С. В. Абламейко[1,2], С. М. Братченя[2], Н. И. Калоша[3], В. Ю. Липень[2]
Беларусь, [1]Белорусский государственный университет,
[2]Объединенный институт проблем информатики НАН,
[3]Институт математики НАН

ЭКСПЕРИМЕНТАЛЬНАЯ СИСТЕМА ИНТЕРНЕТ-ГОЛОСОВАНИЯ «ГАРАНТ» КАК СРЕДСТВО ПРЕДОСТАВЛЕНИЯ ЭЛЕКТРОННЫХ УСЛУГ ОРГАНИЗАЦИЯМ И АДМИНИСТРАЦИЯМ РЕГИОНОВ

Принятая белорусским правительством Национальная программа ускоренного развития услуг в сфере информационных технологий (ИТ) на период 2011-2015 г. и решение о создании Национального центра электронных услуг (НЦЭУ) ставят перед ИТ- специалистами важные задачи по обеспечению опережающего развития в Беларуси собственной информационной индустрии, основанной на создании оригинальных технологий, ресурсов и услуг.

В докладе представлены результаты исследований по системам сбора и отображения персональных данных, а также сведений (ответов), сообщаемых гражданами в ходе проведения различных мероприятий с участием больших групп респондентов. К подобным мероприятиям можно отнести переписи населения, централизованное тестирование знаний, выборы и референдумы различных уровней, включая уровень местного самоуправления, «праймериз», сбор подписей в поддержку кандидатов, партий или решений и др. Принятые в России решения о выборах губернаторов и иных региональных руководителей, а также внедряемые процедуры сбора 100 тыс. подписей для представления в Государственную думу законодательных инициатив населения, также ставят в ряду важнейших проблему минимизации финансовых затрат и человеческого ресурса для успешного проведения такого большого числа электоральных мероприятий.

Следует отметить, что использование бумажных технологий при фиксации ответов респондентов на местах u при переносе данных с опросных листов (бюллетеней) в протоколы и/или компьютер путем визуального считывания и подсчета, клавиатурного ввода или сканирования имеет следствием высокие затраты и возможность влияния «человеческого фактора». В традиционных реализациях нарушается одно из правил информатики, предписывающее осуществлять перевод данных из исходной аналоговой в цифровую форму непосредственно в месте и во время возникновении новой информации. Внедренная в России дорогостоящая система сбора видеозаписей с избирательных участков предоставляет наблюдателям или судебному заседанию лишь аналоговые изображения, требующие их интерпретации человеком для формирования юридически значимых цифровых характеристик мероприятия. Наличие недостатков ручных технологий дает основания проигравшим кандидатам (партиям) говорить о возможных фальсификациях результатов в пользу действующей власти по указанию местных руководителей, которые организуют работу избирательных комиссий.

Противоположной тенденцией является бурное развитием Интернет-сервисов и увеличением числа пользователей сетевых компьютеров, а также мобильных смартфонов и планшетных компьютеров с беспроводным доступом . Это создает условия для того, чтобы, решая проблему повышения эффективности мероприятий по сбору персонализированных данных, переходить к их онлайн-реализации. При этом не потребуется создания сети региональных пунктов сбора подписей и станций голосования, а также вложения значительных финансовых средств для их оснащения комплексами на базе специальных компьютеров или микропроцессорных устройств, подобных внедренным в Индии, Бразилии, Венесуэле, США, Казахстане, России и ряде иных стран. Отметим, что подобные дорогостоящие комплексы используются только в дни проведения мероприятий, простаивая в остальное время. К их недостаткам можно отнести и отсутствие возможности убедить избирателя, что его голос засчитан в актив именно тому кандидату, партии, ответу на вопрос референдума, которые он предпочел при голосовании. Действительно, при опускании бумажного бюллетеня или после клавиатурного (сенсорного) ввода данных о предпочтениях избирателя происходит «деперсонализация» индивидуального результата голосования, и далее система оперирует с интегрированными на уровне избирательного участка локальными результатами.

Для реализации интернет-голосования могут использоваться тысячи взаимодействующих с процессинговым центром компьютеров, которые установлены в квартирах, в пунктах коллективного доступа, интернет-кафе, стационарных и подвижных (на автомобилях) почтовых отделениях, исполкомах, вузах, школах. Возможно использование и «электронных учебников», имеющих доступ к сети. Интернет-голосование успешно используется в Эстонии, Швейцарии, Австрии, хотя при его внедрении возникает ряд но

вых проблем. Известно и об успешном опыте экспериментального апробирования интернет-голосования в России.

