Вестник Томского государственного университета. Философия. Социология. Политология. 2025. № 87. С. 207–214.
Tomsk State University Journal of Philosophy, Sociology and Political Science. 2025. 87. pp. 207–214.

# ПОЛИТОЛОГИЯ

Научная статья
УДК 324
doi: 10.17223/1998863X/87/18

## ОПЫТ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В ШВЕЙЦАРИИ, США И РОССИИ

**Андрей Дмитриевич Дульский**

*Национальный исследовательский Томский государственный университет, Томск, Россия, Dulya_ad@mail.ru*

***Аннотация.*** В статье проводится сравнительный анализ применения дистанционного электронного голосования (ДЭГ) в Швейцарии, США и России. Выявлены ключевые проблемы безопасности и отсутствие значительного влияния на явку. Сделан вывод о необходимости решения технических и правовых задач для дальнейшего внедрения данной технологии.
***Ключевые слова:*** выборы, платформы, дистанционное электронное голосование

***Для цитирования:*** Дульский А.Д. Опыт применения технологии дистанционного электронного голосования в Швейцарии, США и России // Вестник Томского государственного университета. Философия. Социология. Политология. 2025. № 87. С. 207–214. doi: 10.17223/1998863X/87/18

# POLITICAL SCIENCE

Original article

## THE EXPERIENCE OF USING REMOTE ELECTRONIC VOTING TECHNOLOGY IN SWITZERLAND, THE USA, AND RUSSIA

**Andrey D. Dulsky**

*National Research Tomsk State University, Tomsk, Russian Federation, Dulya_ad@mail.ru*

***Abstract.*** This study analyzes international and domestic experiences with remote electronic voting (REV) and assesses its impact on electoral processes. The relevance of this research stems from the first large-scale implementation of REV in Russia during the 2024 presidential election and the ongoing global integration of this technology. The study aims to conduct a comparative analysis of REV models in Switzerland, the United States, and Russia, determine the technology's influence on voter turnout, and identify systemic challenges associated with its application. Switzerland, with its long history of REV experimentation since 2000, shifted towards a model prioritizing maximum transparency and cryptographic security following controversies in 2019. The Swiss system is characterized by complex, multi-stage verification, open-source code, and rigorous stress testing. Despite

its high security, it has been criticized for complexity, which may hinder voter accessibility, and for potential compromises to ballot secrecy. Nevertheless, its use contributed to a 1.5% increase in turnout in the 2023 federal elections, primarily among citizens living abroad and voters with disabilities. The United States exemplifies a cautious and decentralized approach, where REV is fully available only in a few states. American experts highlight key risks, including a lack of proven, reliable technology, the inability to conduct manual recounts, vulnerabilities in voter identification, and the presence of a more established alternative in postal voting. The Russian REV model, first deployed at the federal level in 2024, is built on blockchain technology and integrated with the Gosuslugi portal. As evidenced by the case of Tomsk Oblast, the technology did not significantly impact overall turnout. Its primary challenges include a lack of transparency in auditing procedures, potential security vulnerabilities, and a deficit of trust from the IT community. In conclusion, REV remains an evolving technology that presents a dual potential: to enhance electoral accessibility while simultaneously posing significant risks to the security and legitimacy of the electoral process. Its successful future implementation depends not only on resolving technical issues but also on developing rigorous standards, ensuring transparency, and fostering public trust. The widespread adoption of REV necessitates a thorough examination of the legal framework and a comprehensive strategy that incorporates international experience and addresses critical challenges.
***Keywords:*** elections, platforms, remote electronic voting

***For citation:*** Dulsky, A.D. (2025) The experience of using remote electronic voting technology in Switzerland, the USA, and Russia. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya – Tomsk State University Journal of Philosophy, Sociology and Political Science.* 87. pp. 207–214. (In Russian). doi: 10.17223/1998863X/87/18

Весной 2024 г. прошли выборы Президента Российской Федерации, на которых избиратели из 29 тестовых регионов могли использовать новый способ выражения своей воли – дистанционное электронное голосование (ДЭГ) на базе сервиса «Госуслуги». Это первый раз для нашей страны, когда подобную технологию использовали на выборах такого масштаба, ведь ранее она была доступна только на местных выборах. Первое применение ДЭГ было в единый день голосования 8 сентября 2019 г. и на выборах депутатов в Московскую городскую думу VII созыва. Опыт применения подобной технологии в нашей стране только начинает формироваться. В связи с этим целесообразно рассмотреть опыт других стран по применению ДЭГ, выделить основные тенденции и особенности, а также спрогнозировать дальнейшее развитие и применение данной технологии в Российской Федерации.

