранить бумажный бюллетень как доказательство при ручном пересчете голосов. Устройства для маркировки заполняют бумажный бюллетень от имени избирателя после того, как избиратель вводит инструкции на сенсорном экране. Интернет-голосование — удобное решение, но оно требует точной идентификации при сохранении анонимности избирателя. В настоящее время лишь Эстония смогла внедрить канал интернет-голосования на основе идентификационных карт с чипом на всех выборах без каких-либо ограничений для избирателей.

Основные преимущества цифровизации электорального процесса состоят в следующем:

- возможность осуществить волеизъявление из любой точки мира, а не только по месту регистрации;

- обеспечение участия в голосовании всех граждан, имеющих право голосовать (инклюзивность). Цифровизация может потенциально способствовать повышению явки избирателей, в частности повысить интерес молодежи к политической жизни страны;

- использование онлайн-возможностей позволит расширить временные рамки электоральных кампаний. Так, если основные дебаты проходят в формате телевещания, то избиратель привязан к определенному месту и времени (трансляция передачи на каналах). Цифровизация делает возможным создание личных

кабинетов избирателей и наполнение их информационными сообщениями, ссылками на официальные выступления и т. д. Использование личных кабинетов позволит снизить и воздействие внешних сил через интернет, так как пользователь получит исчерпывающий объем информации в личном кабинете и ему не нужно будет вводить поисковые запросы в Сети;

— переход к электронному голосованию позволит экономить человеческие и финансовые ресурсы (снижается необходимость организации большого числа избирательных участков, уменьшается количество задействованных членов избирательных комиссий, а также наблюдателей, что снизит и общие расходы на проведение референдумов и выборов);

— повышение оперативности и надежности передачи результатов голосования. Институт наблюдения в принципе потребует пересмотра и реорганизации. Возможно, наблюдателям понадобятся дополнительные технические знания, в том числе в сфере информационных технологий, так как с новыми возможностями появляются новые вызовы (нет ли воздействия на обработку и подсчет голосов в электронном формате со стороны вредоносного программного обеспечения? не подвергается ли сервер с данными хакерским атакам?).

Внедрение цифровых технологий сопряжено с противоречиями. Основной характеристикой электронного голосования следует назвать его доступность для включенных в электронный реестр граждан, однако если гражданин не включен в списки голосующих в электронном формате, то в случае изменения его жизненных обстоятельств он может не явиться на голосование. Сокращаются затраты из государственного бюджета на организацию и проведение голосования за счет уменьшения числа членов избирательной комиссии, однако увеличиваются затраты на технические средства, обеспечивающие избирательные процессы, на переобучение членов избирательных комиссий и наблюдателей⁵⁰. Повышаются риски технических сбоев, энергетической диверсии, хакерских атак и воздействия на избирателей извне на протяжении всей электоральной кампании. Уменьшается возможность подкупа избирателей непосредственно в день

⁵⁰ Алексеев Р. А., Абрамов А. В. Указ. соч.

голосования, однако затрудняется техническая возможность мониторинга подкупа голосов. Еще одной характеристикой является динамичность, то есть сокращение времени на подсчет голосов и получение результатов, но возрастает число трудностей с обеспечением прозрачности на стадии обработки избирательных бюллетеней. Электронное голосование способно привлечь интерес активной молодежи к процессу и потенциально обеспечить явку этой категории граждан, но вызывает трудности у людей преклонного возраста и с определенными физическими недостатками, не в полной мере обеспечивая инклюзивность.

Несмотря на то что электронное голосование — на участке или дистанционно — внедряется или планируется к внедрению во всех странах мира, государства не спешат избавляться от традиционного формата, сохраняя приоритет за голосованием на избирательном участке.

2.2. Перспективы цифровизации выборов и референдумов в государствах СНГ

Государства СНГ стараются следовать тенденциям времени и постепенно внедрять элементы электронного голосования в избирательные процессы. За последнее десятилетие накоплен большой практический опыт голосования в электронном формате. Некоторые попытки были довольно успешными, некоторые потерпели неудачу. Тем не менее, вступая в третье десятилетие XXI в., страны совершенствуют законодательство и активно экспериментируют в области обеспечения электоральной безопасности онлайн-голосования.

В Азербайджане планируется внедрить систему электронного голосования. Б. М. Аскеров, член Центральной избирательной комиссии Азербайджанской Республики, отметил, что у каждой страны есть свои традиции развития: «В соответствии с этим, в будущем в Азербайджане будет рассмотрено внедрение электронного голосования»⁵¹. В стране получила распространение

⁵¹ В Азербайджане планируется внедрить систему электронного голосования // Report. — 2021. — 2 октября. URL: <https://report.az/ru/vnutrennyaya-politika/v-azerbajdzhane-planiruet-sya-vnedrit-sistemu-elektronno-go-golosovaniya/>.

практика установления видеокамер на избирательных участках. Еще во время конституционного референдума в 2009 г. по решению ЦИК с целью обеспечения прозрачности голосования на 500 из более чем 5000 избирательных участков были установлены веб-камеры⁵².

Согласно действующему Избирательному кодексу Республики Армения от 2016 г.⁵³ участвовать в дистанционном электронном голосовании (далее — ДЭГ) имеют право ограниченные группы населения:

— избиратели, проходящие службу в дипломатических или консульских представительствах Республики Армения, и обладающие избирательным правом члены их семей;

— военнослужащие, находящиеся в длительной служебной командировке или на обучении в иностранных государствах;

— сотрудники представительств зарегистрированных в Республике Армения юридических лиц, расположенных за рубежом, и обладающие избирательным правом члены их семей, проживающие вместе с ними за рубежом.

ДЭГ применялось на выборах депутатов Национального Собрания Республики Армения 2 апреля 2017 г.⁵⁴; на досрочных выборах депутатов Национального Собрания Республики Армения 9 декабря 2018 г.⁵⁵; на досрочных выборах депутатов Национального Собрания Республики Армения 20 июня 2021 г.⁵⁶ На выборах 2017 г. в список избирателей, голосующих посредством ДЭГ, было внесено 877 человек⁵⁷; на выборах 2018 г. — 729⁵⁸; на выборах 2021 г. — 650⁵⁹. На выборах 2021 г. посредством ДЭГ

⁵² Оппозиция считает, что веб-камеры повлияют на голосование по референдуму в Азербайджане // Кавказский узел. — 2009. — 5 марта. URL: <https://www.kavkaz-uzel.eu/articles/150448/>.

⁵³ Избирательный кодекс Республики Армения: принят Национальным Собранием Республики Армения 25 мая 2016 г. URL: <https://www.arlis.am/documentview.aspx?docid=108731>.

⁵⁴ Центральная избирательная комиссия Республики Армения: официальный сайт. URL: <https://res.elections.am/images/doc/e-vote02.04.17.pdf>.

⁵⁵ Там же. URL: <https://res.elections.am/images/doc/e-vote09.12.18.pdf>.

⁵⁶ Там же. URL: <https://res.elections.am/images/doc/e-vote20.06.2021.pdf>.

⁵⁷ Там же. URL: https://res.elections.am/images/doc/e_voters02.04.17.xlsx.

⁵⁸ Там же. URL: https://res.elections.am/images/doc/e_voters09.12.18.xlsx.

⁵⁹ Там же. URL: https://res.elections.am/images/doc/e_voters20.06.21.xlsx.

проголосовало 500 человек, 45 бюллетеней были признаны недействительными⁶⁰. Для участия в ДЭГ гражданам необходимо предварительно подать заявку в уполномоченный орган, ведущий Государственный регистр населения. Списки граждан, голосующих электронным путем, формируются строго по заявкам, а гражданам для участия в электронном голосовании заранее передается специальный код в запечатанном конверте⁶¹. Таким образом, в Армении граждане голосуют только в зарубежных дипломатических представительствах, голосование через ДЭГ не имеет массового распространения.

Беларусь пока наблюдает за практиками зарубежных стран в подготовке, обеспечении и проведении электронного голосования. Несмотря на то что Беларусь участвовала в разработке технических средств обеспечения электронного голосования, такой формат пока не используется в стране. Одной из причин приверженности к традиционному формату является то, что страна опасается возможного вмешательства в процесс голосования. Необходимо тщательно продумать и обеспечить электоральную безопасность, так как при попытке государственного переворота в 2020 г. в ходе президентской электоральной кампании активно использовались информационные вбросы. Социальные сети, представители оппозиции создавали отдельные платформы для проведения альтернативного голосования именно в электронном формате⁶². Этот факт демонстрирует, что цифровизация в электоральной сфере не только содействует реализации избирательных прав граждан, облегчая жизнь и избирателям, и избирательным комиссиям. Иногда цифровизация становится орудием для поддержания альтернативных процессов, манипуляций общественным мнением, создания альтернативной реальности.

⁶⁰ Там же. URL: https://res.elections.am/images/doc/e_vote.result20.06.21.pdf.

⁶¹ Посредством электронной системы голосования на выборах в Армении проголосовали около 900 граждан // Arka News Agency. — 2017. — 2 апреля. URL: https://arka.am/ru/news/politics/posredstvom_elektronnoy_sistemy_golosovaniya_na_vyborakh_v_armenii_progolosovali_okolo_900_grazhdan/.

⁶² Выборы в Беларуси в 2024–2025 годах пройдут традиционно — ЦИК // Sputnik Беларусь. — 2023. — 12 февраля. URL: <https://sputnik.by/20230212/vybory-v-belarusi-v-2024-2025-godakh-proydut-traditsionno> — tsik-1072189833.html.

Для Беларуси важно обеспечение соответствия формата дистанционного электронного голосования законам и нормам страны. Исходя из заявления Председателя ЦИК Республики Беларусь И. В. Карпенко, «Центральная избирательная комиссия поставила задачу разработать концепцию цифровизации избирательной системы»⁶³. Одна из задач — проведение подготовительной работы по формированию регистра населения, на основе которого будет создан регистр избирателей. Однако во избежание вмешательства в электоральные процессы 2024–2025 гг. (парламентские и президентские выборы) власти страны приняли решение о проведении голосования в традиционном формате.

В Казахстане на выборах президента 20 ноября 2022 г. население имело право проголосовать по предъявлению электронной версии документа, удостоверяющего личность избирателя, в день голосования. На избирательных участках граждане предъявляли цифровой аналог паспорта или других документов, удостоверяющих личность, посредством приложения eGov mobile и мобильных приложений банков Kaspi Bank и Halyk Bank⁶⁴. На основании цифровых документов избиратель получал бюллетень. Дальнейшая процедура голосования проходила в традиционном формате. В республике разработана база данных физических лиц, однако она, как и в случае с другими странами, не совершенна (не в полной мере обеспечивается с технической стороны требование о тайне голосования, фактически функции ЦИК передаются другим организациям, что противоречит Конституции, имеется неполнота данных ввиду миграции населения, сложно получить открепительное удостоверение онлайн)⁶⁵. Кроме этого, голосование через мобильные приложения

⁶³ Когда в Беларуси может быть введено электронное голосование, рассказал глава Центризбиркома // БЕЛТА. — 2023. — 12 февраля. URL: <https://www.belta.by/society/view/kogda-v-belarusi-mozhet-byt-vvedeno-elektronnoe-golosovanie-rasskazal-glava-tsentrizbirkoma-549807-2023>.

⁶⁴ Казахстанцы смогут проголосовать на выборах с цифровым удостоверением // Казинформ. — 2022. — 14 ноября. URL: https://www.inform.kz/ru/kazahstancysmogut-progolosovat-na-vyborah-s-cifrovym-udostovereniem_a4001451.

⁶⁵ В Минюсте объяснили, что мешает ввести электронное голосование в Казахстане // Zakon.kz. — 2022. — 7 ноября. URL: <https://www.zakon.kz/6029376-miniust-ukazal-na-to-chto-meshaet-vvesti-elektronnoe-golosovanie-v-kazahstane.html>.

и интернет-системы недостаточно защищено от хакерских атак и хищения данных.

Кыргызстан перешел на электронное голосование с обязательной биометрической идентификацией избирателей. Для участия на избирательных участках гражданам нужно пройти дактилоскопию и фотографирование. Только в этом случае гражданин регистрируется в реестре избирателей⁶⁶. Согласно информации Центральной комиссии по проведению выборов и референдумов Кыргызской Республики (далее — ЦИК Кыргызстана), для участия необходимо иметь учетную запись на Государственном портале электронных услуг «Тундук», облачную электронную подпись, телефон или компьютер с доступом в интернет⁶⁷.

До 2023 г. речь не шла о дистанционном электронном голосовании. В 2022 г. ЦИК Кыргызстана и Центральная избирательная комиссия Российской Федерации (далее — ЦИК России) провели семинар по вопросам реализации дистанционного электронного голосования⁶⁸. Обмен опытом с ЦИК России стал одним из ключевых этапов подготовки внедрения ДЭГ в избирательную систему республики.

25 февраля 2023 г. ЦИК Кыргызстана заявила, что апробирует в пилотном режиме ДЭГ на выборах Самаркандекского айылного кенеша Баткенского района Баткенской области 9 апреля 2023 г.⁶⁹ 7 марта 2023 г. ЦИК приняла решение добавить к апробации ДЭГ выборы депутатов Ак-Сайского и Ак-Татырского айылных кенешей Баткенского района Баткенской

⁶⁶ Федоров В. И. Электронное голосование как имиджевый донор: случай Кыргызстана // Избирательное законодательство и практика. — 2018. — № 4. — С. 35–37.

⁶⁷ Выборы депутатов: голосование будет электронным // Новости Кыргызстана. — 2023. — 27 февраля. URL: <https://www.ktrk.kg/ru/news/s/76939>.

⁶⁸ ЦИК России провела онлайн-семинар по вопросам ДЭГ с ЦИК Киргизии // Центральная избирательная комиссия Российской Федерации. — 2022. — 29 ноября. URL: <http://www.cikrf.ru/news/cec/52305/>.

⁶⁹ ЦИК КР апробирует в пилотном режиме электронное голосование на выборах депутатов Самаркандекского айылного кенеша, назначенных на 9 апреля 2023 года // Центральная комиссия по выборам и проведению референдумов Кыргызской Республики. — 2023. — 25 февраля. URL: <https://shailoo.gov.kg/ru/news/6515/>.

