

К ВОПРОСУ О ПРЕОДОЛЕНИИ РИСКА ФАЛЬСИФИКАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ НА ВЫБОРАХ

© 2016 г. Ксения Юрьевна Матрёнина¹

В данной статье автор обосновывает актуальность применения средств электронного голосования на выборах, анализирует возможные ситуации фальсификации результатов выборов при использовании современных информационно-коммуникационных технологий. Автор исследует применение государственной автоматизированной системы “Выборы”, комплекса обработки избирательных бюллетеней и комплекса для электронного голосования в российском избирательном процессе, выявляет защитные свойства системы и комплексов от фальсификации результатов голосования. Анализирует мероприятия, направленные на преодоление риска фальсификации результатов выборов на территории таких государств, как Бразилия, США, Нидерланды, Германия и Швейцария (например, тестирование машин для электронного голосования). Автором предложены рекомендации по устранению риска фальсификации.

In this article the author proves a relevance of application of electronic voting methods on elections and analyzes possible situations of falsification of election's results when using modern information and communication technologies. The author investigates the use of the state automated system “Elections”, the optical scan voting system (KOIB in Russian) and the complex for electronic voting in the Russian electoral process, reveals protective properties of the system and the complexes from a falsification of voting's results. The author analyzes the measures directed to a negotiation of the risk of falsification of election's results in the territory of such states as Brazil, the USA, the Netherlands, Germany and Switzerland (for instance, testing the machines for electronic voting). The author proposed the recommendations for removal the risk of a falsification.

Ключевые слова: государственная автоматизированная система “Выборы”, комплекс обработки избирательных бюллетеней, комплекс для электронного голосования, электронное голосование, выборы, информационно-коммуникационные технологии, фальсификация, система электронного голосования, Интернет, тестирование.

Key words: the state automated system “Elections”, the optical scan voting system, the complex for electronic voting, electronic voting, election, information and communication technologies, falsification, the electronic voting system, Internet, testing.

В соответствии с ч. 3 ст. 3 действующей Конституции РФ высшим непосредственным выражением власти народа являются референдум и свободные выборы. Таким образом, средства волеизъявления граждан играют важную роль, значение которой не меньше, чем сам факт проведения выборов. Это обусловлено в первую очередь тем, что институт выборов имеет смысл лишь тогда, когда осуществляется объективная фиксация воли избирателей, формируются и реализуются надлежащие условия для ее изъяснения.

Начиная с 1993 г. осуществляется непрерывная модернизация избирательной системы и избирательного законодательства России, основными направлениями которой являются совершенствование правового регулирования избирательного процесса, разработка мероприятий, направленных на обеспечение эффективной реализации избирательных прав граждан.

Общественное желание не только быстрого, но и объективного подведения итогов голосования на выборах побуждает государства постоянно модернизировать национальную избирательную систему, в частности использовать новые технологии в избирательном процессе. Не стоит забывать, что автоматизация – это сложный процесс, особенно в странах с ограниченной инфраструктурой.

Применение современных информационно-коммуникационных технологий в деятельности государственных органов и органов местного самоуправления, в области образования, здравоохранения и прочих сферах деятельности побуждает государства активно внедрять их в национальную практику. Одним из перспективных направлений их применения являются разработка, введение и дальнейшее развитие системы электронного голосования (далее – СЭГ).

Электронное голосование (далее – ЭГ) представляет собой новую, развивающуюся область избирательного процесса и, соответственно, весьма актуальную. ЭГ подразумевает под собой не только новоявленные формы учета волеизъявления избирателей. Данный вид голосования – качественно новый в организации и проведении выборов.

¹ Аспирант кафедры конституционного и муниципального права Института государства и права Тюменского государственного университета (E-mail: kseniya.matr@yandex.ru).
Kseniya Matryonina, post-graduate student Department of constitutional and municipal law, Institute of state and law of Tyumen state University (E-mail: kseniya.matr@yandex.ru).

Актуальность данной темы, на наш взгляд, чрезвычайно велика, особенно в связи с объективной необходимостью расширения реформационной деятельности в отношении демократических институтов в стране.

