

РЕАЛИЗАЦИЯ КОНСТИТУЦИОННЫХ ПРАВ ГРАЖДАН ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

© 2015 г. Ксения Юрьевна Матрёнина¹

Аннотация: в статье исследована реализация конституционного права граждан на свободные выборы при проведении электронного голосования; рассматривается международное законодательство в области свободного избирательного права. Автор проанализировал возможные варианты нарушения принципа свободных выборов. Исследованы мероприятия, направленные на устранение фальсификации результатов выборов при проведении электронного голосования. Проведен анализ комплекса обработки избирательных бюллетеней и комплекса для электронного голосования на соответствие исследуемому принципу избирательного права. Автор исследовал опыт обеспечения реализации свободных выборов при проведении электронного голосования в Эстонии и Бразилии. В результате проведенного исследования сделаны выводы о позитивном российском опыте по обеспечению свободного избирательного права при использовании электронных средств голосования на выборах.

Annotation: in the article the author has examined the realization of constitutional right of citizens to free election of electronic voting; considers the international legislation in the area of free suffrage. The author has analysed possible options of a violation of the principle of free elections. The author has investigated the actions directed on an elimination of falsification of election results of electronic voting. In the article the author analysed the optical scan voting system (KOIB in Russian) and the complex for electronic voting on compliance to the principle of free suffrage. The author has investigated the experience of ensuring of free elections realization of electronic voting in Estonia and Brazil. The article concludes that there is a positive Russian experience on ensuring of free suffrage of using electronic means of voting on elections.

Ключевые слова: выборы, Интернет, электронное голосование, свободное избирательное право, комплекс обработки избирательных бюллетеней, комплекс для электронного голосования, фальсификация, Эстония, Бразилия, технологии.

Key words: elections, the Internet, electronic voting, free suffrage, the optical scan voting system, the complex for electronic voting, falsification, Estonia, Brazil, technologies.

В настоящее время в сети Интернет существует большое количество сайтов, направленных на реализацию электронной демократии (“Демократ”, “Демократия 2”). Электронная демократия заключается не только в публичном обсуждении общественно значимых проблем с помощью технологий, но и в формировании органов публичной власти с помощью информационных технологий. Таким образом, электронное голосование есть неотъемлемая составляющая электронной демократии.

Электронное голосование – не новая тема для обсуждения в рамках международных семинаров или в национальной электоральной практике. Однако это не исключает ее актуальности, заинтересованности государств, а также наличия различных мнений и подходов к указанному вопросу.

Российская Федерация активно осваивает информационные технологии при организации и проведении выборов. За последние годы выборы в России стали современным и технологичным процессом, использующим новейшие технологии для голосования избирателей, подведения его итогов и определения результатов выборов.

В соответствии с ч. 3 ст. 3 Конституции РФ высшим непосредственным выражением власти народа являются референдум и свободные выборы. Традиционно под свободными

выборами понимают две составляющие: добровольность и запрет оказывать влияние, давление на избирателей. Возникает вполне очевидный вопрос: являются ли электронные выборы свободными? Действительно, вполне возможно оказание влияния на избирателей, как и при традиционном голосовании с использованием бумажных бюллетеней.

Принцип свободных выборов закрепляется конституциями большинства демократических государств; ряд основополагающих международных актов устанавливает обязательность соблюдения данного принципа на выборах. Так, согласно п. “а” ст. 25 Международного пакта о гражданских и политических правах от 16 декабря 1966 г.² каждый гражданин должен иметь право и возможность голосовать на выборах, обеспечивающих свободное волеизъявление избирателей. Пункт 3 ст. 21 Всеобщей декларации прав человека (принята Генеральной Ассамблеей ООН 10 декабря 1948 г.)³ устанавливает, что воля народа должна находить свое выражение в периодических и нефальсифицированных выборах, которые должны проводиться при всеобщем и равном избирательном праве путем тайного голосования или же посредством других равнозначных форм, обеспечивающих свободу голосования.

Безусловно, организация электронного голосования должна обеспечить безопасность свободного формирования

¹ Аспирант кафедры конституционного и муниципального права Института государства и права Тюменского государственного университета (E-mail: kseniya.matr@yandex.ru).

² См.: Бюллетень Верховного Суда РФ. 1994. № 12.

³ См.: Росс. газ. 1995. № 67.

и выражения мнения избирателя, а там, где это требуется, и личного осуществления избирательного права. Более того, система электронного голосования не должна допускать возможности оказания манипулирующего воздействия на избирателя в ходе голосования.