области⁷⁰. Впервые в экспериментальном режиме выборы депутатов айылных кенешей, назначенные на 9 апреля 2023 г., состоялись с использованием дистанционного электронного голосования. Власти гарантировали полное обеспечение тайны волеизъявления. Всего на данных выборах в список ДЭГ был включен 841 избиратель (5,2% от общего количества избирателей в данных округах). Из них воспользовались ДЭГ 694 избирателя, или 82,52% включенных в список (4,3% от общего количества избирателей в данных округах)⁷¹. Помимо непосредственно ДЭГ, на данных местных выборах в Кыргызской Республике также в пилотном режиме были применены модернизированные устройства идентификации избирателей, которые имели следующие функции:

- считывание машиночитаемой зоны паспорта;
- сканирование отпечатков пальцев рук;
- идентификация по геометрии лица при помощи камеры;
- отображение информации о проходящем идентификацию на дисплее;
- распечатка избирательных бюллетеней соответствующего избирательного округа после успешного прохождения процедуры биометрической идентификации⁷².

Успех цифровизации зависит от разъяснительной работы с населением. Так, в Кыргызстане есть граждане, отказывающиеся проходить биометрию, некоторые выражают опасения, что персональные данные могут быть использованы третьими лицами в корыстных целях. Положительный результат дает работа с населением. В 2021 г., по заявлению и. о. премьер-министра

⁷⁰ Электронное голосование будет апробировано на выборах депутатов Самаркандского, Ак-Сайского и Ак-Татырского айылных кенешей // Центральная комиссия по выборам и проведению референдумов Кыргызской Республики. — 2023. — 7 марта. URL: <https://shailoo.gov.kg/ru/news/6527/>.

⁷¹ Подведены предварительные итоги голосования на выборах депутатов 3 айылных кенешей Баткенской области // Центральная комиссия по выборам и проведению референдумов Кыргызской Республики. — 2023. — 9 апреля. URL: <https://shailoo.gov.kg/ru/news/6610/>.

⁷² На избирательных участках Самаркандского айылного кенеша в пилотном режиме применяются модернизированные устройства идентификации избирателей // Центральная комиссия по выборам и проведению референдумов Кыргызской Республики. — 2023. — 9 апреля. URL: <https://shailoo.gov.kg/ru/news/6608/>.

А. Э. Новикова, около 19% граждан не вошли в избирательные списки из-за того, что не сдали биометрические данные⁷³.

В Молдове цифровизация избирательного процесса началась в 2008 г. Однако систему голосования через интернет планируют протестировать и запустить на выборах осенью 2023 г. Центральная избирательная комиссия Республики Молдова приняла решение опробовать формат электронного голосования в экспериментальном режиме. Проголосовать онлайн можно через специальное приложение e-Votare при наличии электронной или мобильной подписи либо электронного внутреннего паспорта. Предварительно избиратель должен оформить электронную или мобильную подпись, для этого необходимо посетить одно из учреждений: Агентство госуслуг, Службу информационных технологий и кибербезопасности, Центр информационных технологий или оператора сотовой связи Moldcell или Orange. Услуга осуществляется на платной основе. Нередко явка среди представителей диаспоры невелика по причине ограниченного количества избирательных участков за границей, и электронное голосование в этом случае могло бы решить проблему, однако процесс оформления электронной или мобильной подписи затруднителен и не увеличит явку среди представителей диаспоры. С этой же проблемой столкнутся и люди с ограниченными возможностями, мамы с грудными детьми и другие категории граждан. Подтверждение правильности голосования происходит с помощью кода для проверки и QR-кода.

Электронное голосование проходит за несколько дней до традиционного, но возможность посещения участка сохраняется. В этом случае приоритет отдается традиционному формату. Система обеспечивает анонимность, результаты не доступны заранее. Контроль за электронной электоральной кампанией осуществляется заблаговременно в целях обеспечения высокого уровня кибербезопасности, блокировки хакерских атак как из-за пределов, так и внутри страны. Система работает с использованием ИКТ-инфраструктуры ЦИК, государственной

⁷³ Почти 900 тыс. кыргызстанцев не сдали биометрию, голосовать не смогут // Sputnik Кыргызстан. — 2020. — 25 декабря. URL: <https://ru.sputnik.kg/20201225/kyrgyzstan-vybory-izbirateli-spisok-1050888757.html>.

инфраструктуры, тщательно продуманы этапы шифрования для обеспечения тайны голосования.

В России выстроена четкая система, которая позволяет исключить двойное голосование, однако электронное голосование внедрено пока в отдельных регионах. Закон об электронном голосовании российские власти создали в целях совершенствования избирательных процессов. Аргументы в пользу электронного голосования следующие: удобство для граждан, находящихся за пределами страны, обеспечение прав людей преклонного возраста и лиц с ограниченными возможностями, форс-мажорные обстоятельства и случаи пандемии в стране, которые затрудняют обеспечение явки.

Для автоматизации и координации избирательных действий разработана и активно используется Государственная автоматизированная система Российской Федерации «Выборы» (ГАС «Выборы»). Создана автоматическая система сбора бюллетеней и подсчета голосов КОИБ (комплекс обработки избирательных бюллетеней), которая сводит к минимуму участие человека в этом процессе. Применяется технология QR-кодирования протоколов участковых избирательных комиссий, позволяющая ускорить процесс введения протоколов участковых избирательных комиссий об итогах голосования в ГАС «Выборы».

Создан интерактивный рабочий блокнот участковой избирательной комиссии, в котором предоставлены подробные методические рекомендации по подготовке к работе участковой избирательной комиссии, по проведению и подготовке отчетности о работе комиссии.

Разработан механизм «Мобильный избиратель». При подаче предварительного заявления о формате участия в выборах этот механизм позволяет гражданам проголосовать на любом участке в пределах избирательного округа, без привязки к месту жительства, а также проголосовать дистанционно посредством интернета, если в регионе предусмотрена такая опция⁷⁴. Система

⁷⁴ О Порядке подачи заявления о включении избирателя, участника референдума в список избирателей, участников референдума по месту нахождения на выборах в органы государственной власти субъекта Российской Федерации, референдуме субъекта Российской Федерации: постановление Центральной избирательной комиссии Российской Федерации от 25 мая 2021 г. № 7/52-8.

ДЭГ дает возможность осуществить волеизъявление из любой точки мира.

Впервые эксперимент по дистанционному электронному голосованию в России провели в 2019 г. на выборах депутатов Московской городской Думы. Затем, летом 2020 г., эту практику распространили на голосование по поправкам в Конституцию. В сентябре 2020 г. ДЭГ применялось на довыборах в Государственную Думу в Ярославской и Курской областях⁷⁵, в 2021 г. — в единый день голосования в Курской, Мурманской, Нижегородской, Ростовской и Ярославской областях, в Москве и Севастополе⁷⁶. В 2022 г. электронное голосование было организовано в единый день голосования в Калужской, Курской, Новгородской, Псковской, Томской и Ярославской областях, в Москве⁷⁷.

Для участия в электронном голосовании в России гражданам необходимо наличие регистрации по месту жительства на территории субъекта Российской Федерации, в котором проводится такое голосование, либо получение гражданства Российской Федерации в упрощенном порядке в соответствии с Указом Президента Российской Федерации от 24 апреля 2019 г. № 183 при отсутствии места жительства на территории Российской Федерации. Гражданам необходимо также подтвердить учетную запись на едином портале государственных услуг⁷⁸.

В России на выборах 2021 г. в списки ДЭГ было включено 635 тыс. избирателей, из которых более 587 тыс. проголосовали⁷⁹;

⁷⁵ Что нужно знать об электронном голосовании // Государственная Дума Федерального Собрания Российской Федерации. — 2022. — 3 августа. URL: <http://duma.gov.ru/news/55046/>.

⁷⁶ Как проголосовать на выборах в Государственную Думу // Государственная Дума Федерального Собрания Российской Федерации. — 2021. — 17 сентября. URL: <http://duma.gov.ru/news/52280/>.

⁷⁷ Единый день голосования // Госуслуги. URL: <https://www.gosuslugi.ru/edg>.

⁷⁸ О Порядке дистанционного электронного голосования с использованием федеральных государственных информационных систем: постановление Центральной избирательной комиссии Российской Федерации от 8 июня 2022 г. № 86/716–8. URL: <http://www.cikrf.ru/activity/docs/postanovleniya/51681/>.

⁷⁹ Минцифры подвело итоги работы цифровых сервисов на выборах-2021 // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. — 2021. — 21 сентября. URL: <https://digital.gov.ru/ru/events/41276/>.

на выборах 2022 г. в списки ДЭГ было включено 110 тыс. избирателей, из которых более 95 тыс. проголосовали⁸⁰.

Узбекистан планирует постепенно применять практики электронного голосования, в стране создана база данных избирателей. Современные технологии используются для информирования граждан о нормах законодательства, с этой целью было разработано специальное мобильное приложение. Одной из трудностей внедрения электронного голосования является защита от вмешательства третьей стороны в тайну волеизъявления.

В 2023 г. в ходе референдума по принятию поправок в Конституцию Республики Узбекистан электронное голосование не внедрялось, однако использовались элементы цифровизации в ходе досрочного голосования. Досрочное голосование было доступно на основании заявления в участковую избирательную комиссию с указанием причины, по которой гражданин будет отсутствовать в день референдума (отпуск, командировка, выезд за границу и т. п.). Подача такого заявления впервые была возможна через интернет. Референдум прошел в соответствии с международными стандартами, были приняты меры по обеспечению электоральной безопасности в соответствии с принципами транспарентности, справедливости, подлинности и свободы выборов на основе всеобщего равного избирательного права при тайном голосовании; осуществления защиты избирательных прав и свобод человека и гражданина, общественного и международного наблюдения за выборами; гарантий реализации избирательных прав и свобод участников избирательного процесса.

Цифровизация затрагивает обеспечение интересов всех слоев населения, включая лиц с ограниченными возможностями. Возрастает и количество инфраструктурных задач: разработка программного обеспечения для слабовидящих, слабослышащих и других категорий граждан. В первую очередь технические возможности должны быть направлены на удовлетворение существующей социальной потребности. Государство должно обеспечить соответствие электронного голосования возможностям избирателя. Следует помнить, что, например, для некоторых

⁸⁰ Минцифры подвело итоги работы цифровых сервисов на выборах 2022 г. // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. — 2022. — 11 сентября. URL: <https://digital.gov.ru/ru/events/41956/>.

избирателей пожилого возраста сама форма проведения электронных выборов может быть неприемлема в первую очередь в связи со страхом использования информационных технологий, недостаточностью знаний и несовершенством владения теми или иными цифровыми устройствами.

Несмотря на внушительный список технологий и вариантов проведения электронных выборов и референдумов, осуществление этого процесса на практике требует пересмотра следующих параметров.

Во-первых, необходимо совершенствование законодательной базы вплоть до внесения поправок на конституционном уровне, так как голосование с использованием цифровых средств обеспечивает принцип транспарентности, сохраняя тайну голосования и защиту массива данных.

Во-вторых, важным аспектом является идентификация гражданина. Практики проведения электронного голосования в странах мира описывают различные способы идентификации избирателя и защиты данных: многоступенчатая идентификация, личные кабинеты и ПИН-коды, электронные идентификационные карты, электронная подпись, биометрические данные избирателя, сканирование отпечатков пальцев и т. д. При дистанционном электронном голосовании довольно трудно проследить обеспечение тайны голосования: возможно, избиратель сообщил данные своего личного кабинета, идентификационные данные и т. д. третьим лицам и голосование осуществляется под его именем, а не им самим.

В-третьих, перед разработчиками программного обеспечения стоит задача обеспечить деперсонафикацию собранных голосов и защитить информацию. Так, данные должны быть зашифрованы, переданы в избирательную комиссию, а только там расшифрованы и обработаны. Тем не менее угроза взлома данных вполне реальна. Хакерское и вредоносное программное обеспечение может перехватить, перенаправить, удалить голос, перенаправить пользователя на мошеннический сайт, что не только снизит явку, но и может привести к дестабилизации ситуации.

Еще одной задачей является обеспечение бесперебойной технической работы системы. Во избежание хакерских атак не должно быть никаких технических сбоев как в самой системе,

так и в работе интернета. Также важно обеспечить устойчивую подачу электроэнергии, поскольку электронные системы легко могут быть выведены из строя в ходе диверсии, направленной на электроэнергетические сети города, страны.

Кроме этого, существует и ряд вопросов, которые вызывают много дискуссий и требуют тщательного планирования и продумывания при внедрении систем электронного голосования. Возникает вопрос о необходимости создания резервной копии в бумажном выражении. Довольно сложно обнаружить фальсификации, особенно в случае коррумпированности избирательных органов или их халатности при подсчете голосов; в отсутствие резервной бумажной копии сложнее и доказать, что манипуляции с голосами имели место.

С одной стороны, требуется продумать, каким образом избиратель сможет проверить и убедиться, что он проголосовал правильно и его голос учтен, с другой — все еще не решена проблема точной идентификации избирателя и многократного голосования. Цифровые средства, обеспечивающие избирательный процесс, должны в автоматизированном порядке исключать возможность повторного голосования. К примеру, в африканских странах для предотвращения махинаций и фальсификаций используют сканирование отпечатка пальца, а в некоторых — даже сканирование радужной оболочки глаза.

Отсутствует и полная гарантия безошибочной идентификации, даже при использовании биометрических данных. Риск фальсификации существует и при обновлении реестра избирателей. Списки избирателей в основном формируются на основе реестров населения. Здесь особое внимание должно уделяться контролю за исключением лишних записей или умерших избирателей. В случае регистрации на электронное голосование избиратель не может проголосовать традиционным способом, потому что в списках на участке его не будет.

Стоит отметить, что в XXI в. в некоторых странах все еще сохраняется проблема неграмотности населения. В этом случае электронное голосование отпугнет избирателей. Также остается проблема попыток внешнего воздействия на ход и результаты голосования, угроз взлома, кражи или покупки голосов.