Особо отметим, что современные технологии существенно меняют характер и архитектуру политической коммуникации. Значительно возросшие темпы развития российского общества, прежде всего связанные с возникновением широкого спектра его структур, «видоизменение функционирования общественных организаций (возникновение сетевых сообществ и организаций, Интернет-парламентов и Интернет-партий)»² подводят к неизбежности применения современных информационно-коммуникационных технологий как инструмента эффективного взаимодействия государства и общества, что также подтверждает высокую актуальность данного направления.

ЭГ как новая и перспективная возможность подачи избирателем голоса интересует все больше исследователей в различных отраслях науки. Полагаем, что ЭГ есть перспективное направление избирательного процесса, который способен при комплексном и глубоком анализе СЭГ, разумном применении современных технологий, создании систем эффективного контроля и надлежащей гарантированной защиты обеспечить другой механизм голосования, отличающийся качественно новым уровнем удобства, скорости, прозрачности и безопасности. Действительно, массовый процесс автоматизации – это новый курс в организации системы голосования как условия модернизации избирательной системы, новый шаг технологического совершенствования избирательного процесса.

Электронная демократия и интерактивное голосование (ЭГ) создают много новых возможностей, но в то же время несут и некоторые очевидные угрозы. Полагаем, при введении новых технологий в избирательный процесс необходимо не только предусмотреть возможные технические проблемы их внедрения, но и проанализировать их воздействие на избирательную систему в целом. Следовательно, как в медицине, следует реализовывать мероприятия, направленные на установление и преодоление побочных эффектов применения современных технологий на выборах.

Нарушение конституционного принципа свободных выборов, по нашему мнению, связано с фальсификацией результатов голосования. Искажая результаты выборов, происходит относительное влияние на волю избирателя, на сделанный им выбор. Фальсификация результатов голосования посягает на суверенитет многонационального народа Российской Федерации в целом, «ибо не позволяет всему народу как единой общности осуществить весь объем принадлежащей ему власти»³.

В 1983 г. программист К. Томсон (*K. Thompson*) сообщил, что при применении технологий при голосовании существует возможность изменения итогов выборов путем введения в программное обеспечение секретного кода, активизирующего в день проведения выборов и фальсифицирующего результаты голосования; Томсон назвал этот код «Рождение

стеньские яйца»⁴. В связи с существованием проблемы фальсификации итогов выборов сотрудниками Массачусетского технологического института создана программа «Безопасные выборы»⁵, воплотившая в себе ключевые требования по защите данных.

Полагаем, что чрезмерное необоснованное убеждение общественности в объективности СЭГ и ее защите от неправомерного доступа может являться ширмой для проведения скрытых манипуляций с итогами выборов. В частности, зарубежный опыт демонстрирует серьезные риски, связанные с возможностью вторжения извне в систему обработки голосов избирателей, поданных с помощью способов электронного удаленного голосования⁶. Однако профессор Вестфальского университета им. Вильгельма (Университет Мюнстера, Германия) Н. Керстинг отмечает, что применение средств ЭГ исключает «внешние манипуляции, например, внедрение компьютерных вирусов, «троянских коней» или хакерских атак»⁷, в связи с тем, что информация фиксируется машинами для ЭГ, конструкцией которых не предусмотрены выходы во внешнюю среду. По словам Ларрабаала (Филиппины), «электронное голосование может стабилизировать демократию»⁸, так как технологии голосования, применяемые в Филиппинах, в соответствии с результатами многочисленных проверок продемонстрировали невозможность совершения манипуляций с машинами для голосования.

В Российской Федерации базой ЭГ является Государственная автоматизированная система «Выборы» (далее – ГАС «Выборы»), которая стала неотъемлемой частью российской избирательной системы. Назначение ГАС «Выборы» заключается в повышении эффективности избирательного процесса на основе применения современных информационно-коммуникационных технологий. Указанная система позволяет параллельно с голосованием проводить проверку подлинности бюллетеней, технически обеспечивать защиту результатов голосования от фальсификации. Более того, она направлена на обеспечение соблюдения норм права, так как «существует более 150 законов, которые учитываются в ГАС «Выборы»»⁹. Нормативные правовые акты, поддерживающие функционирование системы, устанавливают порядок проведения выборов и распределения мандатов, сроки и проч. Таким образом, ГАС «Выборы» гарантирует законность избирательного процесса, защиту от нарушений правовых норм и фальсификации итогов голосования.

