DOI: 10.17803/1994-1471.2026.185.4.176-182

А. В. Шапошников*

# Система правового регулирования практик противодействия киберугрозам для цифрового оборудования избирательных комиссий в США

***Аннотация.*** В рамках исследования анализируется система правового регулирования практик противодействия киберугрозам для цифрового оборудования избирательных комиссий в Соединенных Штатах Америки. Автор приходит к выводу, что, несмотря на отсутствие закрепленных и унифицированных на уровне федерального законодательства норм, правовая основа работы избиркомов в плане обеспечения безопасности цифрового оборудования в целом может быть охарактеризована как удовлетворительная. Наличие существенных правовых лакун в значительной степени компенсируется воздействием двух взаимовлияющих факторов. С одной стороны, Комиссия США по содействию выборам и Агентство по кибербезопасности и защите инфраструктуры предоставляют в распоряжение организаторов выборов в США качественное методическое обеспечение для противодействия киберугрозам. С другой стороны, система неформального двухпартийного контроля над организацией выборов обеспечивает выполнение организаторами голосования большинства рекомендаций федеральных органов, поскольку их игнорирование какой-либо из политических сил подразумевает предоставление конкурирующей партии возможного преимущества.

***Ключевые слова:*** киберугрозы; цифровое оборудование; избирательные комиссии; выборы; США; правовое регулирование; кибербезопасность; электронное голосование; избирательная инфраструктура; сертификация оборудования; двухпартийный контроль; защита информации

***Для цитирования:*** *Шапошников А. В.* Система правового регулирования практик противодействия киберугрозам для цифрового оборудования избирательных комиссий в США // Актуальные проблемы российского права. — 2026. — Т. 21. — № 4. — С. 176–182. — DOI: 10.17803/1994-1471.2026.185.4.176-182



* *Шапошников Алексей Валерьевич*, председатель Московской городской Думы, кандидат юридических наук, заслуженный юрист Российской Федерации, доцент кафедры конституционного и муниципального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Страстной бул., д. 15/29, стр. 1, г. Москва, Российская Федерация, 127994
Lab.kkmp@msal.ru

## The Legal Framework for Countering Cyber Threats to Digital Equipment of Election Commissions in the United States

**Aleksey V. Shaposhnikov**, Chairman of the Moscow City Duma, Cand. Sci. (Law), Honored Lawyer of the Russian Federation, Associate Professor, Department of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
Lab.kkmp@msal.ru

***Abstract.*** The study analyzes the legal framework for countering cyber threats to digital equipment of election commissions in the United States of America. The author concludes that, despite the lack of established and unified norms at the federal legislative level, the legal basis for the work of election commissions in terms of ensuring the security of digital equipment can generally be characterized as satisfactory. The presence of significant legal gaps is largely compensated by the influence of two mutually influencing factors. On the one hand, the US Election Assistance Commission and the Cybersecurity and Infrastructure Security Agency provide US election officials with high-quality methodological support to counter cyber threats. On the other hand, the system of informal bipartisan control over the organization of elections ensures that election organizers comply with most of the recommendations of federal bodies, since ignoring them by any of the political forces implies giving the competing party a possible advantage.

***Keywords:*** cyber threats; digital equipment; election commissions; elections; USA; legal regulation; cybersecurity; electronic voting; electoral infrastructure; equipment certification; bipartisan control; information security
***Cite as:*** Shaposhnikov AV. The Legal Framework for Countering Cyber Threats to Digital Equipment of Election Commissions in the United States. *Aktual'nye problemy rossijskogo prava*. 2026;21(4):176-182. (In Russ.). DOI: 10.17803/1994-1471.2026.185.4.176-182