Представляемая в докладе разработка базируется на оригинальном подходе и использует ряд собственных технологий, позволяющих устранить или снизить влияние недостатков известных систем интернет-голосования. Система «Гарант» может предоставлять электоральные услуги, выполняя при этом роль «доверенной третьей стороны». Услуги по сбору, обработке, отображению и верификации электоральных данных могут предоставляться отечественным и зарубежным организациям, а также муниципальным администрациям, проводящим подобные мероприятия. Для оформления заказа потребитель должен ввести средствами веб-портала сведения о мероприятии, электронные списки избирателей и сведения об объектах кастинга, включая фото кандидата или графическую символику партии. С процедурами заказа и технологическими этапами проведения мероприятия можно ознакомиться на веб-портале http://e-vote.basnet.by/. Там же представлен публикации по системе «Гарант».

В презентации на примере действующего макета веб-портала демонстрируется применение оригинального подхода к формированию защищенных логинов и паролей, используемых для «скрытной» персонализации и верификации результатов, а также для регулирования доступа к исполнению онлайн-процедур в сети. Технология «скрытной» персонализации, предложенная авторами и апробированная в системе «Сайлау» (Казахстан), дает избирателю возможность установить, каким образом в итоговых результатах выборов (референдума) было зарегистрировано его участие (неучастие), а также скрытно проверить, в актив какому кандидату, партии, ответу на вопрос референдума был зачтен его голос. Подобная проверка может осуществляться также и путем обмена SMS-сообщениями. Макет веб-портала позволяет моделировать процедуры внешнего сетевого аудита итогов и коллективного принятия избирателями решения об утверждении итогов выборного мероприятия, отображаемых средствами веб-портала. Результаты моделирования мероприятий с участием 200 тыс. виртуальных респондентов, относящихся к 400 участкам в 20 округах, доступны на странице /demo/ веб-портала. Схема связей системы «Гарант» с множеством субъектов электоральных мероприятий, управление которыми осуществляется параллельно, показана на рисунке.

Рис. Схема взаимодействия системы «Гарант» с субъектами электоральных мероприятий

Важной особенностью предложенной системы является механизм аутентификации, использующий персональные данные избирателя и SID (персональные криптопароли), передаваемые избирателям перед выборами по предъявлении ими паспорта. Каждый SID генерируется по алгоритму $SID_i = EID_i \oplus F_{crypt}(EID_i, K, R_i)$, где *EIDi* - уникальный от-

крытый номер избирателя, $\oplus$ - оператор конкатенации, а F_{crypt} - безопасная криптографическая функция, имеющая аргументы EID_i, секретный ключ K и случайно выбранное секретное R_i, хранимое в доступной лишь криптосерверу базе данных. Функция F_{crypt} действует таким образом, что генерация валидных SID требует знания не только открытых данных и секретного ключа K, но и случайных чисел R_i. Злоумышленнику потребовался бы доступ к базе данных, в которой они хранятся. Секретный ключ и база данных могут быть сделаны открытыми после завершения голосования для проведения аудита удаленными сетевыми наблюдателями.

В Беларуси подобный сервис мог бы быть реализован в составе Общегосударственной автоматизированной информационной системы (ОАИС), являющейся базовым компонентом НЦЭУ. Для подготовки электронных списков избирателей возможно использование данных, накапливаемых в Регистре населения. При этом следует учитывать требования создаваемой Единой системы идентификации физических и юридических лиц, регулирующей реализацию процедур удаленной сетевой аутентификации абонентов, обращающихся к ресурсам ОАИС за предоставлением услуг. За основу при выборе алгоритмов формировании и верификации идентификационных данных физических лиц могут быть приняты переданные в Департамент по гражданству и миграции МВД Беларуси предложения НАН Беларуси, которые используют подходы, представленные в настоящем докладе. Авторы заинтересованы в сотрудничестве с российскими ИТ- специалистами по вопросам развития предложенных подходов, а также в контактах с возможными потребителями услуг системы «Гарант».

Совместное апробирование предложенных технологий может быть осуществлено путем экспериментов по проведению электоральных мероприятий при участии руководителей и респондентов, представляющих отечественные или зарубежные корпорации, университеты, муниципальные образования или партии. Возможны натурные демонстрации работы системы на выставках с участием посетителей в качестве респондентов. Результаты апробирования системы «Гарант» были представлены на ряде конференций [1, 2].

СПИСОК ЛИТЕРАТУРЫ:

1. *Абламейко С. В. Липень В. Ю., Старовойтов В. В.* Моделирование коллективного принятия решений по результатам сетевого сбора персонализированных данных с помощью экспериментальной системы «Гарант» // Искусственный интеллект. Интеллектуальные системы ИИ-2011: материалы Международной научно-технической конференции, пос. Кацивели АР Крым, 19-23 сентября 2011 г. Донецьк: ІПШІ «Наука і освіта», 2011. С. 154-159.
2. *Ablameyko S.* Guarantor E-Voting System Convincing the Electors in Election Transparency / Sergey Ablameyko, Nikolai Kalosha, Sergey Bratchenya, Vitali Lipen // EDEM 2011 - Conference on Elektronic Democracy: Proceedings of the 5th International, September 8-9, 2011, Vienna (ISBN 978-3-85403-284- 7) / Osterreichische Computer Gesellschaft 2011. S. 101-110.