На российских выборах применяются такие средства ЭГ, как комплекс обработки избирательных бюллетеней («электронная урна» – КОИБ) и комплекс ЭГ (машина для ЭГ – КЭГ).

Для обеспечения принципа равного избирательного права, а также для устранения фальсификации итогов голосования при использовании КЭГ проверяется невозможность:

⁴ Селкер Т. Электронное голосование: как оптимизировать процесс проведения выборов // В мире науки. 2005. № 1. С. 64.

⁵ Титовская Н.В. Электронное тайное голосование в России и за рубежом: сравнительно-правовой анализ // Юрид. наука. 2012. № 4. С. 108.

⁶ Подробнее об этом см.: Вешняков А.А. Проблемы использования Интернета на выборах в Российской Федерации // Информационное право. 2006. № 3. С. 15–22.

⁷ Керстинг Н., Грачев М.Н. Электронное голосование и демократия в Европе // Политическая наука. 2007. № 4. С. 128.

⁸ Making elections reliable and interesting // Modern Democracy. 2011. № 1. Р. 5.

⁹ Попов М. Перед началом революции // Intelligent Enterprise/Корпоративные системы. 2010. Спецвып. С. 8.

² Голычев А.А. Электронная демократия как фактор повышения политического участия граждан современной России. Дисс. ... канд. полит. наук. М., 2006. С. 6.

³ Матейкович М.С. Защита избирательных прав граждан в Российской Федерации: проблемы теории и практики. Автореф. дисс. ... доктора юрид. наук. Саратов, 2003. С. 13.

1) голосования с использованием карточки со штрих-кодом до ее активации; 2) повторного голосования по использованной карточке; 3) повторной активации карточки для голосования.

Встречается точка зрения, что при использовании машин для голосования могут возникнуть внутренние ошибки программного обеспечения (например, теоретическая возможность программирования КОИБ и КЭГ на определенный результат еще до начала выборов). Однако эксперты утверждают, что такие действия технически невозможны из-за качественной сертификации СЭГ.

Существует риск возможности осуществить попытку непосредственного воздействия на КОИБ путем установки флешки с неизвестным программным продуктом в разъем КОИБ взамен извлеченной флешки с исходными данными, подготовленными средствами ГАС “Выборы”. Однако данный риск был полностью исключен в ходе публичного тестирования КОИБ в мае 2015 г.

При применении КОИБ исключены возможности обмана при подсчете избирательных бюллетеней и фальсификации итогов голосования на избирательных участках. Во-первых, это связано с обязанностью членов избирательных комиссий следовать инструкциям, законам. Во-вторых, КОИБ представляет собой не просто “электронную урну”, а сертифицированную “электронную урну”. Так, КОИБ выпускается в соответствии с ТУ 4013-001-17404049-2003, сертифицирован в системе ГОСТ Р Госстандарта России (сертификат соответствия № РОСС RU.МЕ20.А02373) и имеет санитарно-эпидемиологическое заключение № 77.МЮ.01.401.П.011522.03.05. Программное обеспечение КОИБ сертифицировано “на отсутствие недеklarированных возможностей, его код зафиксирован контрольной суммой, следовательно, любое изменение программного обеспечения можно проверить”¹⁰.

Было отмечено, что фальсификация итогов голосования при применении КОИБ становится практически невозможной. Однако существует возможность искажения результатов выборов, пусть и минимальная. Как же устранить данный риск? В соответствии с действующим законодательством ключевой носитель (флешка) выдается председателю участковой избирательной комиссии (УИК) накануне выборов в вышестоящей территориальной избирательной комиссии, чтобы можно было провести тестовое включение КОИБ, убедиться в его работоспособности. Ответственность за сохранность данного ключа с этого момента лежит на председателе УИК. При этом закон не требует, чтобы председатель хранил ключевой носитель в сейфе. Не исключено, что для сохранения данных на ключевом носителе используются и дополнительные уровни защиты, которые делают вмешательство в данные невозможным. Тем не менее, на наш взгляд, председателю УИК следует хранить ключевой носитель в специальном сейфе.