2.3. Технологии цифрового вмешательства в выборы и референдумы

Развитие цифровых технологий в странах СНГ во многом упрощает жизнь, но при этом открывает возможности для изучения аудитории и воздействия на нее, в том числе на потенциального избирателя. Посредством технологий выявляются идеологические предпочтения, осуществляется навязывание определенных моделей поведения, рамок и стереотипов, формируется мнение и готовится почва для принятия избирателем решения, выгодного для третьей стороны⁸¹. В этих целях используются технологии: искусственный интеллект и нейротехнологии, блокчейн, «интернет вещей», виртуальная и дополненная реальность, квантовые технологии, создание цифровых двойников и др. Возрастает роль современных мессенджеров, которые позволяют распространять информацию в том числе и без доступа в интернет (технология Multipeer Connectivity Framework)⁸².

Искусственный интеллект способен автоматизировать некоторые этапы электоральных процессов и оптимизировать расходы. Так, например, скоринг при подсчете голосов (метод, основанный на статистической обработке первичных данных) даст возможность исключить неправильные или множественные голоса, оценить, какой формат голосования работает лучше, собрать статистику по голосованию и т. д. Голосовые помощники и чат-боты способны дать подсказки избирателю в процессе электоральной кампании, в том числе лицам с ограниченными возможностями, оптимизировать работу избирательных комиссий. Такие электронные помощники вполне могут обеспечить анонимность и тайну голосования при условии надежной защиты от хакерских атак. С помощью искусственного интеллекта в автоматическом режиме могут обрабатываться реестры избирателей при подготовке к электронному голосованию, в частности в вопросах подтверждения личности, автоматической про-

⁸¹ Пильгун Е. В. Политическое манипулирование через идеологизацию кризиса // Управление и политика. — 2022. — № 1 (2). — С. 30–43.

⁸² Несмашный А. О. Интернет-технологии в политике: проблема интерпретации понятия // Среднерусский вестник общественных наук. — 2017. — № 1. — С. 157–164.

верки данных. Технология в аналогичных целях используется банками.

Развитие «интернета вещей» таит угрозу воздействия на массовое мнение со стороны внешних сил. Бытовые вещи, попадающие под категорию «умные», подключены к интернету как в частных домовладениях, так и на крупных объектах. Параллельно к интернету подключены и промышленные системы контроля. Нередко защита подобных устройств ненадежна, что открывает возможности для хакерских атак. Подобное «умное» устройство может превратиться в способ слежения, получения информации об идеологической картине на объекте, будь то домовладение, офис или промышленное производство.

Технология блокчейна способна обеспечить прозрачность избирательного процесса и неизменность полученных данных, однако при использовании слабых схем шифрования бюллетеней существует и угроза перехвата электронного бюллетеня, то есть злоумышленники в реальном времени смогут узнать, кто за кого голосовал, и подменить данные. Технология уже применялась в экспериментальном ключе в Москве, на выборах депутатов Государственной Думы Федерального Собрания Российской Федерации в Ярославской и Курской областях в 2020 г. Опыт применения технологии был успешен, тем не менее возникали сложности, требующие временных издержек при получении результатов. В связи с тем, что функцией переголосования воспользовались около 15% избирателей, увеличилось и время обработки результатов (установление последнего голоса и удаление предыдущих). Количество принятых бюллетеней по одномандатным округам превышало количество выданных, количество избирателей, получивших бюллетень, не совпадало с суммой избирателей по округам в отдельности⁸⁵. Подобные ошибки в системе были выявлены и устранены. В целом блокчейн «Ростелекома» на базе Waves позволил гарантировать неизменность информации и прозрачность голосования, однако применение технологии в электоральных целях требует дальнейшего совершенствования.

⁸⁵ Какие проблемы возникли при онлайн-голосовании в Москве. Что важно знать // РБК. — 2021. — 22 сентября. URL: <https://www.rbc.ru/politics/22/09/2021/614a05889a7947146622a368>.

Цифровизация электоральных процессов меняет технологии вмешательства. Вмешательство в электоральные процессы с применением технологий блокчейна может происходить в процессе наблюдения. К примеру, система голосования на блокчейне Polys предлагает наблюдателям использовать ноды-аудиторы, которые участвуют в общей блокчейн-сети и осуществляют наблюдение за голосованием, поступающими голосами и выдаваемыми бюллетенями. Однако организации, использующие ноды-аудиторы, имеют право создавать внешние интерфейсы, открывать доступ к наблюдению за ходом выборов широкой публике.

Технологии виртуальной и дополненной реальности обладают способностью воздействия элементов этой искусственной системы на сознание, в том числе на поведение и волю. Разработчики технологии могут найти причинно-следственные связи и перепрограммировать их.

Технологии создания цифрового двойника для вмешательства в электоральные процессы позволяют создать копию процесса, при успешной хакерской атаке на онлайн-платформу для голосования цифровой двойник может сопровождать избирательный процесс, заниматься сбором и анализом данных, в подходящий момент перехватить и заменить голос избирателя.

Технологии электорального позиционирования и мобилизации направлены на проведение информационных кампаний и повышение значимости голосования в массовом сознании. Для этого разрабатываются фандрайзинговые и краудфандинговые платформы⁸⁴. Такие технологии направлены на поиск дополнительных финансовых средств или волонтеров. В президентских кампаниях Б. Обамы в 2008 г. и 2012 г. широко использовался этот инструмент в целях создания эффекта сопричастности рядового обывателя к чему-то глобальному, формируя политическую лояльность к кандидату и вовлекая в избирательный процесс. Электоральная кампания Э. Макрона опиралась на массовое волонтерское движение. Подобный интерактив притягивает внимание и способствует повышению явки избирателей.

⁸⁴ Коллективный сбор средств, привлечение инвестиций, как правило, через интернет.

Если в случае США и Франции наблюдается положительный эффект от использования этих технологий, то в ходе президентской электоральной кампании в Республике Беларусь, наоборот, фандрайзинговые и краудфандинговые платформы действовали как психологически мотивационное средство для мобилизации населения к активному протестному движению. Финансовый вклад в поддержку кандидата даже в минимальном денежном выражении лучше всего мобилизует граждан к осуществлению волеизъявления и дальнейшему отстаиванию своего кандидата. Оппозиция призывала к использованию платформы для альтернативного электронного голосования, разработка и финансирование которой осуществлялись третьими лицами. По задумке в ходе дополнительного голосования отобразилось бы якобы реальное количество голосов, что помогло бы оппозиции обвинить власть в фальсификации и подлоге. Простому гражданину демонстрировалась якобы прозрачность электронной платформы. Однако те же проблемы голосования и защиты голосования через интернет не были решены.

Онлайн-публикации на YouTube-каналах и в социальных сетях создают дополнительный антураж, дискредитируя как действующие власти и выбранный курс страны в целом, так и других кандидатов. Доступность видеокамер в телефонах граждан и программных средств работы с видео способствует созданию искаженных сюжетов и фейковых новостей с последующим их размещением в пабликах. Все это смещает фокус с реальных кандидатов на провокационные действия, усиливает протестные настроения в обществе, способствует подготовке митингов и др.

Технологии привлечения волонтеров и коммуникации с ними позволяют не только расширить агитационные действия, но и использовать такую «рабочую силу» для поддержки лояльности будущих избирателей и критики оппонентов, в том числе через интернет. Среди волонтеров достаточно много специалистов в различных сферах, включая сферы информационных технологий, пиара, коммуникаций и др. Такие возможности открывают доступ к применению технологий интеллектуального анализа, мониторинга и проектирования электоральной динамики (технологии Big Data) и позволяют таргетировать рекламную кам-

панию. В этих целях используются данные социальных сетей, по которым можно определить в том числе и предпочтения избирателя в будущем политическом курсе страны.

Алгоритмы использования Big Data включают в себя следующие этапы: производится географическое сегментирование страны, на выделенные сегменты накладывается информация о явке и об идеологических предпочтениях населения с учетом анализа социально-экономической и демографической статистики, данных соцопросов, затем расставляются агитационные приоритеты, определяются график работы штаба, частота встреч с кандидатом. С учетом особенностей избирателя в рекламные баннеры и пикеты попадает нужная оппозиционным структурам или внешним акторам информация.

В современных электоральных кампаниях технологии Big Data будут пользоваться все большей популярностью, напрямую связываться с целями онлайн-мониторинга и контроля электорального пространства, использоваться для адресного воздействия на аудиторию, позволят изучать мнения, отношение к определенному актору.

Цифровые технологии постепенно становятся неотъемлемой составной частью избирательных кампаний. Из практик, внедряемых и применяемых сегодня, следует, что идеальная система онлайн-голосования должна создаваться исходя из следующих критериев:

- использование доступного кода программного обеспечения в целях контроля, наблюдения и проведения аудита, что позволит достичь прозрачности голосования;

- использование технологии блокчейна и криптографии для обеспечения шифрования голосов, проверки неизменности данных, что позволит обеспечить анонимность и тайну голосования;

- осуществление эффективного контроля в целях устранения технических сбоев в процессе голосования с полным обеспечением тайны голосования и анонимности данных избирателей;

- обеспечение наблюдателям за выборами доступа к результатам подсчета голосов, спискам избирателей, в том числе технической реализации процесса наблюдения;

— создание виртуальных избирательных комиссий и виртуальных урн для голосования (сервер для хранения данных, без доступа сторонних акторов) по аналогии с используемыми при традиционном голосовании;

— использование простого и понятного интерфейса, обеспечение бесперебойной работы технического сопровождения.

Демократия требует свободных, периодических, прозрачных и инклюзивных выборов. В мире число избирателей, имеющих право голоса, оценивается в четыре миллиарда человек. Повсеместное распространение новых технологий, социальных сетей и влияние искусственного интеллекта может намеренно или непреднамеренно подорвать доверие к избирательным системам, тем самым делегитимизируя демократии во всем мире. В этом контексте все субъекты, участвующие в избирательных процессах, должны сыграть важную роль. Органы управления выборами, специалисты по проведению выборов, средства массовой информации, избиратели, политические партии и организации гражданского общества должны понимать масштабы цифровизации и влияние технологий на избирательный цикл. В связи с этим стоит подчеркнуть, что интернет-голосование не сможет стать аналогом традиционного голосования, в первую очередь по причине «цифрового неравенства». Не все избиратели имеют цифровые устройства и навыки использования цифровых сервисов. Электронное голосование дополнит общую систему голосования как один из удобных инструментов. Потребуется время для принятия обществом новых тенденций и формирования понимания работы систем электронного голосования. Кропотливая работа будет проводиться и для снятия технических и репутационных барьеров, вызванных необходимостью защиты персональных данных.

Достаточно сложно обеспечить тайну голосования с технической стороны, более того, на конституционном уровне часто закреплено, что функции ЦИК не могут быть переданы другим органам и организациям. В связи с этим возникают трудности с дополнительным шифрованием данных при организации процесса. В настоящий момент такая система не разработана, так как доступ к данным и подсчету голосов должен быть у ЦИК как ответственного органа. Перед государственными органами

стоит задача усовершенствовать базы данных граждан, в первую очередь для обеспечения возможности электронного открепления для голосования на участках по месту пребывания избирателя.

Существует значительное противоречие в вопросах контроля электоральных процессов и обеспечения достоверности результатов, анонимности и защиты персональных данных. Оно связано с тем, что в целях правильного подсчета, защиты от вмешательства третьих лиц и получения верных результатов необходимо контролировать каждое действие, но поэтапный контроль противоречит требованиям конфиденциальности и значительно затрудняет организационный процесс.

Цифровой контроль должен осуществляться и для предупреждения множественного голосования. Технологическое разнообразие открывает много возможностей для электронного голосования: голосование на сайте посредством персонального компьютера, голосование через мобильное приложение и др.

Процессы цифровизации избирательной сферы требуют разработки подходящего программного обеспечения, основными критериями для которого должны стать доступность и простота использования, при этом сервисы должны быть защищены от внешнего воздействия, хакерских атак и других возможных попыток дискредитации результатов выборов. Необходимо заранее создать реестр цифровых данных об участниках электоральной кампании, обеспечить бесперебойное функционирование цифровой платформы. Цифровые сервисы для обеспечения и сопровождения избирательной кампании должны быть разработаны для всех участников электорального процесса: для избирателей, для кандидатов и (или) политических партий и объединений, для избирательных комиссий.

Для избирателей цифровые сервисы должны выполнять функцию информирования: об особенностях электоральной кампании и сроках проведения выборов или референдума, о зарегистрированных кандидатах и (или) партиях, о местонахождении физических избирательных участков, о проведении кампании, о результатах выборов или референдума после окончания избирательной кампании, предоставлять финансовую сводку. Цифровая платформа должна иметь функцию подачи

заявления. Важно, чтобы сервисы обеспечивали возможность подачи заявления о включении в список избирателей, осуществляющих волеизъявление онлайн, обеспечивали возможность проверки избирателем наличия своей фамилии в списке, а также голосования из любой точки мира.

Кандидатам цифровые сервисы должны предоставить возможность получать информацию о сроках избирательной кампании, результатах регистрации кандидатов, формировании и составах избирательных комиссий, о результатах выборов и референдумов и т. д.

Для избирательных комиссий цифровые сервисы становятся методическим помощником, источником законодательной базы, то есть информационной поддержкой. Также сервисы должны предоставлять доступ к государственным информационным ресурсам в целях проверки документов. Одна из самых важных задач — осуществление автоматизированного подсчета голосов с учетом принципов достоверности и сохранения тайны голосования.

Необходимо рассматривать цифровизацию как общую тенденцию, то есть технологии и информационно-коммуникационные средства должны сопровождать весь избирательный цикл. На всех этапах избирательного цикла необходимо обеспечить цифровое сопровождение веб-порталов, услуг по регистрации избирателей и кандидатов, функций поиска записей избирателей и общей информации, связанной с выборами, инструкций по процессу голосования, справочной информации (нормативно-правовая база) и официальных результатов выборов.

