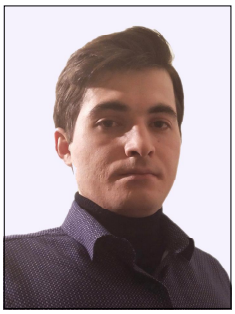
УДК 32.019.5
DOI: 10.21209/2227-9245-2021-27-10-78-84

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РАМКАХ ЭЛЕКТРОННОЙ ДЕМОКРАТИИ

INFORMATION SECURITY IN THE FRAMEWORK OF ELECTRONIC DEMOCRACY



И. С. Широков, Байкальский государственный университет, г. Иркутск
shirokov.iw@yandex.ru

I. Shirokov, Baikal State University, Irkutsk

Современные политические отношения основаны на использовании инновационных технологий в сочетании со средствами массовой коммуникации. Важнейшим звеном обеспечения функционирования таких механизмов является безопасность и стабильность работы всех задействованных систем. Уникальным решением для поддержания политических процессов, широкого вовлечения в них граждан и проведения честных и справедливых выборов является использование механизмов электронной демократии. Анализируется зарубежный и отечественный опыт практического применения онлайн-голосования на региональном примере, выявлена проблема информационной безопасности, выстроены приоритеты для её решения, описаны способы защиты информации личных данных в сети Интернет и в государственных информационных системах. *Актуальность* исследования связана с экспоненциальным ростом информационно-коммуникационных технологий, быстрой сменой стандартов и технологических платформ. Качественные изменения заставляют государства использовать новые возможности техники, искать новые способы администрирования и контроля в политическом поле. Для изучения политических процессов в их развитии и электронной демократии во взаимодействии с политическими институтами в работе использованы исторический и институциональный подходы

Ключевые слова: *кибербезопасность; электронная демократия; многоагентные системы; блокчейн; информационная безопасность; гражданское участие; гражданская инициатива; политическая коммуникация; информационно-коммуникационные технологии; онлайн-безопасность*

Modern political relations are based on the use of innovative technologies in combination with the mass media. The most important link in ensuring the functioning of such mechanisms is the safety and stability of the operation of all involved systems. The use of e-democracy mechanisms is a unique solution to support political processes, broadly involve citizens in them and conduct fair and fair elections. The article analyzes the experience of online voting practical application, identifies the problem of information security, builds priorities for its solution, and describes methods of protecting information, personal data on the Internet and in state information systems. The relevance of the study is associated with the exponential growth of information and communication technologies, the rapid change in standards and technological platforms. Qualitative changes force states to use new technological capabilities, to look for new ways of administration and control in the political field. To study political processes in their development, to study electronic democracy in interaction with political institutions, the historical and institutional method is used in the work

Key words: *cybersecurity; e-democracy; multi-agent systems; blockchain; information security; civic participation; civil initiative; political communication; information and communication technologies; online security*

Безопасность онлайн-среды и информации всегда оставалась проблемой для организаций и населения. Важной составляющей электронной демократии является использование информационно-коммуникационных технологий для контроля исполнения

решений, администрирования процессов, информирования и принятия совместных решений при помощи онлайн-голосования. В такой концепции важным гарантом конституционных идей народовластия становится безопасность информации и надёжность онлайн-голосования.

Актуальность исследования обусловлена стремительно развивающимися коммуникационными интернет-технологиями. В связи с этим возникает потребность восстановления уверенности пользователей в безопасности использования новых технологий и сохранности личной информации в сети.

Объектом исследования данной работы является электронная демократия.

К предмету изучения отнесены проблемы практики применения онлайн голосования в информационной среде.

Целью исследования является изучение проблем функционирования различных форм электронной демократии в онлайн пространстве.

Задачи определены целью исследования и выражаются в выявлении способов защиты информации и личных данных граждан.

Методология исследования. Исследование онлайн-безопасности электронной демократии основано на структурно-функциональном и междисциплинарном подходах.

