С.В. Абламейко, В.Ю. Липень, В.В. Старовойтов

МОДЕЛИРОВАНИЕ КОЛЛЕКТИВНОГО ПРИНЯТИЯ РЕШЕНИЙ ПО РЕЗУЛЬТАТАМ СЕТЕВОГО СБОРА ПЕРСОНАЛИЗИРОВАННЫХ ДАННЫХ С ПОМОЩЬЮ ЭКСПЕРИМЕНТАЛЬНОЙ СИСТЕМЫ "ГАРАНТ"

Белорусский государственный университет, Объединенный институт проблем информатики НАН Беларуси.

abl@bsu.by, lipen@newman.bas-net.by, valerys@newman.bas-net.by

В докладе рассматривается проблематика НИР, выполняемой авторами в рамках ГПНИ и посвященной разработке перспективных ИКТ, которые должны обеспечить возможности предоставления качественно новых видов государственных информационных услуг организациям и гражданам. Данная НИР является развитием исследований и разработок по программе «Инфотех», выполнявшихся в ОИПИ НАН Беларуси в прошлом пятилетии. Основным содержанием работ является формирование подходов, алгоритмов, технологий и структур, которые могут быть использованы при создании и внедрении более совершенных по сравнению с существующими Веб-технологий, обеспечивающих возможность сетевого сопровождения мероприятий, которые связаны со сбором и обработкой персонализированных данных, получаемых в ходе опросов (учета мнений) больших групп граждан.

Следует отметить, что последние годы охарактеризовались бурным развитием сетей Интернет и резким увеличением числа сетевых компьютеров, а также мобильных смартфонов и планшетных компьютеров с беспроводным Интернет. Это создаёт условия для того, чтобы, решая проблему повышения эффективности сбора персонализированных данных, можно было стремиться к чисто

лектронной реализации таких трудоемких мероприятий, как переписи населения, опросы, централизованное тестирование знаний, выборы и референдумы различных уровней, плебисциты, «праймериз», сбор подписей в поддержку кандидатов, партий или важных решений. При этом могут использоваться сотни тысяч взаимодействующих с Веб-центрами компьютеров, которые будут находиться в пунктах коллективного доступа (центрах обслуживания населения), в Интернет-кафе, в стационарных и подвижных (на автомобилях) почтовых отделениях, исполкомах, школах, вузах, а также и в личном пользовании респондентов.

Использование традиционных бумажных технологий при фиксации на местах ответов респондентов и при последующей централизованной обработке собранных данных сопряжено с неоправданно высокими затратами времени и расходами финансовых и людских ресурсов. Внедрение дешевых и оперативных ИКТ сбора и обработки персонализированных данных, изначально формируемых в электронном виде, дает возможность резко снизить подобные затраты. Так, например, при проведении последней переписи населения в Литве сведения о миллионе жителей были сразу сформированы в электронном виде по данным регистров и электронным ответам граждан. Действительно, переход к более дешевому сбору данных в электронном виде мог бы позволить более часто проводить мероприятия рассматриваемого типа, посвящая их решению широкого круга жизненных проблем. Это помогло бы создать базу для развития местного самоуправления и повышения социальной активности граждан.

При разработке Веб-сервиса по организации электоральных мероприятий «Гарант» авторам пришлось решать ряд задач в области идентификации респондентов, событий, транзакций, документов и файлов данных. Отсутствие у граждан Беларуси идентификационных смарт-карт, подобных используемым в Эстонии и ряде стран ЕС, заставляет разработчиков искать иные способы надежной аутентификации удаленных сетевых респондентов, обращающихся к упомянутому Веб-сервису. В докладе рассматриваются предлагаемые авторами способы аутентификации [1, 2].

На протяжении ряда лет авторами развивается подход, основанный на использовании многокомпонентных криптографических идентификаторов, изначально разработанный для штрих-кодовой маркировки документов и товаров. В докладе на примере действующих макетов Веб-порталов демонстрируется применение оригинального подхода к формированию защищенных логинов и паролей, используемых для «скрытной» персонализации и верификации результатов и для контроля доступа к управлению on-line процедурами [3]. Обсуждается возможность использования биометрических данных граждан, например, заверенного с помощью ЭЦП цифрового фотопортрета, который согласно закону «О регистре населения» должен быть доступен в сети для установления достоверности предъявляемых личных документов или аутентификации удаленного сетевого абонента, обратившегося за услугой к Веб-порталу.

Следует отметить, что простановка подписи в списке избирателей, а также практикуемые сбор и последующий просмотр сотен тысяч подписей в поддержку кандидата или решения также не являются достоверно проверяемыми процедурами. Сбор подписей не предусматривает анонимности волеизъявления респондента, поскольку включает регистрацию его паспортных данных. Если вместо сбора мануальных подписей в бумажных списках перейти на сетевой сбор электронных деклараций, а вместо голосования бумажными бюллетенями перейти на Интернет-голосование, то затраты на оплату труда большой армии сборщиков подписей и служащих, привлекаемых к работе в участковых комиссиях и в качестве наблюдателей, могут быть резко снижены.

