

ПЕРСПЕКТИВНЫЕ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

А. А. Кибкало, директор Центра программных разработок (ЦПР) ОАО «Интеллект Телеком», к.ф.-м.н., д.э.н., г. Саров; kibkalo@i-tc.ru

В. С. Ляпер, главный специалист Департамента технической стратегии ОАО «Интеллект Телеком», г. Москва

А. Г. Субботин, начальник отдела мультимедиа разработок ЦПР ОАО «Интеллект Телеком», г. Саров

В. В. Задорожный, старший программист отдела мультимедиа разработок ЦПР ОАО «Интеллект Телеком», г. Саров

Ключевые слова: электронное голосование, мобильное голосование, e-voting, m-voting, SIM-карта.

Стремительное развитие новых информационных технологий и использование их в науке, образовании, здравоохранении побуждает правительства, межгосударственные и международные организации активно внедрять эти технологии в практику государственного и политического управления. Одним из перспективных направлений в области современных информационных технологий является изучение возможностей систем электронного голосования, которые разрабатываются и внедряются сегодня во многих странах мира.

Основное препятствие для повсеместного перехода на электронное голосование — обеспечение безопасности этой процедуры. Безопасность схем современного электронного голосования должна на гарантированной основе реализовывать не противоречащие конституционным правам и свободам процедурные моменты и при этом обеспечивать необходимый уровень доверия к такой системе со стороны как избирателей, так и кандидатов, принимающих участие в голосовании. Критические замечания наблюдателей за регламентом и процедурой голосования являются дополнительным стимулом к применению научно-обоснованных решений [4].

В данной работе освещены современные подходы к построению системы электронного голосования, показаны потенциальные проблемы безопасности систем электронного голосования, а также приведено описание российского опыта создания систем электронного голосования и перспективы такого подхода.

Зарубежный опыт в создании систем электронного голосования.

В международной практике под термином «электронное голосование» понимается применение технологии получения и подсчета голосов избирателей, а также подведения итогов голосования с помощью любых электронных средств. Электронное голосование может проводиться на избирательном участке с использованием таких электронных технологий, как система оптического сканирования, автоматически считывающая информацию с бумажного бюллетеня, или система прямой записи через сенсорный экран. Самостоятельным видом электронного голосования является удаленное (дистанционное) голосование с использованием информационно-телекоммуникационной сети общего пользования Интернет (Интернет-голосование) или других каналов связи (например, телефонная линия), что дает возможность избирателю участвовать в голосовании независимо от места его нахождения. Это, в свою очередь, позволяет привлечь к избирательному процессу граждан, которые в силу тех или иных причин не могут принять непосредственного участия в выборах.

В российской практике в рамках законодательства о выборах — законе № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» определены порядок проведения голосования, а также термин «электронное голосование», а именно «*Электронное голосование — голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием комплекса средств автоматизации ГАС «Выборы».*

Сегодня в России, в связи с жесткими требованиями к процедуре голосования, определенной на законодательном уровне

не, все системы дистанционного электронного голосования называются системами дистанционного электронного опроса (ДЭО). Термин «опрос» не является жестко прописанным в законодательстве и предоставляет большую свободу толкования при его разработке.

Системы электронного голосования начали разрабатываться, главным образом, для выборов в местные, либо национальные органы власти. Однако любая система электронного голосования, благодаря своей очевидной гибкости, может быть адаптирована под различные нужды, не связанные с выборами в органы власти. Везде, где нужен быстрый опрос среди широкой аудитории, технология ДЭО позволяет решить эту задачу быстро и эффективно. Речь здесь идет и о мониторинге общественного мнения на всех уровнях, и об опросах на различных выставках и конференциях, когда агрегирование общего результата будет занимать считанные секунды и результаты можно будет получать, практически, в режиме онлайн. Стоит заметить, что наиболее функционально-законченные системы электронного голосования разрабатываются все же для выборов в органы власти, а также для функционирования этих органов.

В настоящее время системы электронного голосования разработаны и внедрены во многих странах мира, еще больше стран ведут исследования по вопросам перехода на электронное голосование при выборах в местные и национальные органы власти. Среди них — Франция, Нидерланды, Швейцария, Бельгия, Италия, Норвегия, Португалия, Германия, Индия, Австралия, США, Россия и др.

В Эстонии, например, с 28 мая по 3 июня 2009 г. можно было принять участие в электронном голосовании на выборах в Европарламент. Это был первый опыт электронного голосования на выборах в Европарламент среди стран членов Европейского союза. Для участия в электронном голосовании необходимо было зайти через персональный компьютер на официальный сайт электронного голосования, ввести в электронное считывающее устройство электронную карточку, удостоверяющую личность, и PIN-код и проголосовать за своего кандидата. Стоит отметить, что около 10% проголосовавших воспользовались системой электронного голосования.