Следует внедрить системы управления выборами, которые фактически отразят все аспекты управления электоральным процессом и выстроят архитектуру поддержки ИКТ-инфраструктуры избирательных округов. Системы позволят аккумулировать и отчетность о финансировании избирательных кампаний, работе избирательных участков и комиссий; дать перечень инструментов для администрирования выборов, в целях контроля и противодействия попыткам хакерских атак и внешнего вмешательства во время выборов. Создание единой системы управления выборами даст возможность контролировать несколько каналов голосования и избежать многократности. Цифровое

администрирование выборов позволит создать хранилище информации для обработки и анализа больших объемов отчетных данных, а в дальнейшем — автоматизировать многие аналитические процессы.

Внедрение единой системы управления записями позволит создавать, редактировать, публиковать, хранить записи и управлять ими в целом. В первую очередь это будет полезно для формирования реестров избирателей.

На предвыборном этапе цифровые системы содействуют повышению уровня честности выборов⁸⁵ посредством обеспечения прозрачности процессов регистрации избирателей, просмотра списков избирателей. Такие системы должны работать автономно, без зависимости от подключения к интернету, что позволит снизить риск потенциальных хакерских атак.

Еще одним важным вопросом, который необходимо учитывать в системе администрирования, является контроль получения цифровых бюллетеней избирателем в цифровом виде. Необходимо внедрение инструментов для сбора и верификации подписи (цифровой подписи) избирателя.

Кроме того, система администрирования позволила бы международным и местным наблюдателям получать аккредитацию в удаленном формате.

В день голосования на избирательном участке единая система администрирования ускорила бы поиск записей избирателей в электронных журналах, подготовку отчетов о явке избирателей в режиме реального времени в течение дня. Такая информация актуальна для СМИ, ведь только информация о явке избирателей может быть предана огласке до закрытия избирательных участков.

После выборов система администрирования избирательного процесса служит для оптимизации подведения итогов. В отличие от систем регистрации избирателей, информационные системы, поддерживающие передачу результатов с избирательных участков на центральный уровень, не демонстрируют прозрачности, тем не менее их популярность продолжает

⁸⁵ Haque Z., Carroll D. Assessing the Impact of Information and Communication Technologies on Electoral Integrity // Election Law Journal: Rules, Politics, and Policy. — 2020. — № 2 (19). — P. 127-148.

расти, поскольку в информационном обществе важны своевременные результаты. Единая система администрирования полезна для расчета мандатов в парламенте на основе результатов выборов, а также может использоваться для отображения результатов выборов на федеральном/национальном, региональном и муниципальном уровнях (вплоть до уровня избирательных участков).

Безопасность избирательного процесса

3.1. Деятельность государств СНГ по обеспечению электоральной безопасности

Азербайджанская Республика

Концептуальные подходы к обеспечению электоральной безопасности Азербайджанской Республики изложены в Конституции Азербайджанской Республики, Законе Азербайджанской Республики «О национальной безопасности» от 29 июня 2004 г.⁸⁶ (далее — Закон о национальной безопасности) и Концепции национальной безопасности Азербайджанской Республики от 23 мая 2007 г.⁸⁷ В Азербайджане выборы и референдумы являются двумя основными средствами выражения гражданами мнения и внесения предложений, касающихся национальных интересов государства⁸⁸. Избирательная система представляет собой составляющую конституционного строя, граждане и организаторы выборов — объекты национальной безопасности. В соответствии со статьей 5 Закона Азербайджанской Республики «О национальной безопасности» среди основных принципов обеспечения национальной безопасности — соблюдение избирательных прав, сохранение баланса между интересами личности, общества и государства и их взаимная ответственность. Статья 112 Конституции Азербайджанской Республики

⁸⁶ О национальной безопасности: Закон Азербайджанской Республики от 29 июня 2004 г. № 712-III. URL: https://republic.preslib.az/tu_d4-74.html.

⁸⁷ Концепция национальной безопасности Азербайджанской Республики: утв. распоряжением Президента Азербайджанской Республики от 23 мая 2007 г. № 2198. URL: <http://eurasian-defence.ru/?q=node/30535>.

⁸⁸ Статья 12 Закона о национальной безопасности Азербайджанской Республики.

предусматривает введение чрезвычайного положения при возникновении конфликтов, создающих угрозу для нормальной деятельности государственных институтов, в том числе организаторов выборов.

Защита избирательной системы и избирательных прав граждан Азербайджанской Республики представляет собой составляющую национальных интересов в политической и информационной сферах (политическая сфера: защита конституционного строя, демократического правового светского государства, обеспечение прав и свобод человека и гражданина, обеспечение политической стабильности; информационная сфера: обеспечение таких конституционных прав граждан, как получение законным путем, передача, подготовка и распространение информации, защита и развитие информационных ресурсов). Примечательно, что законодательство Азербайджана предусматривает разграничение внутренних и внешних угроз электоральной безопасности (посягательство на конституционный строй, нарушение прав и свобод человека и гражданина, давление на демократические институты внутри страны и извне, разрушение организационной структуры государственных органов, нарушение их деятельности, снижение уровня управления в стране). Основными угрозами в информационной сфере, связанными с электоральной безопасностью, являются: отставание в области информационных технологий, информационная агрессия со стороны других стран, искажение на международной арене правды об Азербайджане, посягательства на свободу информации, на информационную систему и ресурсы.

В Концепции национальной безопасности Азербайджанской Республики 2007 г. вмешательство в избирательные процессы не выделяется как угроза национальной безопасности, хотя и упоминается невмешательство во внутренние дела в качестве основополагающего принципа международного права. Вместе с тем национальные интересы Азербайджана включают в себя обеспечение прав и основных свобод человека, в том числе избирательных прав, а также усиление выполнения государственных функций путем обеспечения развития демократических институтов и институтов гражданского общества.

В качестве угроз национальной безопасности в Концепции признаются посягательства на суверенитет и конституционный

строй Азербайджанской Республики, а также деятельность, направленная против выполнения государственных функций в сфере демократического государственного устройства, верховенства закона, защиты прав и основных свобод человека. Карабахский вопрос в Концепции рассматривается преимущественно с военной и экономической точек зрения.

В Концепции национальной безопасности Азербайджанской Республики отдельный параграф посвящен укреплению демократии в качестве одного из основных внутривнутриполитических средств обеспечения безопасности. В параграфе содержится отсылка к развитию «избирательной практики» как наиболее важного вопроса в процессе демократических реформ. Электоральный элемент информационной безопасности не выделяется, хотя в Концепции отмечается необходимость охраны государственных информационных ресурсов и информационной инфраструктуры.

Республика Армения

Стратегия национальной безопасности Республики Армения принята в 2020 г. на период до 2025 г. В ней закреплено, что свободное волеизъявление народа является единственным источником формирования власти, а обеспечение прав человека и верховенства права признается национальным интересом республики⁸⁹. Хотя в документе не упоминаются избирательные права и свободы, всё же права человека утверждены в нем как гарантия развития эффективной системы государственного управления и внутренней устойчивости страны. Документ не квалифицирует защищенность этих прав как электоральную безопасность, но в то же время регламентирует развитие высокоустойчивой системы государственного управления как инструмент обеспечения государственной и общественной безопасности.

Стратегия национальной безопасности имеет сильный уклон в сторону внешнеполитических угроз национальной безопасности. В том же ключе — как элемент международного

⁸⁹ Стратегия национальной безопасности Республики Армения // Правительство Республики Армения: официальный сайт. URL: <https://www.gov.am/ru/National-Security-Strategy/>.

противостояния, но не внутренних противоречий — упомянута угроза регрессии демократии и прав человека в регионе и в мире.

Дискредитация государственных институтов в указанном документе коррелируется с коррупционными проявлениями, при этом коррупция понимается в общем смысле, без привязки к электоральным процессам. Электоральные процессы упомянуты как элемент права народов на самоопределение.

В заключительной части Стратегии национальной безопасности Республики Армения высокий уровень доверия к государственным институтам называется в качестве гарантии обеспечения национальной безопасности. Подчеркивается, что Армения стремится к продолжительному улучшению институциональных механизмов свободных, справедливых и прозрачных выборов и повышению доверия к выборам. Кроме того, в руководящем документе по безопасности упоминается необходимость более высокого уровня вовлечения отдельных социальных групп, особенно женщин, в процессы государственного управления. Также в Стратегии подчеркивается, что отдельным направлением обеспечения избирательных прав станет развитие эффективной деятельности органов самоуправления.

В части информационной безопасности в Стратегии фиксируется признание кибератак на национальные информационные ресурсы в качестве угроз. В то же время в документе делается вывод, что целью информационного вмешательства становятся «демократические ценности», а это понятие намного шире, чем понятие «избирательные процессы». В связи с этим в Стратегии национальной безопасности Республики Армения перечисляются вызовы национальной безопасности: несовершенство государственной политики, регулирующей сферу информационной и кибербезопасности, отсутствие законодательства, обеспечивающего защиту критической информационной инфраструктуры, неудовлетворительный уровень институциональных возможностей структур реагирования на компьютерные инциденты и отсутствие структуры, координирующей сферу кибербезопасности. Упомянут риск использования технологий иностранного происхождения в критической информационной инфраструктуре.

Республика Беларусь

Элементы электоральной безопасности Республики Беларусь стали нововведением проекта Концепции национальной безопасности Республики Беларусь, принятого постановлением Совета Безопасности Республики Беларусь № 1 от 6 марта 2023 г.⁹⁰ Как и в предыдущей редакции документа, стратегическим национальным интересом в электоральной сфере является обеспечение суверенитета и незыблемости конституционного строя Республики Беларусь. Избирательные процессы выступают связующим звеном между гражданами и национальными интересами: свое видение национальных интересов, способов и средств их защиты граждане реализуют путем участия в выборах, референдумах и других формах непосредственной демократии, а также через государственные органы и органы местного самоуправления. В отличие от предыдущей Концепции, в принятом документе закреплено, что белорусская общественно-политическая модель основана на принципах народовластия, верховенства норм права, незыблемости основ конституционного строя, баланса интересов личности, общества и государства (ранее из принципов были упомянуты лишь демократия и верховенство права).

Одно из существенных отличий новой редакции Концепции заключается в выделении электоральной безопасности в особую подсистему политической безопасности. Если посягательство на конституционный строй и вмешательство извне во внутривнутриполитические процессы были квалифицированы в качестве основных угроз безопасности еще в предыдущей редакции концепции (2010 г.), то в проекте Концепции, принятом в 2023 г., вводятся понятия электорального суверенитета и информационного суверенитета. Понятие информационного суверенитета пока не раскрывается, хотя в документе перечислены основные национальные интересы в информационной сфере (надежное и устойчивое функционирование национальных информационных систем и инфраструктуры, ресурсов субъектов информационных от-

⁹⁰ О рассмотрении проекта новой Концепции национальной безопасности Республики Беларусь»: постановление Совета Безопасности Республики Беларусь от 6 марта 2023 г. № 1 // Национальный правовой интернет-портал Республики Беларусь. URL: <https://pravo.by/document/?guid=3871&p0=P223s0001>.

ношений и т. д.). Электоральный суверенитет определяется как неотъемлемое и исключительное право государства самостоятельно и независимо организовывать и проводить выборы, референдумы в целях обеспечения реализации полновластия народа и свободы его выбора при верховенстве Конституции Республики Беларусь и национального законодательства, недопущения вмешательства в избирательный процесс. Три важнейших элемента электоральной безопасности: обеспечение электорального суверенитета, обеспечение эффективного функционирования государственных институтов в интересах общества, а также достижение сбалансированности политических интересов граждан, общественных объединений и государства, — признаются основными национальными интересами в политической сфере. В качестве основного национального интереса закреплено и обеспечение условий для реализации конституционных прав граждан, куда входят в том числе и избирательные права.

В проекте Концепции обращается внимание и на кибербезопасность критической инфраструктуры, отмечено, что в условиях глобальной цифровизации и больших данных обеспечение кибербезопасности приобретает исключительное значение. В проекте основными национальными интересами в информационной сфере признаны два элемента, связанных с электоральной безопасностью: реализация прав граждан на получение, хранение и распространение информации, а также надежное и устойчивое функционирование национальных информационных систем и инфраструктуры, ресурсов субъектов информационных отношений.

В проекте документа ряд угроз, связанных с электоральными процессами, признаются основными угрозами национальной безопасности. Большая часть из них уже была закреплена в предыдущей редакции: вмешательство во внутренние дела, резкое либо масштабное снижение доверия граждан к основным государственным и прогосударственным общественным институтам, дезорганизация системы государственного управления, создание препятствий функционированию государственных и общественных институтов, деструктивное информационное воздействие на личность. Нововведением является квалификация в качестве основной угрозы нарушения киберустойчивости

национального сегмента сети «Интернет», критически важных объектов информатизации и государственных информационных систем, а также неправомерных действий в отношении персональных данных. Эти два элемента имеют первостепенное значение для обеспечения электоральной безопасности.

Примечателен методологический подход, в соответствии с которым в проекте Концепции выделены внутренние и внешние источники угроз электоральной безопасности. Среди внутренних источников угроз: использование в политической деятельности методов, заведомо направленных на дестабилизацию обстановки в Республике Беларусь, осуществление действий, направленных на дискредитацию либо срыв электоральных кампаний. Также к угрозам электоральной безопасности следует отнести неуважительное отношение к государственным символам и формирование негативного образа государства, так как государственные символы и образ государства служат основой организации выборов и референдумов. К внутренним источникам угроз электоральной безопасности в проекте Концепции отнесены посягательства на государственные символы, манипулирование механизмами международных организаций для дискредитации избирательной системы.

Республика Казахстан

Изложение концепции электоральной безопасности Казахстана содержится в Стратегии национальной безопасности Республики Казахстан на 2021–2025 гг.⁹¹ и Законе Республики Казахстан «О национальной безопасности Республики Казахстан» от 6 января 2012 г. № 527-IV⁹² (далее — Закон о национальной безопасности). Основой обеспечения электоральной составляющей безопасности в политической сфере является безопасность

⁹¹ Глава государства подписал Указ «Об утверждении Стратегии национальной безопасности Республики Казахстан на 2021–2025 годы» // Президент Республики Казахстан: официальный сайт. URL: <https://www.akorda.kz/ru/glava-gosudarstva-podpisal-ukaz-ob-utverzhenii-strategii-nacionalnoy-bezopasnosti-respubliki-kazahstan-na-2021-2025-gody-215354>.