Система «Гарант» должна предоставлять электоральные услуги территориям (организациям), проводящим электоральные мероприятия, выполняя при этом роль «третьей доверенной стороны» [4]. Для оформления заказа потребитель должен ввести электронные списки избирателей и объектов кастинга, а также сведения о мероприятии. С процедурами заказа и сопровождения мероприятия можно ознакомиться на Веб-портале: [5]. 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 on-line процедур в сети. Технология «скрытной» персонализации, впервые предложенная и апробированная авторами в системе ЭГ «Сайлау», используемой в Казахстане, в нынешнем варианте Веб-реализации 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. Наличие действующего макета Веб-портала позволяет разработчикам моделировать как процедуры сбора и верификации скрытно персонализированных данных, так и процедуры коллективного принятия сетевым сообществом решения о том, что отображаемые средствами Веб-портала итоги выборного мероприятия являются корректными и могут быть приняты. Результаты моделирования различных мероприятий с участием 200 000 виртуальных респондентов доступны на странице /demo/ Веб-портала [5]. Схема связей системы «Гарант» с субъектами мероприятия показана на рис.1.

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 EID_i — уникальный открытый 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.

Формально процедура проверки может быть описана следующим образом. Пусть в мероприятии могут участвовать N избирателей, для которых сгенерировано множество SID, которое можно

обозначить как $\boldsymbol{S} = \{S_1, S_2, \ldots, S_N\}$. Пусть $\boldsymbol{S'} \subseteq \boldsymbol{S}$ — множество SID, которое соответствует избирателям, зарегистрированным сервером аутентификации/регистрации. Тогда мощность множества $\boldsymbol{S'}$, обозначаемая N', удовлетворяет неравенству $N' \leq N$. Некоторые из зарегистрированных избирателей могут зарегистрироваться и не голосовать, поэтому множество голосов $\boldsymbol{V} = \{V_1, V_2, \ldots, V_{N''}\}$, зафиксированных сервером голосования, удовлетворят соотношению $N'' \leq N' \leq N$. Таким образом, обозначая номера объектов голосования числами от 1 до M, а число голосов, поданных в пользу каждого из них как $C_1, \ldots, C_M$, мы получим $C_1 + \ldots + C_M = N'' \leq N' \leq N$. После опубликования данных, собранных серверами аутентификации/регистрации и голосования, любой удаленный наблюдатель может проверить это соотношение, а также убедиться, что всякий SID из множества $\boldsymbol{S'}$ является валидным. Любой избиратель, сохранивший криптопароль доступа к серверу кастинга, располагает механизмом верификации голоса. Проверка возможна и путем обмена SMS-сообщениями.

Рис. 1. Схема взаимодействия системы «Гарант» с субъектами электорального мероприятия

Апробация предложенных технологий может быть проведена посредством экспериментов по удаленному мониторингу неофициальных мероприятий, проводимых отечественными или зарубежными

учебными заведениями, корпорациями, органами местного самоуправления или партиями. Возможны натурные демонстрации работы Веб-портала на выставках с участием посетителей в качестве респондентов.

Литература

1. Ablameyko, S. New e-voting technologies presenting a democratic alternative to mass riots / S. Ablameyko [N.Kalosha, S.Bratchenya, V.Lipen] // 9 th Eastern European e│Gov Days 2011, May 8-10, 2011 Ljubljana, Slovenia. –Proceedings of e│Gov Days 2011, Austrian Computer Society. – pp. 85-96.
2. Ablameyko, S. “The Guarantor”: a web-centric system for organization and remote monitoring of election events / S. Ablameyko [N.Kalosha, D.Lipen, V.Lipen] // Transforming Gowernment: People, Process and Policy. – Electronic citizen participation – state of the art. Volume 5. Number 1, 2011. – pp. 56-67.
3. Абламейко, С.В. Система мониторинга электоральных мероприятий “Гарант” / С.В. Абламейко [С.М.Братченя, Н.И.Калоша, В.Ю.Липень] // Развитие информатизации и государственной системы науч.-техн. информации (РИНТИ-2010): материалы IX Междунар. конф., Минск, 18 ноября 2010 г. / РИНТИ-2010 – Минск, 2010. – С. 69-77.
4. Абламейко, С.В. Обеспечение информационной безопасности в системе мониторинга электоральных мероприятий «Гарант» / С.В.Абламейко, В.Ю. Липень // Искусственный интеллект. Интеллектуальные системы ИИ-2010: материалы Междунар. науч.-техн. конф., пос. Кацивели, АР Крым, Украина, 20-24 сент. 2010 г. / Донецк: ИПИИ «Наука і освіта», 2010. – Т. 2. – С. 304-311.
5. http://e-vote.basnet.by/.