Существуют уникальные подходы к обсуждению регулирования процессов электронной демократии. Ряд исследований сосредоточен исключительно на безопасности электронного голосования [4], другие – на операционных аспектах электронной демократии [7], третьи – затрагивают правовые и конституционные вопросы регулирования электронной демократии [9]. Исследователи отмечают и активное использование электронных и онлайн-средств в демократических обществах, значительное влияние политических объединений, организаций и других структур, выступающих в роли посредника и использующих формы электронной демократии в своих целях. За последние два десятилетия отмечается роль технологических систем. Они приравниваются к социальным структурам, как и политические институты, а их деятельность контролируется и регламентируется государством. При этом ведущую роль в демократических режимах продолжают играть различные социальные группы и индивиды, использующие инновационные технологические решения политической коммуникации [2].

Широко понятие «электронная демократия» вошло в употребление в конце XX в. Под электронной демократией принято понимать демократическую форму устройства с использованием ИКТ для реализации гражданских прав и свобод. Электронное голосование основано на конституционных идеях народовластия, и в таком контексте может рассматриваться как механизм электронной демократии. Схожему мнению придерживается ряд исследователей – А. А. Чеботарева [3. С. 53], M. M. Kuryachaya [6] и другие.

В современных условиях при использовании онлайн-голосования актуальной является задача обеспечения общественного и государственного регулирования «невидимой» власти. При этом возможными рисками для функционирования процессов электронной демократии может стать неэффективная процедура аутентификации избирателей. Ошибки или утечки личных данных пользователей при аутентификации в систему могут отрицательно сказаться на надежности онлайн-голосования и снизить уровень доверия к нему.

Осенью 2021 г. на выборах в Госдуму в течение трёх дней применялось онлайн-голосование. Особенность заключалась в отсутствии возможности изменить форму волеизъявления. Если избиратель принял решение голосовать онлайн, в таком случае он не имел возможность получить бумажный бюллетень. При этом избиратель мог переголосовать повторно онлайн в течение трёх дней; «отложенным голосованием» он мог воспользоваться спустя три часа после получения первого электронного бюллетеня. Такая опция голосования объяснялась необходимостью избавить избирателя от давления или принуждения со стороны третьих лиц и за счёт этого повысить честность и справедливость выборов.

В 2020 г. в Москве и Нижегородской области избиратели воспользовались электронной формой волеизъявления на общероссийском голосовании по поправкам в конституцию. Система ДЭГ предложена избирателям только в двух субъектах страны. В 2021 г. в дистанционном электронном голосовании принимало участие большее количество субъектов: Курская область, Мурманская область, Нижегородская область,

Ростовская область, Ярославская область, города федерального значения Москва и Севастополь. В результате, если в 2020 г. количество проголосовавших онлайн составляло около 1,09 млн человек, то на выборах в Госдуму в 2021 г. количество проголосовавших подобным образом составляло около 2 млн человек, то есть число граждан, избравших электронную форму волеизъявления, увеличилось почти в два раза.

По официальной информации, на систему онлайн-голосования в Москве на выборах 2021 г. зафиксировано более 300 кибератак с иностранных серверов, при этом деструктивное информационное воздействие не помешало работоспособности системы и записи голосов избирателей в Blockchain. Система электронного голосования в Москве функционирует с 2019 г. и к моменту проведения выборов в Госдуму была адаптирована и полностью работоспособна, как отмечает регулятор [1]. Однако отмечены сбои системы блокчейн, связанные с одновременным притоком избирателей. Практическое использование онлайн-голосования и сопутствующие проблемы ещё раз доказывают актуальность исследования вопросов кибербезопасности и поиска решений по оптимизации системы.

Согласно совместному аналитическому докладу ВЦИОМ и Центра политической конъюнктуры, как показано на рис.1, главной причиной недоверия граждан к электронному голосованию в России стала возможность умышленных манипуляций и мошенничества. Второй по значимости причиной является недоверие к технической надёжности и безопасности системы.

Рис.1. Причины отказа граждан от электронного голосования, % от тех, кто выбрал голосование по почте или традиционное голосование / Fig. 1. Reasons for citizens' refusal from electronic voting, %

Опыт использования онлайн-голосования в других странах так же показал уровень недоверия со стороны правительства и населения к инновационной форме волеизъявления. Германия, Финляндия, Норвегия на официальном уровне отказались от применения онлайн-голосования, ссылаясь на ненадёжность такого формата, низкое качество кибербезопасности или на несоответствие законодательству. В США, Канаде онлайн-голосование применяется только на муниципальном уровне и для военнослужащих или граждан, проживающих за пределами страны.