Изменение форм осуществления функций государства под воздействием цифровизации — и в этом мы согласимся с В. В. Комаровой — оказывает прямое воздействие на механизмы реализации политических прав. Однако развитие этого процесса зачастую затрудняется в силу недостаточно высоких темпов совершенствования системы правового регулирования. В результате даже представители законодательной власти вынуждены описывать формирующиеся механизмы реализации политических прав посредством неправовых, собирательных понятий. Наглядным примером может служить понятие «электронная демократия» (на данный момент его содержание, согласно нормативным правовым актам, сводится к электронным формам получения государственных или муниципальных услуг). Отсутствие четких концептуальных представлений о роли цифровизации и ее инструментов в процессе развития системы политических прав граждан на фоне наличия значимых пробелов в соответствующих разделах законодательства приводит к ситуации, в рамках которой перед экспертным сообществом встает ряд принципиально важных вопросов. Востребованность и направления конкретных изменений в законодательстве, выбор государством методов правового воздействия на процесс цифровизации электоральных процедур, делегирование соответствующих задач определенным акторам нормотворчества и его объем — каждый из названных элементов служит поводом для активных дискуссий. И это закономерно осложняет задачу инкорпорирования в правовую действительность электронных механизмов, используемых при осуществлении народовластия, включая проведение выборов и референдумов[1], что в перспективе может

[1] *Комарова В. В.* Политические права граждан России в цифровой среде // Право и цифровая экономика. 2021. № 4 (14). С. 63–72 ; *Она же.* Электронная демократия: мифы и реальность // Ученые записки Худжандского государственного университета имени академика Б. Гафурова. Серия гуманитарно-общественных наук. 2016. № 3 (48). С. 44–52.

привести к возникновению проблем в рамках функционирования столь важного конституционно-правового института, как формирование представительного органа. В данном случае уместно сослаться на позицию Е. И. Козловой о значимости данного института с точки зрения обеспечения единства любого представительного органа[2]. Отметим, что, имея сравнительно недавнюю историю, цифровые технологии зарекомендовали себя в качестве эффективного средства предотвращения нарушений и фальсификаций в ходе свободного, политически значимого волеизъявления граждан РФ[3].

Это закономерно актуализирует задачу освоения зарубежного опыта использования цифрового оборудования в рамках организации избирательного процесса. В первую очередь это касается практик, призванных обеспечить доверие избирателей к результатам голосования (в том числе в рамках противодействия киберугрозам). В качестве конкретного исследовательского кейса нами избраны США, что обусловлено наличием сопоставимых с Россией по масштабам организационных задач в рамках проведения выборов, достаточно широким использованием цифрового оборудования и повышенным вниманием властей Соединенных Штатов к пресечению возможностей вмешательства в электоральный процесс посредством технологических уязвимостей.

В соответствии с законодательством США право определения механизмов защиты цифровых процедур в ходе избирательного процесса делегировано на уровень штатов и местных юрисдикций. Федеральный законодатель закрепил за общенациональными органами публичной власти в лице Комиссии США по содействию выборам (U.S. Election Assistance Commission (далее — EAC)) лишь право вырабатывать общие рекомендации относительно соблюдения норм безопасности со стороны организаторов выборов (в отношении использования замков и пломб, камер видеонаблюдения и т.д.)[4].

Как следствие, участие в программе сертификации национальной системы голосования EAC носит лишь добровольный характер. Однако правоприменительная практика свидетельствует о том, что в реальности речь идет об общеобязательном комплексе мер. Последнее обусловлено тем, что в масштабах избирательной системы в целом в соблюдении стандартов EAC заинтересованы члены двух крупнейших партий — республиканской и демократической. Более того, именно их представители внутри экспертного сообщества и органов власти (в первую очередь в лице федеральных агентств) оказывают основное влияние на процесс выработки и утверждения рекомендаций EAC[5].

На уровне штатов за регламентацию процесса обеспечения безопасности цифровых процедур в рамках избирательного процесса в большинстве случаев отвечают местные легислатуры, а контроль за выполнением требований утвержденных нормативных правовых актов осуществляют секретари штатов[6].

В большинстве случаев стандартный протокол обеспечения безопасности волеизъявления граждан от киберугроз включает в себя:

— приобретение проверенных и сертифицированных EAC цифровых систем, используемых в ходе голосования, и программного обеспечения к ним;

---

2 *Козлова Е. И.* Обоснование новых концепций российской конституции в правовой теории // Lex russica. 2009. Т. 68. № 2. С. 311–321.

3 *Шапошников А. В.* Конституционно-правовое регулирование использования цифровых технологий при осуществлении видеонаблюдения за выборами и референдумами // Актуальные проблемы российского права. 2023. № 10. С. 20–27.

4 *Barber B.* If Mayors Ruled the World: Dysfunctional Nations, Rising Cities. Yale University Press, 2013. P. 217.