⁹² О национальной безопасности Республики Казахстан: Закон Республики Казахстан от 6 января 2012 г. № 527-IV (с изменениями и дополнениями по состоянию на 26 февраля 2023 г.). URL: https://online.zakon.kz/Document/?doc_id=31106860&show_di=1.

в области человеческого капитала. В сфере информационной безопасности важная роль отводится противодействию растущим киберугрозам, защите персональных данных казахстанцев, информационной инфраструктуры, стратегических объектов и повышению защищенности национального информационного пространства в целом.

Стратегия национальной безопасности является составной частью Системы государственного планирования в Республике Казахстан, новая редакция которой была утверждена в 2021 г.⁹⁵ Система государственного планирования предусматривает мониторинг выполнения задач по развитию страны, в том числе и в области электоральной безопасности, на среднесрочный (от года до пяти лет включительно) и долгосрочный (свыше пяти лет) периоды.

В соответствии с Законом о национальной безопасности обеспечение прав граждан, включая их избирательные права, выступает одним из основных принципов обеспечения национальной безопасности. Электоральная безопасность в законодательстве Республики Казахстан рассматривается как подвид политической безопасности — состояния защищенности основ конституционного строя, деятельности системы государственных органов и порядка государственного управления от угроз, при котором обеспечивается соблюдение прав и свобод граждан, социальных групп и баланс их интересов. Таким образом, в определении политической безопасности выделяется «порядок государственного управления», к которому следует отнести и избирательную систему.

В Законе о национальной безопасности перечислены основные национальные интересы Республики Казахстан, среди которых есть и интересы, касающиеся электоральной сферы. Это обеспечение прав граждан, общественное согласие и политическая стабильность в стране, незыблемость конституционного строя и президентской формы правления, устойчивое функционирование государственных институтов, защита национального информационного пространства. Деятельность, направленная

⁹⁵ Об утверждении Системы государственного планирования в Республике Казахстан: постановление Правительства Республики Казахстан от 29 ноября 2017 г. № 790. URL: <https://adilet.zan.kz/rus/docs/P1700000790>.

на насильственное изменение конституционного строя Казахстана, дезорганизация деятельности государственных органов, снижение уровня защищенности информационного пространства — эти процессы признаны законодательством основными угрозами национальной безопасности. С 24 ноября 2022 г. в качестве основной угрозы национальной безопасности признано использование денег или имущества от иностранных организаций и лиц для проведения общественных собраний, если их целью является свержение конституционного строя. Таким образом, вмешательство в избирательные процессы с целью дискредитации избирательной системы соотносится с основной угрозой национальной безопасности. Даже в случае отсутствия иностранного финансирования вмешательство будет угрозой ввиду дезорганизации и нарушения бесперебойного функционирования государственных органов.

Реализация гражданами своих избирательных прав предполагает участие граждан в реализации государственной политики в области обеспечения национальной безопасности. При этом статьей 17 Закона о национальной безопасности предусмотрен принцип пропорционального ограничения избирательных прав в целях защиты конституционного строя, а соответственно, избирательной системы.

Отличие концептуального оформления электоральной безопасности в Республике Казахстан заключается в распределении элементов электоральной сферы по общественной, политической и информационной безопасности. В случае с другими государствами СНГ обеспечение электоральной безопасности, как правило, затрагивает политическую и информационную безопасность. В общественную безопасность входит укрепление гарантий обеспечения избирательных прав граждан, в политическую — защита конституционного строя и государственного суверенитета, обеспечение безопасности государственных институтов в области организации выборов, борьба с насильственным прекращением полномочий или воспрепятствованием деятельности избирательных органов и должностных лиц. В информационную безопасность включены недопущение информационной зависимости, обеспечение бесперебойной и устойчивой эксплуатации сетей связи, развитие эффективной

системы защиты информационных ресурсов, информационных систем и инфраструктуры связи. Особому контролю подлежит деятельность организаций с иностранным участием, осуществляющих управление сетями связи и их эксплуатацию. Кроме того, иностранным лицам запрещено владеть, пользоваться, распоряжаться и (или) управлять более чем 20% акций (долей, паев) юридического лица, являющегося собственником СМИ в Республике Казахстан или осуществляющего деятельность в этой сфере. Запрещено управление линиями связи со стороны иностранных лиц без создания юридического лица на территории Казахстана, при этом центр управления сетями связи не может быть размещен за пределами республики.

Кыргызская Республика

Концептуальные элементы электоральной безопасности Кыргызской Республики изложены в Законе Кыргызской Республики от 26 февраля 2003 г. № 44 «О национальной безопасности Кыргызской Республики»⁹⁴ и Концепции национальной безопасности Кыргызской Республики (приложение к Указу Президента Кыргызской Республики от 20 декабря 2021 г. № 570⁹⁵).

В Концепции национальной безопасности республики не выделен подвид политической безопасности, хотя выделено состояние защищенности личности, общества и государства от информационных угроз — информационная безопасность. Во введении к документу отмечены проблемы активизации методов информационно-технического и информационно-психологического воздействия на системы управления государств. Внешние угрозы, упомянутые в Концепции, имеют косвенное отношение к электоральной безопасности. Например, такая внешняя угроза, как гибридные и хакерские атаки на жизненно важные сферы обеспечения деятельности государства, несомненно, несет риски в том числе и для электоральной информационной инфраструктуры: серверов, сетей передачи, личных данных ор-

⁹⁴ О национальной безопасности: Закон Кыргызской Республики от 26 февраля 2003 г. № 44. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/1168?cl=ru-ru#st_10.

⁹⁵ Концепция национальной безопасности Кыргызской Республики к Указу Президента Кыргызской Республики от 20 декабря 2021 г. № 570. URL: <http://cbd.minjust.gov.kg/act/properties/ru-ru/430815/10>.

ганизаторов выборов и избирателей. Внутренние угрозы национальной безопасности Кыргызстана, упомянутые в Концепции, несут большие риски для электоральной безопасности. Это коррупционные проявления в государственных органах, обострение социально-политической обстановки, активизация деструктивной деятельности в социальных сетях, нарушение избирательных прав граждан, рост правового нигилизма, недостаточное развитие защищенности национального информационного пространства страны.

В числе целей обеспечения национальной безопасности традиционно установлены защита конституционного строя и суверенитета, а также соблюдение прав граждан. Эти же процессы перечислены в параграфе 5 как национальные интересы. В национальные интересы Кыргызстана в области национальной безопасности входит в том числе поддержание устойчивости политической системы и обеспечение преемственности власти, что имеет прямое отношение к защите избирательной системы.

В Концепции национальной безопасности Кыргызстана отдельно упоминается угроза политизации религии под прикрытием благотворительной, образовательной или другой социально значимой деятельности. Политизация религии, например в виде создания религиозных партий, на определенном этапе не проявляет признаков экстремизма и насилия, хотя влечет риски радикализации граждан. В Кыргызстане остро стоит проблема стабильного роста числа молодых людей, отправляющихся в зарубежные религиозные образовательные учреждения. Часть из них служит площадками для вербовки в экстремистские организации, которые, в свою очередь, используют граждан для распространения экстремистской политики и идеологии в Кыргызстане. Использование для этих целей избирательных процессов не только маскирует экстремистскую деятельность, но и масштабирует информационный эффект.

Вмешательство в избирательные процессы концептуально связано с проведением «войн нового поколения», или «гибридных войн», когда под видом политической борьбы осуществляются пропаганда по дискредитации избирательной системы, кибератаки на электоральную критическую инфраструктуру, подготовка незаконных вооруженных группировок. Существен-

ную часть таких операций составляют действия в информационной сфере. В Кыргызстане проблемами, связанными с информационной и электоральной сферой, признаны увеличение технологического отрыва других государств, усиливающее зависимость республики от использования зарубежной техники и программного обеспечения для защиты критических информационных инфраструктур, приобретение импортных технических и программно-аппаратных средств, а также средств защиты информации при создании и развитии собственной информационной инфраструктуры. Персональные данные, собираемые в ходе выборов, также защищены Концепцией: в качестве задачи по обеспечению информационной безопасности закреплено усиление ответственности должностных лиц за утечку и утрату персональных данных.

Республика Молдова

Стратегия национальной безопасности Республики Молдова была утверждена постановлением Парламента Республики Молдова № 153 в 2011 г. (до этого действовала утвержденная в 2008 г. Концепция⁹⁶), изменена в 2017 г. и 2023 г. Новая редакция Стратегии национальной безопасности вступила в силу 24 марта 2023 г.⁹⁷ В ней традиционно упоминаются суверенитет, защита прав и свобод человека, укрепление демократии в качестве национальных интересов Республики Молдова, основным же инструментом для защиты и продвижения национальных интересов государства признается «процесс европейской интеграции».

В новой редакции Стратегии обеспечение электоральной безопасности нацелено на нивелирование угрозы снижения политической стабильности. Угроза нестабильности напрямую связывается с чрезмерной частотой электоральных циклов. В качестве инструмента обеспечения электоральной безопасности

⁹⁶ Об утверждении Концепции национальной безопасности Республики Молдова: Закон Республики Молдова от 22 мая 2008 г. № 112. URL: <http://lex.justice.md/viewdoc.php?action=view&view=doc&id=328010&lang=2>.

⁹⁷ Об утверждении Стратегии национальной безопасности Республики Молдова: постановление Парламента Республики Молдова от 15 июля 2011 г. № 153. URL: https://www.legis.md/cautare/getResults?doc_id=105346&lang=ru.

предлагается внедрить «европейские нормы конструктивного диалога между политическими формированиями, особенно вовлеченными в электоральные процессы». На практике Стратегия предлагает проводить широкие консультации с внешними партнерами, включая Совет Европы, Европейский союз, Венецианскую комиссию и иных партнеров, выступающих за «истинные демократические ценности». Среди других инструментов: интеграция страны в ЕС; поддержание взаимовыгодных отношений и налаживание стратегических партнерств с Европейским союзом, Румынией, Украиной, США и Россией; развитие международного сотрудничества с целью заимствования у стран ЕС опыта построения действенного сектора национальной безопасности.

Среди главных угроз национальной безопасности, несущих высокие риски для электоральной сферы Молдовы, упомянуты внешнее давление, криминогенный фактор, коррупция и низкая информационная безопасность. Способность Молдовы отвечать на эти риски, по мнению авторов Стратегии, зависит от «сокращения разрыва в демократическом, экономическом и технологическом развитии между Молдовой и развитыми европейскими странами». Информационные риски, связанные с электоральной безопасностью, упомянуты в документе довольно расплывчато, без конкретных инструментов. В нем признано, что роль информационных технологий в обеспечении безопасности государства возрастает, в ней также закреплено, что одной из приоритетных задач является повышение надежности коммуникационных сетей. Вместе с тем развитие национального сегмента в документе не упоминается, имеется лишь отсылка к «государственному потенциалу для выполнения безопасного обмена информацией». По проблеме защиты личных данных не определено конкретных инструментов, только отмечено, что «будет рассмотрена возможность усиления механизмов защиты персональных данных для исключения их использования в незаконных или политических целях».

Иностранное вмешательство конкретно в избирательные процессы не упоминается в Стратегии. Вместе с тем указано, что провокации медийного характера, попытки дезинформации или манипуляционного информирования извне касаются

информационной безопасности. В качестве инструмента противодействия данным провокациям отмечены «консультации с гражданским обществом».

Сбалансированность политических интересов и безопасность избирательных процессов понимается в Стратегии в качестве социальной безопасности. Консолидация общества в Молдове, согласно этому документу, осуществляется посредством внедрения критериев Евросоюза в соответствии с обязательствами, взятыми на себя Республикой Молдова в Совете Европы и других международных организациях. При этом СНГ упоминается в Стратегии лишь единожды — как организация, в которой Молдова не обсуждает военно-политические проблемы. В контексте социальной безопасности упомянута нацеленность Молдовы обеспечивать избирательные права этнических и других меньшинств.

Российская Федерация

В России концептуальные основы электоральной безопасности содержатся в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400⁹⁸.

Безопасность избирательных процессов соотносится в Стратегии с политической стабильностью, суверенной государственностью, противостоянием внешнему давлению, защитой конституционного строя, прав и свобод человека и гражданина.

Среди национальных интересов, связанных с электоральной безопасностью, отмечены защита конституционного строя и независимости, развитие безопасного информационного пространства, укрепление законности и защита граждан. Электоральная безопасность не выделена в отдельную подсистему, но косвенно реализуется через обеспечение ряда стратегических национальных приоритетов: государственной и общественной безопасности, а также информационной безопасности. Отдельные элементы электоральной безопасности обеспечены в рамках экономической и научно-технологической безопасности. Это — усиление конт-

⁹⁸ О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400. URL: <http://publication.pravo.gov.ru/Document/View/0001202107030001>.

роля за иностранными инвестициями в электоральную информационную инфраструктуру (программы мониторинга и подсчета, камеры для наблюдения, оборудование избирательных комиссий), укрепление технологической независимости, совершенствование системы фундаментальных научных исследований, развитие перспективных высоких информационно-коммуникационных технологий и суперкомпьютерных систем.

В Стратегии замечено, что обеспечение электоральной безопасности связано с противодействием деструктивным силам как за рубежом, так и внутри страны. Деструктивные силы используют объективные социально-экономические трудности для стимулирования негативных социальных процессов, обострения межнациональных и межконфессиональных конфликтов, манипулирования в информационной сфере через распространение недостоверной информации. В частности, манипулирование преследует цель организации незаконных публичных акций. В связи с этим электоральные задачи российской государственной политики включают:

1) недопущение вмешательства во внутренние дела, пресечение посягательств на основы конституционного строя, права и свободы человека и гражданина путем инспирирования «цветных революций»;

2) совершенствование системы общественного контроля, механизмов участия граждан и организаций в обеспечении государственной и общественной безопасности, в том числе в электоральной сфере;

3) обеспечение правовой защиты граждан и юридических лиц от политически ангажированных решений иностранных и международных (межгосударственных) судов, в том числе в случае электоральных санкций.