Уникальным примером использования онлайн-голосования на фоне ряда стран остаётся Эстония. В 2005 г. страна провела первые в мире выборы с применением инновационных технологий, на которых каждый избиратель имел возможность проголосовать через интернет. Целью нововведения являлось увеличение явки, повышение доступности голосования для людей с инвалид-

ностью, привлечение молодого населения. Опыт использования онлайн-голосования в стране показал низкую стоимость такого формата по сравнению с традиционным голосованием. В масштабах страны, в Эстонии, впервые применили технологию Blockchain. Первоначально данная технология использовалась для защиты и сохранности более 1 млн медицинских записей и обеспечивала проверку подлинности данных без опоры на централизованный орган.

Перспективы развития Blockchain оказались актуальны не только для реализации онлайн-голосования, но и индустрии биржевой торговли, банковского сектора, нотариальной сферы.

Технология имеет широкую область применения, при помощи Blockchain можно хранить личные данные в электронной базе данных: свидетельства о рождении, документы об образовании и другое. Основываясь на практическом опыте использования технологии, можно говорить о применении технологии Blockchain и для хранения данных избирателей при проведении электронного голосования. К 2021 г. в Эстонии технология Blockchain Guardtime используется для обеспечения сохранности данных в масштабах страны, платформа Blockchain под названием KSI Blockchain (Keyless Signature Infrastructure) разработана и применяется для защиты серверов. Практика использования такой технологии повысила сохранность информации и баз данных, как следствие – повысилось доверие граждан к электронным формам взаимодействия с регулятором, а также увеличилось число граждан, использующих онлайн-голосование.

На примере прошедших выборов можно зафиксировать востребованность такого формата. Только в период предварительного голосования 2021 г. количество голосов, отданных электронным путем, составило 46,7 % от общего числа проголосовавших (рис. 2).

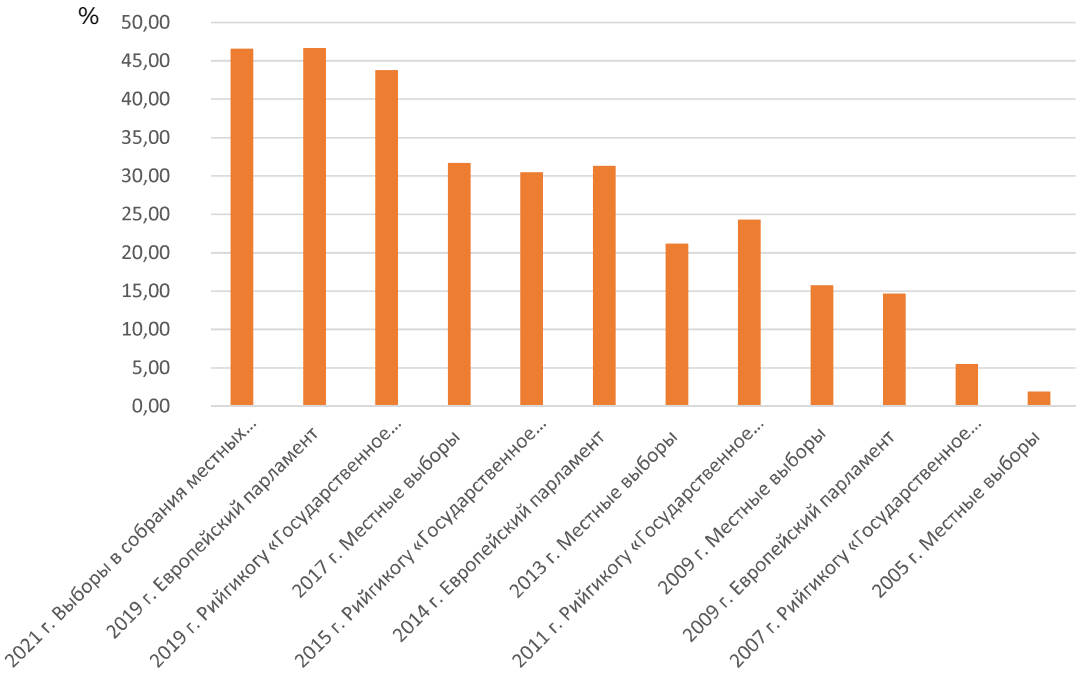


Рис. 2. Доля граждан Эстонии, проголосовавших электронно, от общего числа голосовавших, % / Fig. 2. Percentage of Estonian citizens, who voted electronically of the total number of voters, %

Развитие инновационных технологий, модернизация средств защиты персональных данных, совершенствование правового законодательства постепенно меняют отношение избирателей к онлайн-голосованию. Практическое применение электронного голосования на примере Эстонии за шестнадцатилетний период свидетельствует о повышении уровня доверия к электронному голосованию.