Достоин уважения проведение тестирования средств ЭГ в Российской Федерации. 21 мая 2015 г. в Центральной избирательной комиссии РФ было продемонстрировано российское средство ЭГ – КОИБ. В указанном мероприятии участвовали не только специалисты и эксперты в сфере современных информационно-коммуникационных технологий, но и кандидаты на выборах, журналисты. В рамках испытаний КОИБ проведен пересчет голосов, в итоге проведе-

ния которого результаты ручного подсчета бюллетеней полностью совпали с результатами, полученными с помощью КОИБ. Кроме этого не была выявлена возможность удаленного воздействия как на работу УИК, так и на технические средства подсчета голосов. Таким образом, публичное тестирование в очередной раз подтвердило надежность и безопасность КОИБ.

Следует отметить, что различные группы участников избирательного процесса неоднократно проверяли на “прочность” электоральную технику при активной поддержке организаторов выборов как в ЦИК России и избирательных комиссиях субъектов Федерации, так и на других площадках.

Полагаем, что мероприятия, направленные на проверку средств ЭГ, позволяют убедиться в безопасности и прозрачности избирательного процесса в России.

По нашему мнению, необходимо реализовать использование КОИБ и КЭГ в качестве эксперимента на всех избирательных участках одного из субъектов Федерации при проведении выборов главы субъекта России или законодательного (представительного) органа государственной власти субъекта Федерации. Указанное предложение обеспечит более углубленное внедрение электронного голосования на выборах, позволит эффективнее проанализировать влияние современных технологий голосования на электоральную активность, осуществить комплексный анализ защиты системы от фальсификации.

Таким образом, для устранения риска нарушения принципа достоверности следует реализовывать мероприятия, направленные на постоянные проверки и тестирование СЭГ. В мировой практике существуют подобные примеры.

Бразилия. В данном государстве машины для ЭГ неоднократно подвергались проверкам, суть которых заключалась в выявлении возможных пробелов и проблем в СЭГ путем реализации целенаправленных атак хакеров. Власти Бразилии с целью увеличения активности и заинтересованности в проведении указанных испытаний предусмотрели вознаграждение для победителя “в размере 5000 евро”¹¹. За время использования компьютеризированной системы голосования на бразильских выборах проведено несколько аудитов и обзоров. В 2002 г. университет Кампинаса пришел к заключению, что “СЭГ отвечает фундаментальным требованиям избирательного процесса, другими словами, уважает выбор избирателя и гарантирует свою конфиденциальность”¹². В 2008 г. федеральная полиция Бразилии в техническом отчете о муниципальных выборах 2008 г. в Касинсе отклонила все утверждения о мошенничестве при использовании машин для ЭГ.

США. На примере Бразилии в США проводились экспериментальные проверки СЭГ на безопасность. Так, в штате Мэриленд в ходе проведения эксперимента по взлому компьютеров “специалисты легко взломали систему, подтасовали результаты голосования”¹³. В сентябре 2010 г. ученые

¹⁰ Болотин С.С., Халин В.И. Практика применения специальных технических средств на выборах в органы местного самоуправления // Альманах современной науки и образования. 2013. № 8. С. 30.

¹¹ Бразилия – страна сплошной электоральной автоматизации [Электронный ресурс] // Electorat.info // <http://www.electorat.info/blog/5152.html> (Дата обращения: 20.04.2014 г.).

¹² The Biometrical System in Brazil [Электронный ресурс] // <http://english.tse.jus.br/electronic-voting/the-biometrical-system-in-brazil> (Дата обращения: 20.04.2014 г.).

¹³ О соблюдении в США избирательных прав граждан [Электронный ресурс] // Росс. газ. // <http://www.rg.ru/2012/10/30/vibori-site.html> (Дата обращения: 22.04.2014 г.).

Университета Мичигана провели учебную атаку на пилотную систему голосования с использованием сети Интернет в Вашингтоне (округ Колумбия). Без особых сложностей исследователи под руководством проф. А. Холдермана осуществили инфильтрацию и посягали на СЭГ: трансформировали бюллетени, поменяли пароль и заставили машину играть гимн своего вуза. “За 36 часов... мы установили полный контроль над электронной системой голосования”, – сказал проф. А. Холдерман¹⁴.