5 *Hodgson Q. E., Chan E. W., Bodine-Baron E.,* et al. Securing U.S. Elections: A Method for Prioritizing Cybersecurity Risk in Election Infrastructure // URL: https://www.rand.org/pubs/research_reports/RRA512-1.html (дата обращения: 01.06.2023).

6 *Lindner R.*, *Aichholzer G.* E-Democracy: Conceptual Foundations and Recent Trends // European E-Democracy in Practice / L. Hennen, I. van Keulen, I. Korthagen et al. (eds.). Springer, 2020. P. 15.

— организацию контроля за физическим доступом к машинам для голосования;

— проверку качества работы цифрового оборудования для голосования перед выборами с участием наблюдателей;

— обеспечение доступа к контролю за ходом голосования наблюдателей от демократов и республиканцев;

— ручную проверку бюллетеней для обеспечения точного подсчета голосов цифровым оборудованием.

В числе передовых практик, закрепленных в обеспечительных процедурах на уровне законодательства штатов, зарубежные исследователи отмечают:

— хранение цифрового оборудования в помещениях с ограниченным доступом (при помощи ключ-карты) и видеонаблюдением;

— запрет на подключение используемых для формирования бюллетеня компьютеров к Интернету или другой внешней сети;

— организацию регулярного просмотра журналов пользователей и их действий членами комиссии;

— периодическую проверку программного обеспечения компьютера на предмет отсутствия изменений[7].

В ряде штатов на уровне законодательства графств используются дополнительные обеспечительные процедуры. Так, программирование цифрового оборудования (панелей для голосования с сенсорным экраном и сканеров) специально доверяется группе из двух человек (их принадлежность к двум доминирующим партиям может как закрепляться в нормативных правовых актах, так и не использоваться в качестве «фигуры умолчания»). При этом данная процедура осуществляется посредством USB-носителя или иного устройства, предназначенного для хранения информации. После ее завершения сотрудники избирательных комиссий прикрепляют к оборудованию пломбы с целью защиты от несанкционированного доступа.

В большинстве случаев законы штата и муниципальные нормативные правовые акты предписывают должностным лицам избирательных комиссий документировать любые перемещения цифрового оборудования, а также фиксировать информацию о состоянии пломб и местоположении устройств для голосования. Следует подчеркнуть, что в большинстве штатов закон обязывает членов комиссии отслеживать состояние каждой части оборудования для голосования[8].

Во многих «колеблющихся» штатах (избиратели которых не демонстрируют явного предпочтения по отношению к демократам или республиканцам) в законодательстве прописано создание мониторинговых двухпартийных групп, также на регулярной основе проверяющих состояние цифрового оборудования для выборов[9].

В Мичигане, Огайо и Флориде тоже регулярно осуществляют проверки работоспособности цифрового оборудования избиркомов. Они включают в себя следующие этапы:

— проверку наличия актуальной версии программного обеспечения;

— оценку пригодности оборудования для считывания отметок на всех бюллетенях;

— проверку соответствия итоговых табличных результатов ожидаемому (заранее заданному) результату теста;

— загрузку результатов теста в центральный компьютер для составления итоговых таблиц и проверку результатов со всех устройств;

— очистку памяти от результатов тестирования и подготовку оборудования для голосования;

— замену пломб с защитой от несанкционированного доступа (при необходимости) и возврат оборудования в безопасное хранилище;

---

[7] *Hasen R. L.* Election Meltdown: Dirty Tricks, Distrust, and the Threat to American Democracy. Yale University Press, 2020. P. 55.

[8] *Holbein J. B.*, *Hillygus D. S.* Making Young Voters: Converting Civic Attitudes into Civic Action. Cambridge University Press, 2020. P. 53.

[9] *Hodgson Q. E., Chan E. W., Bodine-Baron E.,* et al. Op. cit.

— документирование результатов тестирования[10].

После утверждения президентом США исполнительного приказа 14028 «Об улучшении кибербезопасности страны» Белый дом поручил Агентству по кибербезопасности и защите инфраструктуры США (Cybersecurity and Infrastructure Security Agency, CISA) разработать стандартные руководства для использования при планировании и проведении мероприятий по реагированию на киберугрозы. Такие руководства были предназначены в первую очередь для федеральных учреждений гражданской исполнительной власти, однако на практике их также начали активно использовать избирательные комиссии[11].