В подавляющем большинстве избирательные системы разных стран стремятся найти баланс между репрезентативностью и эффективностью [11]. В современных условиях избирательные системы не обеспечивают пропорциональное представительство интересов граждан в органах власти [10]. Одним из способов решения таких задач может стать набирающее популярность онлайн-голосование с надёжной системой сохранности личных данных пользователей. Это предъявляет требования к применяемым технологиям. Из ряда таких технологий, имеющихся на рынке, можно выделить системы обнаружения атак (СОА или англ. Intrusion Detection System, IDS), системы обнаружения вторжений SDN, многоагентные системы.

Многоагентные системы хорошо изучены и могут использоваться для обеспечения информационной безопасности. В частности, такие системы применяются для фильтрации электронных писем, систем антивирусной защиты, обнаружения и предотвращения кибератак, предотвращения утечки личных данных пользователя, решения задач планирования и составления расписаний; управления информационными потоками, оценки состояния систем. Многоагентная система представляет собой ветвь искусственного интеллекта и определяется как набор агентов, представляющих физические или логические объекты, способные координировать друг друга для достижения своих целей [8].

Для улучшения перспектив электронной демократии, повышения гражданского участия и доверия населения к форме электронного волеизъявления требуется решить проблему информационной безопасности. Многоагентные системы способствуют решению такой задачи и могут обеспечить фильтрацию информации и входящих данных, нейтрализовать угрозы кибербезопасности и утечки данных.

Разделение составных задач на подзадачи – основной принцип работы таких систем. Обработка подзадач осуществляется программными агентами, которые разрабатываются и программируются автономно. При этом агенты могут автоматически создавать события и обмениваться информацией между собой, анализировать результаты, передавать сигналы обратной связи другим агентам, поддерживать с ними взаимодействие. Такая концепция применима для задач с большим количеством участников и, как следствие, может применяться в ИТ-сфере для обеспечения онлайн - безопасности.

Для обеспечения безопасности приложений, сервисов и информации существует прототип системы обнаружения вторжений для сети SDN. Ее алгоритм основан на программных вычислениях и включает в себя оценку уровня безопасности информационных систем, управление рисками информационной безопасности и обнаружение угроз с последующим их устранением [5].

Заключение. Целью электронной демократии является оптимизация деятельности политических институтов путем отказа от посреднических структур и информационных барьеров, обеспечение прямого и активного политического участия народа в общественных делах. К последнему можно отнести не только электронное голосование (часто используемое с целью увеличения явки), но и реализацию власти в электронной форме, включающую неформальную политику и неправительственных участников (социальные сети, интернет-ресурсы, предназначенные для создания общественных инициатив, форумы, информационные порталы). Как свидетельствует практика использования форм электронной демократии, не существует безупречной системы, способной обеспечить справедливое онлайн-голосование, стабильную и независимую политическую коммуникацию. При этом наиболее уязвимой к умышленной интеракции остаётся политическая коммуникация в социальных сетях.

Список литературы

1. Замахина Т. В ЦИК рассказали о кибератаках в период выборов // Российская газета. 2021. URL: https://rg.ru/2021/09/20/v-cik-rasskazali-o-kiberatakah-v-period-vyborov.html (дата обращения: 31.10.2021). Текст: электронный.

2. Омеличкин О. В. Электронная демократия: понятие, проблемы // Вестник Кемеровского государственного университета. 2014. № 1, т. 2. С. 87.

3. Чеботарева А. А. Механизмы электронной демократии: возможности и проблемы их реализации в Российской Федерации // Правовая информатика. № 3. 2012. С. 53.

4. Chang-Fong, N., Essex A. The Cloudier Side of Cryptographic End-to-End Verifiable Voting: A Security Analysis of Helios // In Proceedings of the 32-nd Annual Conference on Computer Security Applications. 2016. P. 324–335.