В разделе об информационной безопасности отмечается проблема расширения использования информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности. Отдельно отмечена проблема распространения недостоверной информации, в частности заведомо ложных сообщений об угрозе террористических актов. Установлена цель укрепления информационного суверенитета

Российской Федерации в информационном пространстве, так как использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов, включая объекты критической информационной инфраструктуры Российской Федерации, для воздействия из-за рубежа. С электоральной безопасностью связаны следующие задачи государственной политики в информационной сфере:

1) повышение защищенности национальной информационной инфраструктуры и устойчивости ее функционирования;

2) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры;

3) снижение до минимально возможного уровня количества утечек персональных данных;

4) обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий;

5) обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности.

Немаловажно, что в Стратегии принцип невмешательства проецируется на международные отношения Российской Федерации. Подчеркивается, что устойчивость системы международных отношений зависит от безусловного соблюдения норм международного права, включая принцип невмешательства, при разрешении глобальных и региональных проблем. В случае совершения вмешательства с использованием информационно-коммуникационных технологий, представляющих угрозу суверенитету Российской Федерации, считается правомерным принятие таких мер, чтобы не только пресечь, но и предотвратить вмешательство в будущем. Достижение целей внешней политики Российской Федерации обеспечивается в том числе через оказание союзникам и партнерам Российской Федерации поддержки при решении ими вопросов, связанных с нейтрализацией попыток внешнего вмешательства в их внутренние дела.

Республика Таджикистан

Стратегия национальной безопасности Республики Таджикистан основана на Законе Республики Таджикистан от 28 июня 2011 г. № 721 «О безопасности»⁹⁹.

Уважение и соблюдение прав и свобод человека и гражданина выступают одним из принципов обеспечения безопасности в Таджикистане наряду с принципом взаимной ответственности граждан, общества и государства в области обеспечения безопасности. Обеспечение избирательных прав граждан в качестве составляющей прав и свобод человека и гражданина является одним из основных национальных интересов Республики Таджикистан. Другим национальным интересом в соответствии с Законом Республики Таджикистан «О безопасности» (далее — Закон о безопасности) признается избирательная система. Незыблемость конституционного строя, республиканской формы правления, устойчивое функционирование государственных институтов, укрепление и повышение эффективности их деятельности — все это отнесено законодательством к национальным интересам Республики Таджикистан. Угрозы безопасности не разделены на внешние и внутренние, хотя выделены внутренние и внешние источники угроз, внутренняя и внешняя безопасность. К электоральной безопасности имеют отношение следующие угрозы безопасности: деятельность, направленная на насильственное изменение конституционного строя; дезорганизация деятельности государственных органов, органов самоуправления, нарушение их бесперебойного функционирования, снижение степени управляемости; осложнение социально-политической ситуации, выражающееся в межнациональных и межрелигиозных конфликтах, массовых беспорядках, несанкционированных собраниях, митингах, шествиях, демонстрациях и незаконных забастовках.

Электоральные элементы, такие как единство народа, права и свободы граждан, общественное согласие и политическая стабильность, регламентированы законодательством Таджикистана

⁹⁹ О безопасности: Закон Республики Таджикистан от 28 июня 2011 г. № 721 (в редакции законов от 27 ноября 2014 г. № 1137, 15 марта 2016 г. № 1283, 3 августа 2018 г. № 1540). URL: https://ncz.tj/system/files/Legislation/721_ru.pdf.

в контексте обеспечения общественной безопасности. Деятельность по обеспечению электоральной безопасности в Таджикистане отличается акцентом на предотвращение политизации конфессиональных и религиозных различий: законом Таджикистана предусмотрена особая ответственность представителей политических партий и общественных объединений за призывы к свержению или насильственному изменению конституционного строя, захвату власти, насильственному прекращению полномочий или воспрепятствованию деятельности государственных органов, использованию существующих конфессиональных различий и разных религиозных воззрений в политических целях.

Отдельные элементы безопасности в электоральной сфере регулируются в рамках обеспечения информационной безопасности и безопасности государственных институтов. В Законе о безопасности установлена необходимость укрепления национальной системы защиты информации для недопущения информационной зависимости Таджикистана, информационной изоляции органов государственной власти, информационной экспансии и блокады со стороны других государств. К безопасности государственных институтов отнесено бесперебойное функционирование единой системы государственных органов, к которым можно причислить и избирательные комиссии, хотя в законе не содержится отсылки к ним.

Туркменистан

Концептуальные основы обеспечения национальной безопасности Туркменистана заложены в Законе Туркменистана от 4 мая 2013 г. № 388-IV «О национальной безопасности Туркменистана». В стратегии национальной безопасности страны предусмотрено разделение угроз на внутренние и внешние, а конституционный строй, жизнь, права и свободы человека признаны объектами национальной безопасности. К принципам обеспечения национальной безопасности также относятся баланс интересов человека и гражданина, общества и государства, их взаимная ответственность.

Электоральные элементы безопасности установлены в рамках обеспечения общественной, политической, информационной безопасности. В число основных национальных интересов

включены обеспечение прав и свобод человека и гражданина, сохранение общественного согласия и политической стабильности, незыблемость конституционного строя, независимости и нейтралитета, устойчивое функционирование государственных институтов, повышение эффективности их деятельности, защита национального информационного пространства.

В стратегии обеспечения национальной безопасности Туркменистана определены основные угрозы для избирательных процессов: 1) обострение социальной и политической обстановки, межнациональные и межрелигиозные конфликты, массовые беспорядки; 2) действия, направленные на насильственное изменение конституционного строя Туркменистана; 3) дезорганизация деятельности государственных органов, нарушение их бесперебойного функционирования, снижение степени управляемости в стране; 4) снижение уровня защищенности информационного пространства, в том числе национальных информационных ресурсов; 5) негативное воздействие на общественное сознание путем распространения недостоверной информации.

В рамках обеспечения общественной безопасности не допускается принятие решений, способных привести: 1) к нарушению единства народа и ухудшению межнациональных, религиозных и этнических отношений; 2) нарушению общественной солидарности, единства; 3) необоснованному ограничению прав и свобод; 4) незаконному вмешательству общественных объединений, религиозных организаций и групп в дела государства. Обеспечение политической безопасности государства также содержит элементы, касающиеся электоральной безопасности. Это защита основ конституционного строя и государственного суверенитета, совершенствование деятельности государственных органов и порядка государственного управления, обеспечение безопасности государственных органов. В рамках обеспечения политической безопасности законодательство Туркменистана регламентирует, что деятельность граждан, политических партий и общественных объединений не может быть направлена на свержение или насильственное изменение конституционного строя, захват власти, насильственное прекращение полномочий или воспрепятствование деятельности органов и должностных лиц. В Туркменистане не допускается принятие решений или совершение действий,

препятствующих формированию и бесперебойному функционированию целостной, единой системы государственных органов. Обеспечение информационной безопасности Туркменистана предполагает обеспечение информационной независимости, предотвращение информационной экспансии и блокады со стороны других государств, организаций и отдельных лиц, обнаружение и дезорганизацию механизмов скрытого информационного влияния на процесс выработки и принятия государственных решений в ущерб национальной безопасности, развитие системы защиты информационных ресурсов, систем и инфраструктуры связи. Отдельно регламентируется контроль за организациями по управлению линиями связи с иностранным участием. Управление основными линиями связи или их эксплуатация иностранными юридическими лицами запрещена. Также запрещены создание и работа на территории Туркменистана сетей связи, центр управления которыми расположен за его пределами.

Республика Узбекистан

В 2022 г. Президент Республики Узбекистан Ш. Мирзиёев выступил с предложением обновить Концепцию национальной безопасности Республики Узбекистан в виде конституционного закона¹⁰⁰. Концептуальные основы электоральной безопасности Узбекистана содержатся в Законе Республики Узбекистан от 5 апреля 2018 г. № ЗРУ-471 «О службе государственной безопасности Республики Узбекистан», а также в комплексной концепции общественной безопасности, утвержденной Указом Президента Республики Узбекистан № УП-27 от 29 ноября 2021 г. В последний документ входят Концепция общественной безопасности Республики Узбекистан, Стратегия развития системы обеспечения общественной безопасности в Республике Узбекистан на 2022–2025 годы, «Дорожная карта» по реализации в 2022 году Стратегии развития системы обеспечения общественной безопасности в Республике Узбекистан на 2022–2025 годы.

¹⁰⁰ Выступление Президента Республики Узбекистан Ш. Мирзиёева на встрече с членами Конституционной комиссии Олий Мажлиса // Исполнительный комитет СНГ. — 2022. — 21 июня. URL: https://cis.minsk.by/news/23676/vystuplenie_prezidenta_respubliki_uzbekistan_sh.mirzijoeva_na_vstreche_s_chlenami_konstitucionnoj_komissii_olij_mazhlisa.

В соответствии с Законом Республики Узбекистан «О службе государственной безопасности Республики Узбекистан» избирательные процессы соотносятся с государственными интересами Республики Узбекистан: обеспечение верховенства закона, безопасности и стабильности в обществе, защиты конституционного строя и суверенитета. В числе национальных интересов в сфере обеспечения общественной безопасности Республики Узбекистан зафиксированы следующие элементы электоральной безопасности: 1) обеспечение общественно-политической стабильности общества; 2) расширение участия общественности в построении правового демократического государства и сильного гражданского общества, укреплении системы государственного и общественного управления, управлении делами государства и общества. Защита и уважение прав, свобод и законных интересов граждан регламентированы как принцип обеспечения общественной безопасности. Обеспечение общественной безопасности осуществляется во взаимодействии государственных органов и организаций, органов самоуправления граждан, негосударственных некоммерческих организаций, общественных формирований, граждан и средств массовой информации. Среди основных задач Стратегии развития системы общественной безопасности названо доведение уровня цифровизации системы общественной безопасности до 90% (по доле документооборота).

3.2. Региональные механизмы обеспечения электоральной безопасности в СНГ

В национальных концепциях безопасности государств СНГ электоральная безопасность не выделена в качестве подсистемы. Как правило, безопасность избирательного процесса обеспечивается в рамках политической и информационной безопасности, в отдельных случаях — общественной безопасности. Характерной для концепций всех стран Содружества (за исключением новой редакции концепции в Молдове) формулировкой, связанной с обеспечением безопасности избирательных процессов, стала «защита конституционного строя» (в Молдове — «кон-

ституционного порядка»). Особый акцент на вмешательстве в избирательные процессы сделан в концепциях национальной безопасности Республики Беларусь, Кыргызской Республики, Российской Федерации, Республики Таджикистан, Туркменистана. В то же время во всех концепциях отмечена необходимость обеспечения политической стабильности, баланса политических и общественных сил, предотвращения посягательств на суверенитет.

Тематика электоральной безопасности и электорального суверенитета стала актуальной в последние годы на фоне учащающихся попыток иностранного вмешательства. Совместимость концепций национальной безопасности стран региона обусловила согласование подходов на региональном уровне. Региональные механизмы — договоры, модельное законодательство, консультативные структуры — в основном нацелены на содействие государствам в предотвращении внешнего вмешательства, то есть вмешательства иностранных субъектов. Внутреннее вмешательство в выборы остается прерогативой государств, этим объясняется уклон региональных структур, в частности в области межпарламентского сотрудничества, в противодействие именно внешнему вмешательству. Между тем в СНГ работа в области противодействия новым угрозам безопасности на многостороннем уровне уже ведется. Концепция электоральной безопасности государств СНГ могла бы усилить международный компонент координации в рамках Содружества, а также закрепить в качестве стратегических интересов региона обеспечение электоральной безопасности и развитие национально ориентированных избирательных систем.

Основным и на данный момент единственным международным договором в области электоральных стандартов является Конвенция о стандартах демократических выборов, избирательных прав и свобод в государствах — участниках Содружества Независимых Государств от 7 октября 2002 г. (Конвенция СНГ)¹⁰¹. В ней закреплено, что проведение выборов и реализация иных форм народовластия должны осуществляться на

¹⁰¹ Стандарты демократических выборов: история и практика / А. С. Бояшов, В. И. Лысенко, И. И. Мушкет [и др.]. — Санкт-Петербург: Секретариат Совета МПА СНГ, 2023. — 136 с. — (Демократия, выборы, парламентаризм).

основе верховенства права и национального законодательства, а также максимального учета национальных и исторических традиций.

В числе рекомендательных документов в области электоральной безопасности надо отметить модельный закон «О национальной безопасности», принятый МПА СНГ в 2022 г. в Самарканде. В нем предпринята попытка гармонизации норм законодательства государств СНГ, обуславливающая необходимость уточнения отдельных формулировок национальных законов. Так, в модельном законе выделены «национальные интересы», «важные национальные интересы», «жизненные национальные интересы», «значимые национальные интересы», «национальные цели», «национальные стратегические приоритеты», тогда как концепции национальной безопасности СНГ, как правило, включают в себя лишь понятие «национальные интересы». Отдельное достоинство модельного закона заключается в определении критически важной инфраструктуры как объектов, систем и служб, разрушение или выведение из строя которых может привести к нарушению или прекращению функционирования органов государственной власти, государственных органов, органов местного самоуправления (управления) и создаваемых гражданами институтов. Такое определение позволяет обеспечить защиту критической электоральной информационной инфраструктуры. На данный момент не все информационные электоральные системы в СНГ относятся к категории критических. Необходимо обсудить возможность отнесения личных данных избирателей и организаторов выборов также к критической информационной инфраструктуре, как следствие выделения электоральной безопасности в отдельную подсистему. В рамках защиты конституционного строя следует отдельно закрепить обеспечение устойчивости избирательных систем и электоральных кампаний. Во всех концепциях национальной безопасности стран Содружества упомянута необходимость защиты национального информационного сегмента. В модельном законодательстве или концепции на уровне СНГ можно было бы учесть данный факт при разработке государственных подходов к «суверенному интернету» и «технологической независимости».