Комплекс рекомендаций, закрепленный в указанных руководствах, включает в себя следующие меры:

— внедрение многофакторной аутентификации с целью получения удаленного доступа к сети организации, а также доступа администратора или иного привилегированного лица;

— регулярную установку обновлений, устраняющих известные эксплуатируемые уязвимости программного обеспечения, идентифицированные CISA;

— систематические проверки отключения сотрудниками всех портов и протоколов, которые не являются необходимыми для решения задач организации;

— организацию доступа персонала к облачным сервисам в соответствии с руководствами CISA;

— установку бесплатных сервисов кибергигиены CISA;

— использование функции ведения журнала, фиксирующего события в рамках изменения состояния оборудования;

— периодическое тестирование систем резервного копирования данных.

Помимо того, в рамках избирательных комиссий могут формироваться группы реагирования на киберугрозы для цифрового оборудования. Для отработки их действий постоянно проводятся учения[12].

Обеспечение безопасности цифрового оборудования избирательных комиссий от киберугроз также осуществляется за счет регулярного устранения актуальных уязвимостей в программном обеспечении на основании консультативного заключения по кибербезопасности (CSA), регулярно публикуемого профильными органами публичной власти Соединенных Штатов, Австралии, Канады, Новой Зеландии и Великобритании[13]. Это обусловлено тем, что, как было отмечено выше, предписания по реализации программ кибербезопасности формулируются лишь на уровне законодательства штатов и муниципальных образований, в силу чего запрет на подключение оборудования к внешним сетям применяется избирательно[14].

Отдельно следует отметить, что CISA рекомендует избирательным комиссиям использовать централизованную систему управления исправлениями в программном обеспечении, а также при необходимости прибегать для устранения уязвимости к одобренным поставщиком программного обеспечения бэкдорам — скрытым алгоритмам обхода обычной аутентификации или шифрования[15].

В руководствах CISA, изданных в 2021 г., также появилась рекомендация внедрить многофакторную аутентификацию для всех пользователей без исключения и ко всем VPN-соединениям. В случаях, если инструментарий

[10] *Hasen R. L.* Election Meltdown: Dirty Tricks, Distrust, and the Threat to American Democracy. Yale University Press, 2020. P. 72.

[11] The White House. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (дата обращения: 01.06.2023).

[12] Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/sites/default/files/2023-06/Guide%20to%20Securing%20Remote%20Access%20Software_508c.pdf (дата обращения: 01.06.2023).

[13] URL: https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01 (дата обращения: 01.06.2023).

[14] URL: https://www.cisa.gov/topics/election-security (дата обращения: 01.06.2023).

[15] URL: https://www.cisa.gov/news-events/alerts/2022/06/03/cisa-releases-security-advisory-dominion-voting-systems-democracy (дата обращения: 01.06.2023).

многофакторной аутентификации недоступен для избиркома, его руководителю предлагается требовать от сотрудников, выполняющих удаленную работу, использовать надежные пароли.

Обновленная система мер безопасности предписывает организаторам голосования как минимум ежегодно просматривать, проверять или удалять привилегированные учетные записи. Настройку контроля доступа предлагается осуществлять в соответствии с концепцией принципа наименьших привилегий.

Помимо того, к организаторам голосования предъявляется требование ужесточить контроль за часто используемыми сетевыми службами внутренней сети, включая протокол разрешения имен локальной многоадресной рассылки (LLMNR), протокол удаленного рабочего стола (RDP), общую файловую систему Интернета (CIFS), Active Directory и OpenLDAP.

Равным образом руководителям комиссий рекомендовано строго контролировать использование собственных скриптовых приложений, таких как командная строка, PowerShell и объектная модель распределенных компонентов (DCOM).

Избиркомам также предлагается сегментировать локальные сети, чтобы ограничить или заблокировать нежелательные перемещения внутри них, контролируя доступ к устройствам и базам данных, а также использовать частные виртуальные локальные сети.

Организаторам избирательного процесса рекомендуется применять дополнительные инструменты безопасности: обнаружение конечных точек и реагирование на них (EDR), средства управления информацией о безопасности и событиях (SIEM)[16].