В Рекомендациях R (2004) 11 Комитета Министров Совета Европы по правовым, организационным и техническим стандартам электронного голосования (приняты Комитетом Министров 30 сентября 2004 г. на 898-м заседании)⁴ (далее – Рекомендации) закреплено, что система электронного голосования должна четко и ясно указать избирателю на то, что его голос был успешно принят, и что вся процедура голосования завершена. Кроме этого Рекомендации устанавливают, что система электронного голосования должна предотвратить возможность изменения содержания поданного голоса после того, как он был подан. На наш взгляд, изменение голоса избирателя имеет наибольший риск при проведении дистанционного электронного голосования, в частности интернет-голосования, ведь, как показывает практика, через Интернет можно проголосовать неоднократно. Например, в Эстонии голосовать электронным путем можно в течение семи дней: с 10 дня по четвертый день перед днём выборов⁵. Кроме этого в период электронного голосования избиратель может заново отдать электронный голос, однако учитывается только последний отданный голос. Следует отметить, что в Эстонии традиционное голосование обладает приоритетом: если избиратель придет на избирательный участок в период предварительного голосования и проголосует обычным способом (до этого проголосовав электронным путем), то его электронный голос будет аннулирован. Однако в день выборов голос изменить нельзя.

Рассмотрим возможные *варианты нарушения принципа свободных выборов* путем оказания влияния на избирателей при электронном голосовании. Во-первых, при дистанционном электронном голосовании (например, через Интернет) существует риск прямого, физического влияния на избирателя. Голосуя за того или иного кандидата, нет абсолютной уверенности, что за спиной избирателя не стоит человек, оказывающий влияние на волю избирателя, на его решение.

Во-вторых, нарушение конституционного принципа свободных выборов связано с фальсификацией результатов голосования. Искажая результаты выборов, происходит относительное влияние на волю избирателя, на сделанный им выбор.

Остановимся более детально на фальсификации итогов выборов. Необходимо согласиться с В.А. Холоповым, что при любом уровне защиты данных работа этих созданных человеком систем не исключает полностью возможность доступа специалиста к результирующим данным, а следовательно, принципиально существует способ изменить нужным образом результаты голосования⁶. С нашей точки зрения, ссылки на объективность компьютера и защиту информации от несанкционированного доступа в этом случае могут служить ширмой для прикрытия манипуляций с результатами голосования. Зарубежный опыт показывает,

что при проведении электронного голосования существуют серьезные риски, связанные с возможностью вторжения извне в системы обработки голосов избирателей, поданных при помощи дистанционных способов голосования, и связанная с этим необходимость обеспечения неизменности информации о волеизъявлении⁷. Что касается комплексов обработки избирательных бюллетеней (далее – КОИБ), которые весьма активно применяются на территории Российской Федерации, то и здесь могут быть определенные риски. Например, сложно исключить возможность программирования КОИБ еще до начала выборов на определенный результат. Однако многие эксперты выделяют среди достоинств КОИБ именно исключение возможности подлогов 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 сертифицирован Госстандартом России (сертификат соответствия) и Министерством здравоохранения РФ (гигиенический сертификат).

Целесообразно сказать о Государственной автоматизированной системе России “Выборы” (далее – ГАС “Выборы”), которая является неотъемлемой частью избирательной системы Российской Федерации. Основное назначение указанной системы заключается в повышении эффективности избирательного процесса на основе применения современных информационно-коммуникационных технологий. Несмотря на повышенную защиту ГАС “Выборы”, на нормативно-правовое регулирование, в день голосования на выборах Президента РФ в марте 2004 г.⁸, а также в ходе федеральных выборов в декабре 2011 г. и в марте 2012 г. были обнаружены преступные посяательства в виде неправомерного внешнего воздействия (атаки хакеров) на структурные элементы ГАС “Выборы”. Кроме того, возможно вмешательство в деятельность системы изнутри с целью искажения передаваемых через систему данных. Например, путем указаний системному администратору о введении измененных данных протоколов участковых, территориальной или иной избирательных комиссий.

Другое активно применяемое на территории Российской Федерации средство электронного голосования – комплекс для электронного голосования (далее – КЭГ) – характеризуется отсутствием ошибок при подсчете бюллетеней и своей безопасностью. КЭГ обеспечивает реализацию свободного избирательного права, так как комплексы локальны, не связаны с Интернетом, благодаря чему они надежно ограждены от хакерских атак. Кроме этого при создании комплексов использовалось “прошитое” микропрограммирование на уровне микроконтроллеров, которое практически невозможно изменить⁹.