Цель данной работы заключается в анализе опыта применения технологии ДЭГ в Швейцарии, США и России, определении влияния электронного голосования на явку избирателей и выделении сложностей, возникающих при применении данной технологии. Актуальность работы обусловлена тем, что на сегодняшний день развитие электронных сетей позволяет сделать ДЭГ доступным для граждан, и многие страны вводят эту систему для голосования на разных уровнях.

## Швейцария

Свой эксперимент с внедрением электронного голосования правительство Швейцарии начало с 2000 г. За первое десятилетие XXI в. была разработана система, которую в дальнейшем дополняли и изменяли. Фактически ДЭГ стал применяться с 2011 г. на референдумах и выборах различного уровня. Однако из-за серьезной угрозы взлома и фальсификации результатов

выборов 2019 г. было принято решение об ограничении технологии ДЭГ сроком на 5 лет. За это время предполагалось разработать и внедрить новую платформу для контроля безопасности и легитимности голосования. Её разработка была поручена государственной компании Swiss Post. Уже на выборах в парламент 2023 г. компания представила свои наработки, но только в тестовом формате: не более 30% избирателей в каждом кантоне и не более 10% избирателей по всей стране. В 2023 г. электронное голосование использовалось в кантонах Базель-Штадт, Санкт-Галлен и Тургау для избирателей, живущих за границей, а также для людей с ограниченными возможностями. 22 ноября 2023 г. Федеральный совет Швейцарии также предоставил кантону Граубюнден разрешение на тестирование онлайн-голосования в период с 2024 по 2026 г.

В основу своей технологии Swiss Post внедрила криптографические ключи шифрования, что обеспечивает высокий уровень безопасности и прозрачности процедуры выборов [1]. Все компоненты и документы об электронном голосовании открыты для общественности и доступны для изучения независимыми экспертами. Swiss Post регулярно публикует новые версии разработки и релизы на платформе GitLab [2], где доступны исходный код, криптографические алгоритмы и программа проверки. Особое внимание разработчики уделили двойной проверке действительности бюллетеней, что предотвращает попадание в систему «несуществующих» голосов. Для большей доступности система доступна на всех национальных языках Швейцарии: немецком, французском, итальянском и ретороманском. Для проверки системы на возможность взлома Swiss Post в 2023 г. организовала публичный стресс-тест. В рамках его всем желающим предлагалось попробовать найти уязвимости в программе. Те, кто находил подобные ошибки и бреши, получали денежные вознаграждения. В тесте приняли участие 2 650 энтузиастов со всего мира, однако никто из них так и не смог взять систему под контроль или получить доступ к репозиторию голосов. За тест были выявлены несколько незначительных ошибок, которые быстро были исправлены. Компания получила около 300 различных отчётов от участников теста, выплатив им суммарно 170 000 франков. После теста Swiss Post выложила все его результаты в открытый доступ, чтобы с ним могли ознакомиться граждане страны. Накануне федеральных выборов 2023 г. Swiss Post предоставила доступ к тестовой платформе электронного голосования для обучения избирателей [3]. Для входа на портал нужно было ввести код инициализации из удостоверения личности избирателя. Чтобы отдать свой голос, избиратель должен был самостоятельно зашифровать его, вводя индивидуальный код подтверждения, соответствующий выбранному кандидату. После отправки голоса избиратель сравнивал код завершения, отображаемый на экране, с кодом из удостоверения личности. При совпадении кодов голосование завершалось. Избиратель выбирал кандидатов в приложении, которое использовало ключ избирателя для шифрования и аутентификации результатов голосования, передавая их на сервер. Далее избирателю высылались коды возврата, вычисленные на основе закрытого ключа, известного серверу, но не избирателю или клиентскому приложению. Избиратель сравнивал коды результатов на бумажном носителе с выбранными кандидатами. Взломанное приложение не могло отобразить правильные коды результатов, если не получало их с сервера. Оно также не