5. Dotcenko S., Vladyko A., Letenko I. A fuzzy logic-based information security management for software-defined networks // 16-th International Conference Advanced Communication Technology (ICACT). 2014. P. 167–171.

6. Kuryachay M. M. E-Democracy in modern Russia: the establishment, development and prospects // Kutafin university law review. №1. Vol. 1. P. 93–105.

7. Langer L., Schmidt A., Buchmann J. Secure and Practical Online Elections via Voting Service Provider. Published, 2008. P. 255–262.

8. Leitao P. Vrba P. Agent-based distributed manufacturing control: a state-of-the-art survey // Springer. 2011. P. 15–28.

9. Schwartz B., Grice D. Establishing a Legal Framework for E-Voting in Canada. Elections Canada 2013. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/manitob36&div=44&id=&page (дата обращения: 07.08.2021). Текст: электронный.

10. Skowron P., Faliszewski P., Slinko A. Achieving fully proportional representation: approximability results // Artif. Intell. 2015. P. 67–103.

11. Young P. Optimal voting rules // The Journal of Economic Perspectives. 2014. Vol. 9, № 1. P. 51–64.

References

1. Zamahina T. *Rossiyskaya gazeta. 2021* (Russian Newspaper. 2021.). Available at: https://rg.ru/2021/09/20/v-cik-rasskazali-o-kiberatakah-v-period-vyborov.html (date of access: 31.10.2021). Text: electronic.

2. Omelichkin O. V. *Vestnik Kemerovskogo gosudarstvennogo universiteta* (Bulletin of the Kemerovo State University), 2014, no. 1, vol. 2, p. 87.

3. Chebotareva A. A. *Pravovaya informatika* (Legal informatics), 2012, no. 3, p. 53.

4. Chang-Fong, N., Essex A. *In Proceedings of the 32-nd Annual Conference on Computer Security Applications* (In Proceedings of the 32-nd Annual Conference on Computer Security Applications), 2016, pp. 324–335.

5. Dotcenko S., Vladyko A., Letenko I. *16-th International Conference Advanced Communication Technology* (16-th International Conference Advanced Communication Technology) (ICACT), 2014, pp. 167–171.

6. Kuryachay M. M. *Kutafin university law review* (Kutafin university law review), no. 1, vol. 1, pp. 93–105.

7. Langer L., Schmidt A., Buchmann J. *Secure and Practical Online Elections via Voting Service Provider* (Secure and Practical Online Elections via Voting Service Provider). Published, 2008. pp. 255–262.

8. Leitao P. Vrba P. *Springer* (Springer), 2011, pp. 15–28.

9. Schwartz B., Grice D. *Establishing a Legal Framework for E-Voting in Canada* (Establishing a Legal Framework for E-Voting in Canada). Elections Canada 2013. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/manitob36&div=44&id=&page (date of access: 07.08.2021). Text: electronic.

10. Skowron P., Faliszewski P., Slinko A. *Artif. Intell* (Artif. Intell), 2015, pp. 67–103.

11. Young P. *The Journal of Economic Perspectives* (The Journal of Economic Perspectives), 2014, vol. 9, no. 1, pp. 51–64.

Информация об авторе **Information about the author**

Широков Иван Сергеевич, аспирант, кафедра международных отношений и таможенного дела, Институт мировой экономики и международных отношений, Байкальский государственный университет, г. Иркутск, Россия. Область научных интересов: электронная демократия, гражданская инициатива, политическая коммуникация
shirokov.iw@yandex.ru

Ivan Shirokov, postgraduate, International Relations and Customs department, Institute of World Economy and International Relations Baikal State University, Irkutsk, Russia. Sphere of scientific interests: e-democracy, civic initiative, political communication

Для цитирования

Широков И. С. Информационная безопасность в рамках электронной демократии // Вестник Забайкальского государственного университета. 2021. Т. 27, № 10. С. 78–84. DOI: 10.21209/2227-9245-2021-27-10-78-84.

Shirokov I. Information security in the framework of electronic democracy // Transbaikal State University Journal, 2021, vol. 27, no. 10, pp. 78–84. DOI: 10.21209/2227-9245-2021-27-10-78-84.

Статья поступила в редакцию: 16.11.2021 г.
Статья принята к публикации: 22.11.2021 г.