Что касается международного опыта, то с целью улучшения программного обеспечения бразильские машины для электронного голосования неоднократно подвергались испытаниям на безопасность. Так, с 10 до 13 ноября 2009 г. проводились первые испытания системы электронного голо-

⁴ См.: <http://idemocracy.ru/projects/стандарты/45-e-voting-rec2004-11.html> (Дата обращения: 12.01.2015 г.).

⁵ См.: Электронное голосование в Эстонии // <http://www.valimised.ee/ru/uldkirjeldus> (Дата обращения: 13.01.2015 г.).

⁶ См.: Холопов В.А. Модернизация механизмов реализации институтов непосредственной демократии: анализ зарубежного и российского опыта проведения электронного голосования // Конституционное и муниципальное право. 2011. № 9. С. 67.

⁷ Подробнее об этом см.: Вешняков А.А. Проблемы использования Интернета на выборах в Российской Федерации // Информационное право. 2006. № 3. С. 15–22.

⁸ См.: Турищева Н.Ю. Государственная автоматизированная система Российской Федерации “Выборы” как автономный признак состава преступления // Росс. следователь. 2008. № 16. С. 27.

⁹ См.: там же.

сования Бразилии. Суть заключалась в том, что целенаправленные атаки хакеров должны были найти в бразильских машинах для голосования любые возможные пробелы в безопасности системы. Победитель должен был получить 5 тыс. евро¹⁰. Однако ни один из тестов не смог нарушить машину и поместить в программное обеспечение вредоносный вирус. Второй этап тестов проводился с 20 до 22 марта 2012 г., где следователи, ученые и программисты смогли участвовать в предварительной фазе, в которой они уже имели доступ к исходному коду машины электронного голосования и смогли узнать еще больше об особенностях системы¹¹.

Бесспорно, если программное обеспечение надежно не защищено паролем, то оно может подвергаться хакерским и вирусным атакам, а также злоупотреблениям со стороны заинтересованных лиц. Эту проблему впервые отметили еще американские эксперты (Джефферсон, Симонс, Рубин и Вагнер). Кроме этого, учитывая особое геополитическое значение нашей страны, при введении подобных новшеств должна быть твердая уверенность и стопроцентная гарантия того, что в период проведения выборов Интернет не будет использован с целью повлиять на результаты голосования различными экстремистскими и террористическими организациями, разведывательными службами иных государств. Как и в зарубежных странах, в России уровень защиты играет и должен играть главенствующую роль.

На наш взгляд, дистанционное электронное голосование – далекая перспектива для России, однако другие средства электронного голосования (КОИБ, КЭГ), применяемые на территории Российского государства, должны быть на высшем уровне как с технической стороны, так и с правовой. Именно поэтому нормативно-правовое регулирование и техническое состояние автоматизированных средств голосования должны быть на высшем уровне и постоянно совершенствоваться.

Другим способом фальсификации итогов голосования, нарушения конституционного принципа свободных выборов выступает наличие фальшивого сервера для голосования. Технически создание такого сервера вполне возможно. Если есть физическая возможность подключения к сети Интернет, то, используя похищенное программное обеспечение (пароли, ключи и т.д.), можно создать фальшивый сервер для голосования. Он будет аккумулировать варианты голосования реальных избирателей, изменять их в нужную сторону и затем отправлять по Сети на сервер вышестоящей избирательной комиссии. При хорошо продуманной организации фальшивого сервера ни избиратели, ни вышестоящие избирательные комиссии ничего не заметят.

Следует отметить, что в настоящее время необходимый уровень безопасности информации в ГАС “Выборы” обеспечивается путем применения сертифицированных средств защиты информации в соответствии с требованиями эксплуатационно-технической документации, а также путем реализации всех требований, содержащихся в постановлениях ЦИК России, регламентирующих вопросы эксплуатации, порядка использования системы при проведении выборов различного уровня и вопросы безопасности системы¹². Предусмотренные и реализуемые сегодня в системе процедуры

контроля ввода данных, с нашей точки зрения, являются действенной мерой защиты, гарантирующей исключение ошибки при передаче результатов голосования.

Проанализировав отчет о применении КОИБ на выборах 8 сентября 2013 г., мы заметили, что данные 86 (1.44%) протоколов об итогах голосования были введены в базу данных ГАС “Выборы” с признаком ручного ввода. Таким образом, количество протоколов с признаком ручного ввода увеличилось (14 октября 2012 г. количество протоколов с признаком ручного ввода составило 1.1%). В 2013 г. лидерами протоколов с признаком ручного ввода стали следующие регионы: Московская область (20 протоколов), Архангельская область и г. Москва (по 15 протоколов у каждого субъекта)¹³. Практика введения протоколов об итогах голосования в базу данных ГАС “Выборы” с признаком ручного ввода – естественное явление, если речь идет о ручном пересчете голосов. Однако, если данное обстоятельство вызвано другими причинами, это заставляет о многом задуматься.