могло получить их с сервера, если не зашифровало нужных кандидатов изначально. Приложение не видело коды результатов, хранимые на бумажном носителе, если к компьютеру избирателя не было подключено устройство слежения. Важной ступенью безопасности швейцарской системы электронного голосования был внешний канал связи, недоступный компьютеру избирателя. Голосование избирателя зашифровывалось в системе, анонимизировалось и сохранялось в электронном накопителе бюллетеней.

Стоит отметить, что по сравнению с 2019 г., когда не применялась технология ДЭГ, в 2023 г. явка на выборы увеличилась на 1,5% [4]. В данные проценты входят люди, которые по разным причинам не могут голосовать на участках: проживающие за пределами Швейцарии и люди с ограниченными возможностями. «Одним из наиболее нежелательных недостатков является отсутствие доступа для незрячих людей и людей с нарушениями зрения к осуществлению их права голосовать и быть избранными, а также к защите тайны их голосования» [5], – отметил президент Ассоциации слепых и слабовидящих Швейцарии Роланд Штудер.

Несмотря на защищённость, технология электронного голосования в Швейцарии имеет ряд недостатков:

1. ДЭГ является сложным и неудобным для избирателя, которому нужно несколько раз вводить коды для подтверждения выбора и передачи голоса. При этом пакет идентификационных документов для голосования избиратель должен получить бумажным письмом через почтовую службу.

2. Швейцарский избиратель на этапе проверки корректности учета своего волеизъявления раскрывает тайну голосования, что создает возможность для контроля его действий.

## США

США имеют долгую историю развития и совершенствования технологий для упрощения гражданам волеизъявления. В рамках заявленной темы представляют интерес две технологии: использование компьютеров для голосования непосредственно на территории избирательного участка и непосредственно ДЭГ.

Первый способ представляет собой многоуровневый процесс. Сперва гражданин верифицирует свою личность через специальную электронную платформу, чем подтверждает своё право на участие в голосовании. Затем отправляется к ближайшему устройству для голосования – кабинке со специальным компьютером внутри, а уже там гражданин может отдать свой голос. Так как эти машины подключены к сети и главному компьютеру, куда уходят все данные о голосовании, подобный тип голосования остаётся крайне чувствительным к воздействию извне. Многие исследователи критикуют электронные системы голосования, считая их недостаточно надежными. Эксперт по компьютерной безопасности Алекс Хайдерман называет этот метод «устаревшим и недостаточно протестированным», приводя в пример случаи, когда электронные системы давали сбои, неправильно засчитывая голоса.

В 2018 г. на выборах в Сенат от штата Техас были зафиксированы случаи, когда компьютеры самостоятельно изменяли голоса избирателей. Голоса, отданные за демократа Бето О’Рурка, неожиданно перераспределялись в пользу республиканца Теда Круза [6]. В 2010 г. в Южной Каролине элек-

тронные машины для голосования выдали сбой, из-за которого неверно посчитали как минимум 420 бюллетеней [7]. На выборах в округе Йорк, штат Пенсильвания, в 2017 г. произошла более серьезная ошибка. Из-за неправильной настройки электронные машины позволяли избирателям голосовать дважды. Этим воспользовались более 3 000 человек, что составило 5% от проголосовавших. На выборах 2011 г. в Фэрфилде, штат Нью-Джерси, фавориты выборов – Синтия и Эрнест Зиркль – проиграли с удивительно низкими результатами. Они подали в суд, и в результате было установлено, что гораздо больше людей проголосовало за них, чем было указано в официальных данных. В итоге суд назначил повторные выборы без использования электронных машин. На этот раз кандидаты одержали победу с большим отрывом [8].