Таким образом, в США практики противодействия киберугрозам для цифрового оборудования, используемого в рамках избирательного процесса, не закреплены и не унифицированы на уровне федерального законодательства. Однако порожденные данной правовой лакуной риски нивелируются благодаря воздействию двух взаимовлияющих факторов: с одной стороны, такие институты, как EAC и CISA, снабжают организаторов выборов в США качественными методическими материалами; с другой стороны, система неформального двухпартийного контроля над проведением выборов обеспечивает выполнение организаторами голосования большинства соответствующих рекомендаций федеральных органов, поскольку игнорирование таких рекомендаций какой-либо из политических сил подразумевает предоставление конкурирующей партии возможного преимущества.

## БИБЛИОГРАФИЯ

1. *Козлова Е. И.* Обоснование новых концепций российской конституции в правовой теории // Lex russica. — 2009. — Т. 68. — № 2. — С. 311–321.
2. *Комарова В. В.* Политические права граждан России в цифровой среде // Право и цифровая экономика. — 2021. — № 4 (14). — С. 63–72.
3. *Комарова В. В.* Электронная демократия: мифы и реальность // Ученые записки Худжандского государственного университета имени академика Б. Гафурова. Серия гуманитарно-общественных наук. — 2016. — № 3 (48). — С. 44–52.
4. *Шапошников А. В.* Конституционно-правовое регулирование использования цифровых технологий при осуществлении видеонаблюдения за выборами и референдумами // Актуальные проблемы российского права. — 2023. — № 10. — С. 20–27.
5. *Barber B.* If Mayors Ruled the World: Dysfunctional Nations, Rising Cities. — Yale University Press, 2013. — 432 p.

[16] URL: https://www.cisa.gov/sites/default/files/2023-01/cisa_insights-implement_cybersecurity_measures_now_to_protect_against_critical_threats_508c.pdf (дата обращения: 01.06.2023).

6. *Hasen R. L.* Election Meltdown: Dirty Tricks, Distrust, and the Threat to American Democracy. — Yale University Press, 2020.
7. *Holbein J. B.*, *Hillygus D. S.* Making Young Voters: Converting Civic Attitudes into Civic Action. — Cambridge University Press, 2020. — 282 p.
8. *Lindner R.*, *Aichholzer G.* E-Democracy: Conceptual Foundations and Recent Trends // European E-Democracy in Practice / L. Hennen, I. van Keulen, I. Korthagen et al. (eds.). — Springer, 2020. — P. 11–45.

*Материал поступил в редакцию 18 июля 2025 г.*

**REFERENCES (TRANSLITERATION)**

1. Kozlova E. I. Obosnovanie novykh kontseptsiy rossiyskoy konstitutsii v pravovoy teorii // Lex russica. — 2009. — T. 68. — № 2. — S. 311–321.
2. Komarova V. V. Politicheskie prava grazhdan Rossii v tsifrovoy srede // Pravo i tsifrovaya ekonomika. — 2021. — № 4 (14). — S. 63–72.
3. Komarova V. V. Elektronnaya demokratiya: mify i realnost // Uchenye zapiski Khudzhandskogo gosudarstvennogo universiteta imeni akademika B. Gafurova. Seriya gumanitarno-obshchestvennykh nauk. — 2016. — № 3 (48). — S. 44–52.
4. Shaposhnikov A. V. Konstitutsionno-pravovoe regulirovanie ispolzovaniya tsifrovykh tekhnologiy pri osushchestvlenii videonablyudeniya za vyborami i referendumami // Aktual'nye problemy rossijskogo prava. — 2023. — № 10. — S. 20–27.
5. Barber B. If Mayors Ruled the World: Dysfunctional Nations, Rising Cities. — Yale University Press, 2013. — 432 p.
6. Hasen R. L. Election Meltdown: Dirty Tricks, Distrust, and the Threat to American Democracy. — Yale University Press, 2020.
7. Holbein J. B., Hillygus D. S. Making Young Voters: Converting Civic Attitudes into Civic Action. — Cambridge University Press, 2020. — 282 p.
8. Lindner R., Aichholzer G. E-Democracy: Conceptual Foundations and Recent Trends // European E-Democracy in Practice / L. Hennen, I. van Keulen, I. Korthagen et al. (eds.). — Springer, 2020. — P. 11–45.