Нидерланды. В сентябре 2006 г. после трансляции по телевидению заявления, уверяющего общественность, что машины для ЭГ не обладают важнейшим признаком – безопасностью, в начале октября того же года экспертная группа Нидерландов приобрела две машины *NEDAP ESB3* с целью их проверки. В результате многочисленных проверок эксперты смогли заменить микросхему памяти в машине для голосования менее чем за пять минут, что позволило им управлять результатами выборов.

После этого Правительство Нидерландов объявило о необходимости укрепления безопасности машин и потребовало провести их независимое тестирование. Что касается тестирования, то три из четырех машин для голосования *NEDAP* прошли тест. Однако в результате проверки машины *SDU* была выявлена серьезная проблема, а именно – перехват радио-эмиссии. В результате было принято решение не использовать машины *SDU* на выборах. Указанное решение было принято всего за три недели до выборов, вследствие чего “1200 машин для ЭГ не могли быть использованы на выборах”¹⁵. Несколько больших городов должны были или вернуться к традиционному голосованию, как сделал Амстердам, или применять для ЭГ машины *NEDAP*.

Германия. В конце 2008 г. политолог Й. Виснер (*J. Wiesner*) и его сын, программист, У. Виснер (*U. Wiesner*) обратились с иском в суд в Карлсруэ о запрете голосовать с помощью компьютера по причине противоречия данного вида голосования основополагающим принципам демократии. Для правильного рассмотрения иска и принятия обоснованного решения по существу заявленного спора судом было поручено группе специалистов изучить “1,8 тыс. компьютеров голландской фирмы *NEDAP*, задействованных для голосования 3,5 г. назад”¹⁶. В ходе проверок, испытаний было доказано, что электронная система голосования *NEDAP* является ненадежной, а сами компьютеры для голосования – “безнадёжно отставший от времени мусор, которому место на свалке вместе с выданной этой фирмой 20-летней гарантией их надежности”¹⁷. Несмотря на тот факт, что комплексная, детальная проверка протоколов голосования с использованием машин для ЭГ на выборах 2005 г. не обнаружила манипуляции с избирательными бюллетенями и результатами голосования, а также сбои в работе машин,

вице-президент Бундестага П. Пау (*P. Pau*) заявила: “Не все, что технически возможно, политически допустимо”¹⁸.

В результате неоднократного подтверждения отсутствия безопасности в СЭГ при применении машин для голосования *NEDAP* было принято решение не о полном запрете электронной системы голосования, а только о “запрете использования машин указанного поколения”¹⁹. Однако в 2009 г. Германия приостановила работу как над разработкой новой СЭГ, так и над использованием старой.

Швейцария. Следует отметить, что ЭГ в Швейцарии достойно доверия. Так, при применении технологий на выборах отсутствует возможность систематического увода голосов. Рассмотрим данное утверждение детальнее.

СЭГ состоит из трех основных элементов: компьютера избирателя, канала связи и официального сайта для голосования. Данные защищаются с помощью специального туннеля связи между компьютером избирателя и сайтом для голосования. Туннель создает дополнительный слой шифрования на канал связи, препятствует проникновению вирусов из компьютера избирателя на сайт для голосования и накопец, в урну для голосования²⁰.

Для устранения риска фальсификации результатов голосования избирателю перед выборами по почте направляется карточка для проведения голосования, содержащая следующую информацию: номер избирателя, секретный код для регистрации на сайте для голосования, а также контрольный четырехзначный код, который позволяет обеспечить тайное волеизъявление. С целью предотвращения повторного голосования карточка является одноразовой, тем самым обеспечивается равное право на участие граждан в выборах. Более того, избиратель обладает правом проверить подлинность сайта с помощью электронного сертификата сайта и исходный код системы. Указанные выше принципы электронной системы голосования позволяют утверждать о наличии эффективного механизма независимого аудита электронной системы голосования у избирателей.