Но самым серьезным скандалом в истории использования машин для голосования в США является случай, произошедший на выборах в Джорджии. Долгое время компьютеры для голосования не работали автономно, а были подключены к общему серверу, куда передавались все данные. В 2014 г. один или несколько злоумышленников взломали систему и проникли в главный сервер, получив возможность вмешиваться в процесс подсчета голосов. Вся информация о деятельности хакеров была удалена из системы, поэтому невозможно точно сказать, как они повлияли на ход выборов. ФБР не обнаружило доказательств фальсификации результатов выборов, а в Джорджии не печатаются бумажные бюллетени, что делает невозможным проверку данных [9].

Интернет-голосование через ДЭГ на момент исследования доступно только в одном штате Америки, а именно на Гавайях. Процесс начинается с регистрации и верификации пользователя, затем гражданин указывает себя как «постоянно отсутствующего» и выбирает электронный вариант голосования. В Гавайях нет ограничений для того, чтобы признать себя «постоянно отсутствующим» и выбрать электронное голосование, и этим может воспользоваться любой резидент штата [10].

Потенциально при соблюдении определённых условий житель США может проголосовать через ДЭГ и в других штатах. В штате Айдахо граждане имеют право голосовать с помощью электронной почты или факса, но только в том случае, если во время проведения выборов в штате объявлено чрезвычайное положение. В Луизиане и Юте проголосовать по интернету могут исключительно избиратели с ограниченными возможностями, чей статус подтвержден юридически. Также по интернету проголосовать могут все моряки Военного и Торгового флота США, находящиеся на момент выборов за пределами страны. Голоса этих избирателей распределяются по штатам, резидентами которых они являются.

Эксперты выражают большое количество опасений и критики в сторону применения ДЭГ в США [11]. Первая проблема – несовершенство технологии. Многие критики сходятся во мнении, что несмотря на развитие технологии блокчейна и кибербезопасности, на сегодняшний день не существует технологий, способной создать и защищать платформу для голосования. Вторая проблема – отсутствие доказательства голосования. При ДЭГ, в случае сбоя или саботажа, нет возможности вручную пересчитать голоса, ведь они хранятся в электронном формате. Третья проблема – существование альтернативного дистанционного голосования. Во многих штатах с давних пор существует практика почтового голосования. И, несмотря на несколько круп-

ных скандалов, подобный способ считается надежнее и безопаснее, чем ДЭГ. Четвёртая проблема – отсутствие достоверного механизма идентификации пользователя. Нельзя наверняка сказать, что человек голосует со своего аккаунта сам, а не кто-то другой, а если это не сделать, то существует реальный риск подорвать доверие к институту выборов, что повлечет за собой самые неприятные последствия.

## Россия

Как уже говорилось выше, первое масштабное применение ДЭГ в России произошло на выборах президента 2024 г. Пробный доступ к системе получили жители, зарегистрированные в 28 регионах страны. Для участия дистанционно гражданин должен был подать заявление через портал «Госуслуги». Сама процедура голосования также проходила через этот сервис. В основе механизма голосования лежит технология блокчейн, основанная на одноранговом шифровании, что должно обеспечивать децентрализованную и анонимную систему голосования и подсчета результатов. Информация о бюллетене не сохраняется на компьютере пользователя или обшей сети. Независимые ИТ-эксперты предупреждают, что использование технологии блокчейна может изменить результаты выборов – «не обнаружено, или даже если это будет обнаружено, будет непоправимо без проведения новых выборов» [12. С. 75]. Технология по-прежнему имеет серьезные уязвимости в системе безопасности, которые могут подорвать целостность избирательной системы. Непрозрачная экспертная группа консультирует ЦИК РФ по новой технологии, а отсутствие прозрачных процедур мониторинга вызывает дополнительное недоверие к новому онлайн-голосованию.

Что касается явки по сравнению с прошлыми выборами, итоговые цифры не сильно изменились. Для примера возьмём Томскую область: так, в 2018 г. явка на выборы президента составила 59,27%, а в 2024 г. явка составила 60,12%.

Использование ДЭГ также подверглось критике со стороны политологов и ИТ-специалистов. Из числа сообщений особенно выделяют слабую систему защиты и возможность влиять на выборы дистанционно [13. С. 348].