Признанным лидером в проведении электронного голосования на избирательных участках считается Бельгия — программа электронного голосования здесь действует с 1999 г., и этой возможностью пользуется около половины всех приходящих на участки избирателей.

Информационная безопасность как элемент доверия к системе электронного голосования. Несмотря на положительный опыт в проведении электронного голосования, многие страны откладывают переход на системы подобного рода. Так, например, в Великобритании в 2002—2003 гг. проводились масштабные тесты систем электронного голосования. В 2002 г. в ряде районов разрешено голосование в Интернете (с домашних компьютеров) и с мобильных телефонов (посредством SMS-сообщений). По результатам этих экспериментов система электронного дистанционного голосования подверглась серьезной критике. Основные аргументы ее противников — ненадежность систем дистанционного голосования и большая вероятность мошенничества. Аналогично с большой долей осторожности к электронному голосованию подходят и в США. По мнению американских экспертов, подобные системы открывают широкие возможности для мошенничества и злоупотреблений.

Как уже было отмечено, системы электронного и дистанционного голосования не внедряются повсеместно, в первую очередь, из-за недоверия к системам подобного класса. Причем это недоверие идет как от рядовых избирателей, которые хотят получить гарантию, что их голос учтен и учтен корректно,

так и со стороны кандидатов на выборах, которым важна достоверность процедуры подсчета голосов избирателей и отсутствие возможностей для нечестных манипуляций. Достаточно сложной проблемой при использовании систем электронного голосования является также необходимость сохранения тайны голосования, например в соответствии с требованиями законодательства. Система электронного голосования, как и любая другая автоматизированная система, в высшей мере подвержена влиянию угроз информационной безопасности, а с учетом критичности данных, обрабатываемых в этой системе, решение вопросов обеспечения информационной безопасности может создать необходимый уровень доверия, нужный для дальнейшего продвижения технологии ДЭО.

С точки зрения информационной безопасности необходимо обеспечить прозрачность и защищенность процедуры электронного голосования на всем временном интервале ее функционирования в соответствии с регламентом — от предоставления приложения для голосования пользователю до подсчета и опубликования результатов.

Часть задач информационной безопасности системы электронного голосования может быть решена с использованием стандартных средств, например защита от вирусов, несанкционированного доступа, либо DoS-атак. Однако обеспечение достоверности результатов голосования на уровне приложения является комплексной наукоемкой задачей, в состав которой входят следующие подзадачи [3]:

- установление строгой взаимной аутентификации голосующего и сервера голосования;
- разработка надежной процедуры подписи и верификации приложения для голосования и электронного бюллетеня, исключающей возможность их подмены злоумышленником, (при использовании для голосования таких личных пользовательских терминалов, как мобильный телефон, персональный компьютер и др.)
- защита с помощью надежного контейнера всего ключевого материала, используемого в процедуре электронного голосования, чтобы исключить возможность злоумышленника проголосовать за кого-либо другого;
- выполнение необходимых криптографических операций на производительном криптографическом устройстве, исключающем доступ к нему извне.



Рис. 1

Для решения задач информационной безопасности в системах электронного голосования требуется внедрение пользовательского устройства, выполняющего роль аутентификатора, хранилища ключей и криптопроцессора.

В качестве таких устройств в большинстве современных систем электронного голосования используются смарт-карты [1, 2] (рис. 1). Преимущества смарт-карт очевидны — они универсальны с точки зрения терминала для голосования и могут быть использованы как в стационарном общественном терминале, так и на домашнем компьютере или в мобильном телефоне. Кроме того, смарт-карты позволяют защищенно хранить ключевой материал, используемый в процедуре электронного голосования для подписи и шифрования, а также производить криптографические операции.

Электронное голосование в России — мобильное голосование. Результатом аккумулирования мирового опыта в разработке систем электронного голосования и собственных технологических разработок, стала созданная компанией ОАО «Интеллект Телеком» первая в России система ДЭО с помощью мобильных телефонов — мобильное голосование.

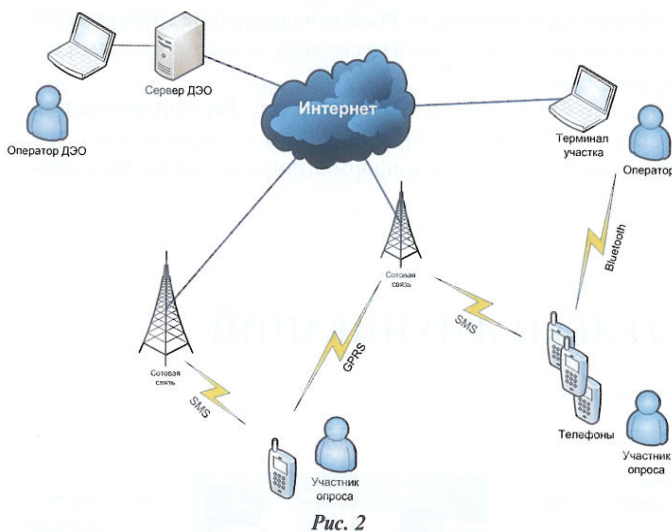


Рис. 2

Система была разработана по заказу Федерального центра информатизации при Центральной избирательной комиссии России для работы в первую очередь в удаленных от центра регионах России. Данная версия системы электронного голосования представляет собой систему, в которой пользователь может проголосовать на выборах с помощью своего собственного мобильного телефона, загрузив в него специализированное приложение.