С точки зрения необходимости системного обеспечения электоральной безопасности целесообразно объединить принципы международного наблюдения, имеющие отношение к безопасности избирательного процесса. На данный момент, если исходить из содержания модельного закона «О международном наблюдении за выборами и референдумами» (постановление МПА СНГ от 28 октября 2022 г. № 54-4), к принципам международного наблюдения относятся принципы уважения суверенитета, профессионализма, беспристрастности, невмешательства в избирательный процесс, безопасности, взаимности. Каждый из них предполагает сотрудничество с государством, знание национального законодательства и международных стандартов, реализацию права на развитие (учет национальных и исторических особенностей), обеспечение электоральной безопасности.

Это же наблюдение касается и Рекомендаций МПА СНГ по противодействию иностранному вмешательству в национальные выборы и референдумы, а также проекта концепции по защите электорального суверенитета. Принципиально учесть в данных рекомендациях существующее на национальном уровне разделение внутренних и внешних источников угроз безопасности, разделение в случае некоторых государств внутренней и внешней национальной безопасности и зафиксировать принцип невмешательства в электоральную безопасность. Концентрация лишь на иностранном вмешательстве не позволяет учитывать использование иностранными субъектами внутренних участников для осуществления вмешательства. Для этих случаев рекомендации квалифицируют деятельность внутренних субъектов как деятельность в интересах иностранных лиц (в случае «правовой связи с иностранными субъектами»), что не всегда легко установить.

Парламентской Ассамблеей Организации Договора о коллективной безопасности в 2019 г. приняты Рекомендации по гармонизации законодательства государств — членов ОДКБ по обеспечению внутренней стабильности и противодействию технологиям внешнего деструктивного воздействия, направленного на дестабилизацию социально-политической обстановки. 1 июля 2021 г. Совет ПА ОДКБ принял Заявление о недопустимости иностранного вмешательства в избирательные процессы государств — членов Организации.

О повышенном внимании государств к электоральной безопасности свидетельствует утверждение 5 декабря 2022 г. Парламентской Ассамблеей ОДКБ Рекомендаций по совершенствованию законодательства в области обеспечения защиты электоральных процессов и суверенитета в государствах — членах ОДКБ¹⁰². С электоральной безопасностью в Рекомендациях связана защита электоральных процессов и электорального суверенитета. Достоинство Рекомендаций заключается в разработке понятий «иностранный вмешательство» и «электоральный суверенитет». В то же время Рекомендации отличает чрезмерное внимание именно к иностранному вмешательству, не к электоральной безопасности в целом. С одной стороны, принятие Рекомендаций позволяет государствам ОДКБ выйти с общей инициативой в области иностранного невмешательства в выборы в Генеральную Ассамблею ООН, что расширит пространство для переговоров с государствами Латинской Америки, Африканского региона, Азии. С другой стороны, практическое исполнение Рекомендаций в самих государствах будет иметь сложности из-за чрезмерного внимания к иностранному вмешательству: грань между внутренними и внешними источниками вмешательства, как правило, размыта, а субъектам вмешательства проще скрыться именно через территорию сопредельных стран.

Кроме этого, в вышеуказанных рекомендациях МПА СНГ и ПА ОДКБ безопасность избирательного процесса рассматривается узко, как противодействие иностранному вмешательству в ходе формальной электоральной кампании (от объявления ее начала до подведения итогов). Практика показывает, что иностранное вмешательство сопряжено с обострением внутренних противоречий и готовится еще до начала избирательной кампании. Например, в международных структурах типа Управления Верховного комиссара ООН по правам человека через инструмент дополнительного финансирования создаются целые депар-

¹⁰² Рекомендации по совершенствованию законодательства в области обеспечения защиты электоральных процессов и суверенитета в государствах — членах ОДКБ: утв. постановлением Парламентской Ассамблеи ОДКБ от 5 декабря 2022 г. URL: <https://paodkb.org/documents/rekomendatsii-po-sovershenstvovaniyu-zakonodatelstva-v-oblasti-obespecheniya>.

таменты по оценкам выборов: оценка такими структурами выборов 2020 г. в Беларуси выступает подготовкой к вмешательству в будущие электоральные кампании и нацелена на отдельные слои населения¹⁰³.

Практическую работу в области региональной электоральной безопасности ведут две организации СНГ: Международный институт мониторинга развития демократии, парламентаризма и соблюдения избирательных прав граждан государств — участников МПА СНГ (МИМРД МПА СНГ) и недавно созданный Консультативный совет руководителей избирательных органов государств — участников СНГ (Консультативный совет ЦИК).

МИМРД выполняет функции вспомогательного консультативного органа МПА СНГ, содействует обмену информацией, обобщению передового опыта по развитию демократии и парламентаризма, соблюдению избирательных прав граждан. Институт осуществляет аналитическую, научную, методическую, учебно-консультативную деятельность; проводит мониторинг выборов и референдумов; взаимодействует с международными и партнерскими организациями. Отличительной особенностью МИМРД является наличие филиалов в некоторых столицах СНГ. Филиалы позволяют сотрудничать с научными институтами, вести информационную, учебную, организационную деятельность непосредственно в странах Содружества. Такой механизм позволяет гармонизировать национальные подходы к электоральной безопасности, учесть исторические и национальные особенности при многосторонней координации.

Консультативный совет ЦИК был создан 14 октября 2022 г. на заседании Совета глав государств СНГ. Совет был создан для обмена опытом по вопросам обеспечения избирательных прав и свобод граждан, совершенствования правовых условий проведения выборов и референдумов в соответствии с национальным

¹⁰³ Бояшов А. С. Инструменты интеграционных структур Содружества по противодействию приватизации гуманитарного сотрудничества // Гармонизация интеграционных процессов на евразийском пространстве: материалы международного круглого стола по инновациям в международных исследованиях / под ред. О. Н. Лешенюка, А. М. Байчорова, А. В. Русаковича. — Минск: БГУ, 2022. — С. 10–20.

законодательством и международными обязательствами стран Содружества.

Указанные механизмы ни в коей мере не обеспечивают электоральную безопасность государств, но выполняют вспомогательную функцию в информационном и аналитическом сопровождении международного сотрудничества по вопросам электоральной безопасности: невмешательства, развития избирательной системы, реализации прав граждан. В настоящий момент особенно актуальной задачей представляется обеспечение координации между основными механизмами, устранение излишней бюрократизации и «разделение труда» с целью устранения аппаратной конкуренции¹⁰⁴.

¹⁰⁴ Лешенюк О. Н. Потенциал интеграционных структур в области стандартизации регионального экономического сотрудничества // Евразия. Эксперт: аналитический портал о евразийской интеграции. — 2021. — № 3. — С. 38–42.

Заключение

Развитие цифровых технологий в сфере электоральной безопасности полностью соответствует духу и требованиям времени. Новые технологии во многом упрощают работу избирательных комиссий, участков, обеспечивают избирателям возможность удаленного голосования, считают голоса. Однако обеспечение гарантий цифровых процессов повышает риски, связанные с технической оптимизацией участков, защитой данных и кибербезопасностью, противодействием вмешательству. Появляются новые цифровые технологии, применяемые в электоральных процессах, создается программная инфраструктура для обеспечения бесперебойной работы. Возникает общественный запрос на «цифровые партии», которые не только отстаивают цифровые технологии и защиту данных, но и устроены по принципу «политического блокчейна»: когда делегат в парламенте проводит оперативный электронный опрос избирателей своего округа или членов партии. Если в случае «цифровых партий» еще понятно, каким образом будет выстроена работа «цифровых парламентариев», то с «цифровыми референдумами» дело обстоит сложнее. Оперативные цифровые общенациональные референдумы со временем могут потеснить парламенты в области принятия законодательных актов или привести к тому, что политические партии будут организованы по функциональному (военные, научные, финансовые, промышленные, рабочие), а не идеологическому признаку.

Попытки цифровизации избирательных процессов предпринимаются во многих странах мира, однако преодолеть все трудности и требования электорального процесса — задача не из легких. Страны экспериментируют, внедряют элементы цифровизации, иногда возвращаются к традиционному голосованию. На момент написания данной книги ни одна цифровая избирательная система не была на 100% устойчивой и безопасной.

Цифровизация электорального процесса осуществляется на принципах доступности, инклюзивности, экономии ресурсов, надежности и оперативности передачи результатов голосования, транспарентности, анонимности и сохранения тайны голосования, защиты данных, контроля и администрирования избирательного процесса, приоритетности избирательного участка, безопасности электорального процесса и предупреждения множественного голосования.

Государства СНГ накапливают опыт в цифровизации электоральной сферы, некоторые из них уже вполне уверенно двигаются к успеху, другие делают первые шаги в этом направлении. Программное обеспечение, цифровые сервисы и устройства разрабатываются для всех участников электорального процесса: избирателей, кандидатов и (или) политических партий и объединений, избирательных комиссий. Цифровое администрирование выборов позволит: внедрить системы, которые будут отражать все аспекты управления электоральным процессом на предвыборном этапе, в день голосования, после выборов; выстроить архитектуру поддержки ИКТ-инфраструктуры избирательных округов; учесть многие другие аспекты, включая финансы, киберпреступность и т. д.

Один из серьезных вызовов использования цифровых технологий в электоральном процессе — потенциальное воздействие на идеологические предпочтения избирателей со стороны третьих лиц и организаций. В этих целях используются: искусственный интеллект и нейротехнологии, блокчейн, «интернет вещей», виртуальная и дополненная реальность, квантовые технологии, технологии создания «цифровых двойников», электорального позиционирования и мобилизации, привлечения волонтеров и коммуникации, в том числе через социальные сети и мессенджеры, Big Data и т. д. Несмотря на такой широкий перечень цифровых возможностей, интернет-голосование не сможет стать аналогом традиционному голосованию по причине «цифрового неравенства»: не все избиратели имеют равный доступ к цифровым возможностям. Будет проводиться работа по снятию технических и репутационных барьеров, вызванных необходимостью защиты персональных данных и обеспечения гарантий электоральной безопасности.

Каковы возможности и риски цифровизации избирательных систем государств — участников СНГ с точки зрения обеспечения электоральной безопасности? Цифровизация избирательных систем стоит дорого, но приносит пользу в стратегической перспективе. Для этого необходимо обеспечить устойчивость избирательной системы через комплексный мониторинг электоральной безопасности. Одно из достоинств цифровизации — возможность мониторинга количественных показателей электоральной безопасности (помимо традиционной явки), таких как электронные заявления граждан, использование блокчейн-технологий, распределение избирателей по демографическим характеристикам (все то, что связано с доверием граждан к государственным институтам или участием граждан в государственных делах). Недостаток цифровизации состоит в том, что обеспечить защиту национального информационного сегмента, личных данных граждан, а также критической электоральной инфраструктуры можно лишь на высоком уровне технологического развития. С этой точки зрения электоральная безопасность требует развития фундаментальной науки, качественного образования, плотной региональной координации.

Результаты анализа данного исследования показали, что в государствах — участниках СНГ электоральная безопасность не выделена в особую подсистему национальной безопасности, а входит в политическую и информационную безопасность. Вместе с тем представляется необходимым уже в краткосрочной перспективе обеспечить не только невмешательство иностранных субъектов, но и нейтрализацию внутренних источников угроз электоральной безопасности. Обеспечение устойчивости избирательной системы и защита народа как источника государственной власти является стратегическим интересом государств СНГ.

Анализ прикладной и академической литературы показывает, что основными национальными интересами в электоральной сфере являются: 1) обеспечение гражданам права избирать и быть избранными; 2) устойчивое развитие постоянно действующих институтов бесперебойного прямого волеизъявления; 3) обеспечение сбалансированности интересов и недискриминации общественных групп, организаций и государственных органов по вопросам государственного развития; 4) устойчивость

явки и поступательное развитие правовой культуры граждан; 5) обеспечение защиты личных данных граждан в ходе цифровизации избирательных систем.

К основным угрозам национальной безопасности в электоральной сфере следует отнести: 1) посягательства на суверенитет и конституционный строй; 2) дискредитацию избирательной системы; 3) дезорганизацию системы государственного управления, создание препятствий функционированию государственных и общественных институтов; 4) деструктивное информационное воздействие на личность, общество; 5) резкое либо масштабное снижение доверия граждан к основным государственным и прогосударственным общественным институтам и, как следствие, снижение участия; 6) цифровую уязвимость электоральной инфраструктуры.

Источники угроз национальной безопасности в электоральной сфере целесообразно разделять на внешние и внутренние. Внутренними источниками угроз являются: 1) нарушение избирательных прав и свобод человека, принципа верховенства права; 2) использование в политической, экономической, общественной и иной деятельности методов, заведомо направленных на дискредитацию избирательной системы; 3) осуществление действий, направленных на срыв электоральных кампаний; 4) профессиональная неподготовленность организаторов избирательных процессов; 5) недостаточное развитие цифровых технологий защиты электоральной инфраструктуры.

К внешним источникам угроз целесообразно отнести: 1) кризис партийного строительства в странах «старых демократий»; 2) нарастание противоречий между разными политическими и избирательными системами; 3) расширение участников международных процессов за счет неправительственного сегмента с целью продвижения избирательных систем отдельных стран; 4) смешение мандатов международных организаций с целью вмешательства под видом международного наблюдения; 5) использование санкций для влияния на выбор граждан; 6) технологическое неравенство, обуславливающее цифровую зависимость от отдельных стран и корпораций; 7) концентрацию информационных ресурсов в узкой группе государств и транснациональных корпораций.

Необходимость обеспечения электоральной безопасности объясняет более высокие требования к профессионализму и невмешательству со стороны субъектов, не являющихся непосредственными участниками избирательных процессов, например международных наблюдателей и иностранных СМИ. Сегодня учащаются попытки западных государств и международных структур заявить претензии как на оценку выборов, так и на включение отдельных экспертов в круг субъектов избирательных процессов иностранных государств. Так, специальные докладчики международных организаций предлагают квалифицировать международных наблюдателей как правозащитников, при этом спецдокладчики произвольно расширяют свои мандаты, претендуя на оценку выборов. Примечательно, что подобное вмешательство осуществляется задолго до выборов и, скорее всего, имеет целью достижение эффекта дестабилизации, пусть и отсроченного.