## Вывод

Рассматривая вышеприведённые примеры, можно заметить, что в настоящее время технология ДЭГ ещё находится в стадии разработки и содержит множество возможностей для фальсификации данных выборов. В то же время из-за слабой осведомлённости граждан и недоверия к электронным выборам прирост избирателей невелик. Однако дистанционное электронное голосование – это перспективное направление, которое может революционизировать избирательный процесс, делая его более удобным и доступным для граждан. Вместе с тем перед широким внедрением этой технологии необходимо решить ряд сложных задач, связанных с обеспечением безопасности и прозрачности голосования, а также защитой от мошенничества и манипуляций.

Важно помнить, что дистанционное электронное голосование – это не просто техническая задача, а комплексный вопрос, требующий глубокого анализа и проработки правовой базы, разработки строгих стандартов безопасности и общественного доверия к самой системе. В настоящее время

разработка и внедрение дистанционного электронного голосования является предметом активных исследований и дискуссий. Использование этой технологии в будущем будет зависеть от того, насколько эффективно будут решены проблемы безопасности, а также от готовности общества принять новый способ осуществления своего гражданского права.

### *Список источников*

1. *E-voting,* Online voting, and elections // Swiss Post. [S. l.], 2024. URL: https://digital-solutions.post.ch/en/egovernment/digitization-solutions/e-voting?shortcut=redirect-business-solutions-e-voting (access date: 06.09.2024).

2. *Swisspost-evoting* // GitLab. [S. l.], 2024. URL: https://gitlab.com/swisspost-evoting (accessed: 06.09.2024).

3. *E-Voting* ausprobieren. [S. l.], 2024. URL: https://demo.evoting.ch/ (accessed: 06.09.2024).

4. *Nationalratswahlen:* Korrektur bei den publizierten nationalen Parteistärken 2023 // Bundesamt für Statistik. [S. l.], 2024. URL: https://www.bfs.admin.ch/bfs/de/home/aktuell/neuevero-effentlichungen.assetdetail.29025149.html (accessed: 06.09.2024).

5. *Visually* Impaired Demand E-Voting In Switzerland // The Zuricher. [S. l.], 2024. URL: https://thezuricher.com/visuallyimpaired-demand-e-voting-in-switzerland/ (accessed: 06.09.2024).

6. *Schwartz J.* The Vulnerabilities of Our Voting Machines // Scientific American. [S. l.], 2018. 1st November. URL: https://www. scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/ (accessed: 06.09.2024).

7. *Freed V.* South Carolina voting machines miscounted hundreds of ballots, report finds // Statescoop. [S. l.]. 2019. 7th January. URL: https://statescoop.com/south-carolina-voting-machinesmiscounted-hundreds-of-ballots-report-finds/ (accessed: 06.09.2024).

8. *Thibodeau P.* If the election is hacked, we may never know // CSO. [S. l.], 2016. 5th October. URL: https:// www.csoonline.com/article /3128077 /if-the-election-is-hacked-we-may-neverknow.html (accessed: 06.09.2024).

9. *Bajak* E Expert: Georgia election server showed signs of tampering // City News. Ottawa, 2024. URL: https://ottawa.citynews.ca/2020/01/16/georgia-election-server-showed-signs-of-tampering-expert/ (accessed: 06.09.2024).

10. *VOTE.ORG.* [S. l.], 2024. URL: https://www.vote.org/registerto-vote/hawaii/ (accessed: 06.09.2024).

11. *Webb J.* Security Experts Say Online Voting Is a Bad Idea. Here's Why // Medium. [S. l.], 2020. 20th July. URL: https://medium.com/digital-diplomacy/sccurity-experts-say-online-voting-isa-bad-idea-heres-why-1792c9a876b0 (accessed: 06.09.2024).

12. *Фатуллаева Э.А.* Российские выборы 2021 года: новый этап применения электронных технологий в избирательном процессе // Вестник СурГУ. 2022. № 1 (35). С. 69–78.

13. *Цаплин А.Ю.* Перспективы дистанционного электронного голосования в России // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2016. № 3. С. 345–350.