Приложение для голосования передает данные в центр обработки результатов опроса по SMS-каналу в зашифрованном и подписанном виде, гарантируя тем самым достоверность результатов голосования и обеспечивая максимальный территориальный охват пользователей, за счет того, что услуга SMS предоставляется везде, где имеется сеть GSM, включая роуминг.

Архитектурно система содержит всего лишь несколько элементов (рис. 2). При этом, поскольку данные между мобильным телефоном и сервером передаются в зашифрованном виде, взаимодействие между этими функциональными элементами возможно по открытым каналам связи.

Система мобильного голосования работает по следующей схеме.

- Перед первым днем опроса избиратель получает у организаторов голосования свой PIN-код, с помощью которого он будет аутентифицирован в системе, и уникальную ссылку для

скачивания приложения, либо производит скачивание приложения непосредственно при получении у организаторов PIN-кода.

- В день проведения опроса участник запускает приложение и вводит PIN-код, после чего разрешает отправку SMS о готовности к опросу. В качестве ответа участник получает доступ к электронному бюллетеню с формой опроса, корректность этого бюллетеня гарантируется приложением.

- Участник делает выбор, разрешает отправку SMS, содержащего зашифрованное значение его выбора на сервер ДЭО, после чего получает сообщение, что его голос успешно учтен.

При этом от участника опроса не требуется никаких специфических навыков и знаний. Все указанные действия производятся быстро, интерфейс приложения интуитивно понятен.

С точки зрения организаторов опроса система также проста и удобна в использовании. Перед проведением опроса организаторы с использованием автоматизированных инструментов готовят необходимое количество копий приложения для голосования и PIN-кодов, выдают участникам PIN-коды и ссылки на приложение. Система голосования позволяет организаторам в любой момент посмотреть, в соответствии с законодательством, актуальные данные по проголосовавшим, а также собрать необходимую статистику. Итоги голосования подводятся в автоматическом режиме.

Система мобильного голосования доказала свою работоспособность при проведении ЦИК России эксперимента по дистанционному опросу в ЗАТО г. Радужный Владимирской области в единый день голосования 1 марта 2009 г. По результатам эксперимента система была признана удобной, в том числе пользователями, которые охотно голосовали с общественного терминала. Около 5% проголосовавших воспользовались личными мобильными телефонами. Всего же системой воспользовались более 40% от общего числа избирателей, пришедших на участки. Один из недавних примеров использования системы электронного голосования — эксперимент по дистанционному опросу на выборах в муниципальные органы власти 11 октября 2009 г. в г. Кингисепп Ленинградской области. Системой воспользовались около половины пришедших на участки избирателей.

В заключение, стоит отметить, что системы электронного голосования продолжают совершенствоваться, предоставляя пользователям все более высокий уровень защищенности, давая возможность взаимодействовать по любому доступному каналу связи и с использованием любой платформы. Голосование посредством мобильного телефона может также стать перспективной дополнительной услугой (VAS), либо услугой для корпоративного сектора.

ЛИТЕРАТУРА

1. Voting using Java Card smart cards (a case study) Martijn Oostdijk (joint work with C-B. Breunese & B. Jacobs) University of Nijmegen <http://www-sop.inria.fr/lemme/verificard/2002/slides/oostdijk.pdf>
2. Use of Java Cards in a telematic voting system Justo Carracedo Gallardo, Ana Gomez Oliva, Emilia Perez Belleboni, Jesus Moreno Blazquez, Sergio Sanchez Garcia Universidad Politicnica de Madrid, Espana EUITT. Telecomunicacion <http://vototelematico.diatel.upm.es/articulos/JavaCardsinVotingSystem.pdf>
3. Cryptographic Methods for Storing Ballots on a Voting Machine John Bethencourt, Carnegie Mellon University, Dan Boneh, Stanford University, Brent Waters SRI International <http://www.cs.berkeley.edu/~bethenco/ndss07.pdf>
4. Центральная Избирательная Комиссия Российской Федерации «Дистанционное электронное голосование: российские и зарубежные исследования», 2008, http://www.cikrf.ru/actual/elektr_oprosov/2glava.pdf.

Получено 07.12.09