Литература

Алексеев Р. А., Абрамов А. В. Проблемы и перспективы применения электронного голосования и технологии избирательного блокчейна в России и за рубежом // Гражданин. Выборы. Власть. — 2020. — № 1. — С. 9–13.

Антушин Н. А. Избирательная поддержка в эпоху дискурса «внешнего вмешательства» // Российская государственность на пути в будущее: традиции и траектории политико-правовых реформ: материалы IX научно-практической конференции по исследованию российской государственности (Владимир, 15 октября 2021 г.). — Владимир: Владимирский филиал РАНХИГС, 2021. — С. 139–145.

Борисов И. Б. Вмешательство в национальные выборы как сопутствующий фактор демократических процессов в глобальном мире // Гражданин. Выборы. Власть. — 2021. — № 3 (21). — С. 122.

Борисов И. Б. Иностранцы (международные) организации на выборах в Российской Федерации: правовая «халатность» или вынужденная необходимость // Гражданин. Выборы. Власть. — 2018. — № 3. — С. 40–57.

Борисов И. Б. Трансформация избирательных систем под воздействием неблагоприятных факторов // Гражданин. Выборы. Власть. — 2022. — № 2 (24). — С. 43.

Борисов И. Б. Электоральный суверенитет. — Москва: РОИИП, 2010. — 94 с.

Бояшов А. С. Инструменты интеграционных структур Содружества по противодействию приватизации гуманитарного сотрудничества // Гармонизация интеграционных процессов на евразийском пространстве: материалы международного круглого стола по инновациям в международных исследованиях / под ред. О. Н. Лешенюка, А. М. Байчорова, А. В. Русаковича. — Минск: БГУ, 2022. — С. 10–20.

Бояшов А. С. Президент в Послании неслучайно обратил внимание на электоральную безопасность // СБ. Беларусь сегодня. — 2023. — 24 мая. URL: <https://www.sb.by/articles/prezident-v-poslanii-nesluchayno-obratil-vnimanie-na-elektoralnuyu-bezopasnost-ekspert-iz-bgu.html>.

Бродовская Е. В., Домбровская А. Ю., Карзубов Д. Н., Синяков А. В. Развитие методологии и методики интеллектуального поиска цифровых маркеров политических процессов в социальных медиа // Мониторинг общественного мнения: экономические и социальные перемены. — 2017. — № 5. — С. 79–104.

Бубнов А. Ю., Шаповалов В. Л., Дмитриева О. В. Интенсивность вовлеченности россиян в интернет-коммуникацию // Мониторинг общественного мнения: экономические и социальные перемены. — 2013. — № 3. — С. 19–27.

Ватыль В. Н. Защита государственного суверенитета в Республике Беларусь: противодействие деструктивным угрозам в политической сфере // Вестник Гродненского государственного университета имени Янки Купалы. Серия 1: История и археология. Философия. Политология. — 2023. — № 1. — С. 123–128.

Володенков С. В. Big Data как инструмент воздействия на современный политический процесс: особенности, потенциал и акторы // Журнал политических исследований. — 2019. — № 1. — С. 7–13.

Выступление Президента Республики Узбекистан Ш. Мирзиёева на встрече с членами Конституционной комиссии Олий Мажлиса // Исполнительный комитет СНГ. — 2022. — 21 июня. URL: https://cis.minsk.by/news/23676/vystuplenie_prezidenta_respubliki_uzbekistan_sh.mirzijoeva_na_vstreche_s_chlenami_konstitucionnoj_komissii_olij_mazhlisa.

Герасимов В. В. Основные тенденции развития форм и способов применения ВС, актуальные задачи военной науки по их совершенствованию: доклад на общем собрании Академии военных наук, 2013. URL: <https://vpk-news.ru/articles/14632>.

Гольтяев А. О. Соотношение прав человека и развития: новые веяния в Совете ООН по правам человека // Современное право. — 2017. — № 11. — С. 119–121.

Грачев М. Н. Электронное голосование «за» и «против» // Известия Тульского государственного университета. — 2011. — № 1. — С. 360–366.

Гугняк В. Я. Жан Боден (1530–1596) как представитель раннего меркантилизма // Вопросы экономики и права. — 2015. — № 5. — С. 80–85.

Давыдов Д. А. Интернет-голосование как электоральная политическая технология // Вестник Пермского университета. — 2010. — № 1 (9). — С. 59.

Евстафьев Д. Г. Информационные манипуляции и государственный суверенитет: риски для России // Гражданин. Выборы. Власть. — 2019. — № 2 (12). — С. 98–110.

Евстифеев Р. В. Иностранное вмешательство в национальные выборы в цифровую эпоху: постановка проблемы и перспективы исследований // Вестник РГГУ. Серия: Политология. История. Международные отношения. — 2022. — № 3. — С. 10–27.

Зиновьева Е. С. Проблема «цифрового вмешательства» в российско-американских отношениях // Российский совет по международным делам. — 2020. — 23 октября. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/problema-tsifrovogo-vmeshatelstva-v-rossiysko-amerikanskikh-otnosheniyakh/>.

Косоруков А. А., Котлярова Т. Ю. Информационно-коммуникационные технологии как фактор трансформации публичной сферы современного общества // Тренды и управление. — 2018. — № 4. — С. 88–96.

Кочетова П. О., Тепляшин П. В. Криминологические аспекты электоральной преступности: понятие, структура и формы // Актуальные вопросы юридической науки. — 2019. — № 4 (4). — С. 89–97.

Лешенюк О. Н. Потенциал интеграционных структур в области стандартизации регионального экономического сотрудничества // Евразия. Эксперт: аналитический портал о евразийской интеграции. — 2021. — № 3. — С. 38–42.

Лешенок О. Н. Укрепление электоральной безопасности через синхронизацию межпарламентского компонента Союзного государства, ОДКБ, СНГ // Региональная политика, политическая география и геополитика. История и современность: материалы международной научной конференции, посвященной 20-летию кафедры региональной политики и политической географии СПбГУ / под ред. Н. М. Михеевой, Н. В. Каледина. — Санкт-Петербург: Издательство ВВМ, 2022. — С. 719–725.

Манойло А. В., Авдеева Н. В., Лавринов Б. Б. Внешнее вмешательство в выборы как угроза безопасности Российской Федерации // Гражданин. Выборы. Власть. — 2018. — № 3. — С. 58–91.

Международное наблюдение за выборами / А. С. Бояшов, И. И. Мушкет, С. Г. Караваев [и др.]. — Санкт-Петербург: Секретариат Совета МПА СНГ, 2021. — 84 с. — (Демократия, выборы, парламентаризм).

Мушкет И. И., Амбурцев Р. А., Ксендзов А. Н. Противодействие иностранному вмешательству в электоральные процессы: опыт государств — участников Межпарламентской Ассамблеи СНГ // Право. Безопасность. Чрезвычайные ситуации. — 2022. — № 2 (55). — С. 52–62.

Несмашный А. О. Интернет-технологии в политике: проблема интерпретации понятия // Среднерусский вестник общественных наук. — 2017. — № 1. — С. 157–164.

Пильгун Е. В. Политическое манипулирование через идеологизацию кризиса // Управление и политика. — 2022. — № 1 (2). — С. 30–43.

Пильгун Е. В. Семантика и прагматика кризисного дискурса. — Минск: ИВЦ Минфина, 2020. — 203 с.

Прогнозируемые вызовы и угрозы национальной безопасности Российской Федерации и направления их нейтрализации / под общей редакцией А. С. Коржевского; редакционная коллегия: В. В. Толстых, И. А. Копылов. — Москва: РГГУ, 2021. — С. 42–48.

Рекомендации для международных наблюдателей от Содружества Независимых Государств по наблюдению за выборами и референдумами (новая редакция). — Санкт-Петербург: Секретариат Совета МПА СНГ, 2023. — 144 с.

Стандарты демократических выборов: история и практика / А. С. Бояшов, В. И. Лысенко, И. И. Мушкет [и др.]. — Санкт-Петербург: Секретариат Совета МПА СНГ, 2023. — 136 с. — (Демократия, выборы, парламентаризм).

Тимофеев И. Н., Чарап С. Кодекс невмешательства. Российский совет по международным делам. — 2019. — 14 июня. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/kodeks-nevmeshatelstva/>.

Титовская А. В. Электронное тайное голосование в России и за рубежом: сравнительно-правовой анализ // Юридическая наука. — 2012. — № 4. — С. 106.

Федоров В. И. Электронное голосование как имиджевый донор: случай Кыргызстана // Избирательное законодательство и практика. — 2018. — № 4. — С. 35–37.

Фельдман П. Я. Концептуализация понятия «электоральное вмешательство» в эпоху «гибридных войн» // Известия Тульского государственного университета. Гуманитарные науки. — 2018. — № 4. — С. 3–12.

Фельдман П. Я., Федакин А. В., Ежов Д. А. Технологии вмешательства в выборы: научное осмысление в поисках семантической определенности // Вестник Томского государственного университета. Философия. Социология. Политология. — 2019. — № 50. — С. 210–218.

Boyashov A. Network Governance of the UN Human Rights Council. Diplomatic, Institutional, and Organizational Actors. — New York: Routledge, 2022. — 180 p.

Buzan B., Wæver O., Wilde J. de. Security: A New Framework for Analysis. — London: Lynne Rienner, 1998. — 239 p.

Corstange D., Marinov N. Taking Sides in Other People's Elections: The Polarizing Effect of Foreign Intervention // American Journal of Political Science. — 2012. — № 3. — P. 655–670.

Defending Democracies Combating Foreign Election Interference in a Digital Age. / ed. by Hollis D., Ohlin J. — New York: Oxford University Press, 2021. — 400 p.

Elections, Violence and Transitional Justice in Africa / ed. by Opongo E., Murithi T. — New York: Routledge, 2022. — 202 p.

Haque Z., Carroll D. Assessing the Impact of Information and Communication Technologies on Electoral Integrity // Election Law Journal: Rules, Politics, and Policy. — 2020. — № 2 (19). — P. 127–148.

Miller M. Shock to the System // Coups, Elections, and War on the Road to Democratization. — New Jersey: Princeton University Press, 2021. — 348 p.

National Intelligence Council. Foreign Threats to the 2020 US Federal Elections // Office of the Director of National Intelligence. URL: <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf>.

Senate Intel Committee Releases Unclassified 1st Installment in Russia Report, Updated Recommendations on Election Security // U. S. Senate Select Committee on Intelligence. — 2018. — May 8. URL: <https://www.intelligence.senate.gov/press/senate-intel-committee-releases-unclassified-1st-installment-russia-report-updated>.

Zanden J. L. van. Colonial State Formation and Patterns of Economic Development in Java, 1800–1913 // Economic History of Developing Regions. — 2010. — № 2 (25). — P. 155–176.

Willard-Foster M. Toppling Foreign Governments: The Logic of Regime Change. — Philadelphia: University of Pennsylvania Press, 2018. — 344 p.

Оглавление

Введение	3
Глава 1. Электоральная безопасность государства	11
1.1. Электоральная безопасность государства в ходе проведения выборов и референдумов.	12
1.2. Национальные интересы государства и источники угроз электоральной безопасности	19
Глава 2. Цифровые технологии в избирательном процессе	31
2.1. Опыт внедрения цифровых технологий в избирательные процессы.	32
2.2. Перспективы цифровизации выборов и референдумов в государствах СНГ	36
2.3. Технологии цифрового вмешательства в выборы и референдумы	48
Глава 3. Безопасность избирательного процесса	58
3.1. Деятельность государств СНГ по обеспечению электоральной безопасности	58
3.2. Региональные механизмы обеспечения электоральной безопасности в СНГ	78
Заключение	85
Литература	90

Авторский коллектив

Бояшов Анатолий Сергеевич, эксперт МИМРД МПА СНГ, советник Белорусского института стратегических исследований, кандидат политических наук.

Мушкет Иван Ильич, заместитель руководителя Секретариата Совета МПА СНГ — директор Международного института мониторинга развития демократии, парламентаризма и соблюдения избирательных прав граждан государств — участников МПА СНГ, доктор юридических наук, профессор, почетный работник сферы образования Российской Федерации.

Лешенюк Олег Николаевич, эксперт МИМРД МПА СНГ, директор центра международных исследований факультета международных отношений Белорусского государственного университета (заместитель декана факультета международных отношений на общественных началах по международной деятельности и интернационализации образования).

Амбурцев Роман Альбертович, начальник отдела аналитики и мониторинга выборов МИМРД МПА СНГ.

Караваяев Сергей Георгиевич, советник Генерального секретаря — руководителя Секретариата Совета МПА СНГ, кандидат юридических наук.

Ксендзов Александр Николаевич, начальник отдела по работе с филиалами МИМРД МПА СНГ.

Научное издание

ДЕМОКРАТИЯ, ВЫБОРЫ, ПАРЛАМЕНТАРИЗМ

Бояшов Анатолий Сергеевич,
Мушкет Иван Ильич,
Лешенюк Олег Николаевич,
Амбурцев Роман Альбертович,
Караваев Сергей Георгиевич,
Ксендзов Александр Николаевич

БЕЗОПАСНОСТЬ ИЗБИРАТЕЛЬНОГО ПРОЦЕССА

Редакторы: *А. В. Разумеева, Н. В. Куликова*

Компьютерная верстка: *А. Г. Закиров*

Подписано в печать 18.04.2023. Формат 60×84¹/₁₆. Бумага офсетная.
Гарнитура PT Astra. Усл. печ. л. 5,58. Тираж 300 экз. Заказ № рп-67803

Адрес Секретариата Совета МПА СНГ:
191015, С.-Петербург, Шпалерная ул., д. 47.

Телефон редакции: +7 (812) 404-57-05.

web-страница: www.iacis.ru; e-mail: kia@iacis.ru.

Отпечатано с оригинал-макета в ООО «Принт»:
190020, Санкт-Петербург,
наб. Обводного канала, д. 136, корп. 1, лит. Б, оф. 1Н-165

ISBN 978-5-86857-045-2



9 785868 570452 >