### *References*

1. Switzerland. (2024a) *E-voting, Online voting, and elections*. [Online] Available from: https:// digital-solutions.post.ch/en/egovernment/ digitization-solutions/e-voting?shortcut=redirect-business-solutions-e-voting (Accessed: 6th September 2024).

2. Switzerland. (2024b) *Swisspost-evoting*. [Online] Available from: https://gitlab.com/swisspost-evoting (Accessed: 6th September 2024).

3. Switzerland. (2024c) *E-Voting ausprobieren*. [Online] Available from: https://demo.evoting.ch/ (Accessed: 6th September 2024).

4. Switzerland, Bundesamt für Statistik. (2024) *Nationalratswahlen: Korrektur bei den publizierten nationalen Parteistärken 2023*. [Online] Available from: https://www.bfs.admin.ch/ bfs/de/home/aktuell/neuevero-effentlichungen.assetdetail.29025149.html (Accessed: 6th September 2024).

5. *The Zuricher*. (2023) Visually Impaired Demand E-Voting in Switzerland. 5th September. [Online] Available from: https://thezuricher.com/visuallyimpaired-demand-e-voting-in-switzerland/ (Accessed: 6th September 2024).

6. Schwartz, J. (2018) The Vulnerabilities of Our Voting Machines. *Scientific American*. 1st November. [Online] Available from: https://www. scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/ (Accessed: 6th September 2024).

7. Freed, V. (2019) South Carolina voting machines miscounted hundreds of ballots, report finds. *Statescoop*. 7th January. [Online] Available from: https://statescoop.com/south-carolina-voting-machines-miscounted-hundreds-of-ballots-report-finds/ (Accessed: 6th September 2024).

8. Thibodeau, P. (2016) If the election is hacked, we may never know. *CSO*. 5th October. [Online] Available from: https:// www.csoonline.com/article /3128077 /if-the-election-is-hacked-we-may-neverknow.html (Accessed: 6th September 2024).

9. Bajak, E. (2020) Expert: Georgia election server showed signs of tampering. *City News*. 16th January. [Online] Available from: https://ottawa.citynews.ca/2020/01/16/georgia-election-server-showed-signs-of-tampering-expert/ (Accessed: 6th September 2024).

10. Vote.org. [n.d.] [Online] Available from: https://www.vote.org/registerto-vote/hawaii/ (Accessed: 6th September 2024).

11. Webb, J. (2020) Security Experts Say Online Voting Is a Bad Idea. Here's Why. *Medium*. 20th July. [Online] Available from: https://medium.com/digital-diplomacy/sccurity-experts-say-online-voting-isa-bad-idea-heres-why-1792c9a876b0 (Accessed: 6th September 2024).

12. Fatullaeva, E.A. (2022) Rossiyskie vybory 2021 goda: novyy etap primeneniya elektronnykh tekhnologiy v izbiratel'nom protsesse [Russian Elections of 2021: A New Stage in the Application of Electronic Technologies in the Electoral Process]. *Vestnik SurGU*. 1(35). S. 69–78.

13. Tsaplin, A.Yu. (2016) Perspektivy distantsionnogo elektronnogo golosovaniya v Rossii [Prospects for Remote Electronic Voting in Russia]. *Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: Sotsiologiya. Politologiya*. 3. pp. 345–350.

***Сведения об авторе:***
**Дульский А.Д.** – аспирант кафедры политологии факультета исторических и политических наук; старший лаборант кафедры политологии факультета исторических и политических наук Национального исследовательского Томского государственного университета (Томск, Россия). E-mail: Dulya_ad@mail.ru

***Автор заявляет об отсутствии конфликта интересов.***

***Information about the author:***
**Dulsky A.D.** – postgraduate student, senior laboratory assistant at the Department of Political Science, Faculty of Historical and Political Sciences, National Research Tomsk State University (Tomsk, Russian Federation). E-mail: Dulya_ad@mail.ru

***The author declares no conflicts of interests.***

*Статья поступила в редакцию 04.09.2025;*
*одобрена после рецензирования 30.09.2025; принята к публикации 24.10.2025*
*The article was submitted 04.09.2025;*
*approved after reviewing 30.09.2025; accepted for publication 24.10.2025*