Необходимо, на наш взгляд, признать, что информация в современном и динамично развивающемся обществе имеет большое значение. Прогресс человечества видится французскому мыслителю Ж.-А.-Н. Кондорсе (1743–1794 гг.) как прогресс развития²¹. Канадский социолог Г.М. Маклюэн считал, что основным двигателем истории и “важнейшим инструментом процесса развития общества является смена информационных технологий”²². Движение к информационному обществу – это путь в будущее человеческой цивилизации, как отмечено в Окинавской хартии глобального информационного общества²³, которая была подписана лидерами стран “Большой восьмерки” в 2000 г. в Японии.

¹⁴ См.: Используемая в США система Интернет-голосования была взломана за три часа [Электронный ресурс] // Компьюлента // <http://compulenta.computerra.ru/archive/election/572479/> (Дата обращения: 22.04.2014 г.).

¹⁵ Goldsmith B., Ruthrauff H. Implementing and overseeing Electronic voting and counting technologies. USA: The National Democratic Institute, 2013. P. 260.

¹⁶ Германия отказывается от электронного голосования [Электронный ресурс] // Журнал “ПЛАС” // <http://www.plusworld.ru/daily/germaniya-otkazivaetsya-ot-elektronno-go-golosovaniya/> (Дата обращения: 14.10.2014 г.).

¹⁷ Электронная демократия // NewsBabr.com // <http://newsbabr.com/?IDE=77528> (Дата обращения: 14.10.2014 г.).

¹⁸ Там же.

¹⁹ Рудницкий Г. Электронное голосование: опыт зарубежных стран [Электронный ресурс] // Госбук // <http://www.gosbook.ru/node/12744> (Дата обращения: 16.10.2014 г.).

²⁰ См.: Шульга-Морская Т.В. Электронное голосование: опыт и перспективы Швейцарии и России // Адвокат. 2013. № 3. С. 60.

²¹ Цит. по: Елимаев А.Т. Электронная демократия как инновационный инструмент развития гражданского общества в Российской Федерации // Вестник ТюмГУ. 2014. № 8. С. 115.

²² Маклюэн Г.М. Галактика Гутенберга. Сотворение человека печатной культуры. М., 2013. С. 52.

²³ Доступ из СПС “КонсультантПлюс” (Дата обращения: 05.02.2013 г.).

При проведении работы по разработке голосования через Интернет нужно очень системно подойти к разработке такого голосования, чтобы избежать возможных сбоев, хакерских атак и проч., ведь атаки хакеров и фальсификация итогов голосования могут в значительной степени подорвать легитимность политической системы. По нашему мнению, самое надежное Интернет-голосование возможно с помощью электронного паспорта, как в Эстонии. При этом целесообразно установить возможность использовать *ID-карты* и для других электронных услуг. Указанное решение позволит гражданам быстрее изучить, как использовать указанные карты, а также убедиться в простоте и удобстве их применения.

Итак, при всех положительных сторонах использования в избирательных кампаниях государственного масштаба СЭГ есть один важный момент, который заставляет еще раз задуматься над проблемами развития этой автоматизированной системы: это – вторжение извне в электронную систему голосования и гипотетическая возможность фальсификации результатов выборов. Во избежание искажения результатов голосования «развитие автоматизации на российских выборах должно идти параллельно с законодательным обеспечением гарантий открытости и гласности при использовании

автоматических средств»²⁴. Таким образом, с практической точки зрения институт ЭГ в правовом аспекте нуждается в детальной законодательной регламентации.

Необходимо понимать, что ЭГ не является панацеей, однако при разумном введении и правильном применении оно может стать полезным инструментом для демократических выборов. Полагаем, что будущее – за электронным голосованием. Успешный и богатый зарубежный опыт некоторых государств в области применения технологий на выборах показывает, что электронные выборы возможны. Вопрос только в том, когда будет введено масштабное электронное голосование на выборах в России, в какой форме оно будет осуществляться: с помощью КОИБ и КЭГ или будет введено Интернет-голосование? Ответы на указанные вопросы находятся в прямой зависимости от уровня развития техники, качества нормативно-правового регулирования, инфраструктуры государства, готовности избирателей реализовывать свое активное избирательное право таким способом и проч.

²⁴ Загайнов С.В. Избирательный процесс в современной России: конституционно-правовой аспект. Дисс. ... канд. юрид. наук. Майкоп, 2006. С. 37.