Каковы же причины ввода данных протоколов с признаком ручного ввода? В 48 случаях нарушение членами участковых избирательных комиссий (далее – УИК) требований инструкции стало прямой причиной ввода протоколов вручную. В девяти случаях такой причиной стали ошибочные действия членов УИК или системного администратора комплексов средств автоматизации территориальной избирательной комиссии (КСА ТИК). Таким образом, компетентность членов избирательных комиссий оставляет желать лучшего.

Полагаем, одной из возможных причин такого большого количества ошибок, допущенных членами УИК (именно намеренных ошибок) может являться фальсификация результатов голосования, так как с помощью КОИБ сфальсифицировать результаты намного сложнее или же вообще нельзя, как отмечают некоторые эксперты. Целью таких намеренных нарушений также может выступать стремление к сокращению или вообще ликвидации доверия граждан к электронному голосованию в целом, к дискредитации новой технологии, и, как следствие, неприменение наиболее защищенных средств электронного голосования, что может привести к фальсификации итогов голосования.

Таким образом, необходимо установить более жесткие требования к членам УИК. Разработать более эффективную модель их обучения. Ведь члены УИК выполняют важную функцию государственного значения, от их компетенции и профессионализма зависит не только процесс голосования и его исход, но и развитие избирательной системы в целом. Необходимо также ужесточить уголовную ответственность за неправомерный доступ и искажение документированной информации в ГАС “Выборы”.

Другие государства давно используют электронное голосование и вполне удачно. Например, в Эстонии интернет-голосование существует с 2005 г. Всего в Эстонии было проведено семь масштабных избирательных кампаний с использованием *I-Voting*: выборы местного уровня 2005, 2009, 2013 гг.; парламентские выборы 2007, 2011 гг.; выборы в Европейский парламент 2009, 2014 гг. При этом, по данным Республиканской избирательной комиссии, отмечается

¹⁰ См.: Бразилия – страна сплошной электоральной автоматизации // <http://www.electorat.info/blog/5152.html> (Дата обращения: 20.04.2014 г.).

¹¹ См.: The Biometrical System in Brazil // <http://english.tse.jus.br/electronic-voting/the-biometrical-system-in-brazil> (Дата обращения: 20.04.2014 г.).

¹² См.: Турищева Н.Ю. Указ. соч. С. 28.

¹³ См.: Отчет о применении технических средств подсчета голосов – комплексов обработки избирательных бюллетеней при проведении голосования на выборах, проведенных на территории субъектов Российской Федерации в единый день голосования 8 сентября 2013 года // <http://www.cikrf.ru/news/relevant/2013/10/21/01.html> (Дата обращения: 12.01.2015 г.).

последовательное увеличение числа избирателей, проголосовавших электронным способом: 1.9% среди всех проголосовавших в 2005 г., 5.5% избирателей в 2007 г., 14.7% избирателей в 2009 г. на выборах в Европарламент, 15.8% избирателей в 2009 г. на муниципальных выборах, 24.3% избирателей в 2011 г., 21.2% избирателей в 2013 г. и 31.3% избирателей в 2014 г. на выборах в Европарламент¹⁴.

В Бразилии машины для электронного голосования применяются с 1996 г., а с 2010 г. с целью защиты от фальсификации – биометрические технологии (идентификация по отпечаткам пальцев)¹⁵.

¹⁴ См.: General Statistics about Internet Voting in Estonia // <http://www.vvk.ee/index.php?id=11178> (Дата обращения: 16.01.2015 г.).

¹⁵ См.: Бразилия – страна сплошной электральной автоматизации.

Считаем, сегодня не подвергается сомнению необходимость продолжения работы над системами электронного голосования. По мнению специалистов по избирательным технологиям, вопрос не в том, нужно ли электронное голосование, а в том, как подготовить и оптимально внедрить его в практику, какое именно средство электронного голосования будет применяться на выборах и в каком масштабе.

В заключение следует отметить, что при детальной законодательной регламентации вопросов электронного голосования и наличии сертификации по единым централизованным стандартам, при высочайшей квалификации членов избирательных комиссий мы сможем предотвратить фальсификацию итогов выборов. Решив данную проблему, мы добьемся действительной реализации конституционного права граждан на свободные выборы, уверенности каждого гражданина в подлинной фиксации своего голоса.