ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ И СЕТИ

УДК 004.7

ПРИМЕНЕНИЕ ПРОТОКОЛА СЛЕПОЙ ПОДПИСИ ДЛЯ ПРОВЕДЕНИЯ ТАЙНОГО ГОЛОСОВАНИЯ

С.А. Македонский, В.С. Лукьянов

Интенсивное развитие государственных информационных систем создает условия для разработки и внедрения современных информационных средств, позволяющих автоматизировать и тем самым более эффективно реализовывать программы федеральных, региональных, отраслевых и межведомственных уровней. Одним из примеров таких программ, которые можно автоматизировать, являются проводимые периодически государственные выборы, например президентские выборы. Создание системы электронного голосования, которая позволила бы автоматизировать процесс выборов, существенно сократило бы расходы на выборы, повысило бы скорость и уменьшило вероятность ошибок в подсчете голосов.

Ключевые слова: *электронное голосование, электронные выборы, тайное электронное голосование, протокол слепой подписи.*

Key words: *electronic voting, electronic election, secret electronic voting, blind signature protocol.*

В случае перехода к какой-либо системе электронного голосования необходимо потребовать, чтобы такая система удовлетворяла ряду требований, выполнение которых необходимо для соблюдения действующего законодательства и пресечения возможностей фальсификации результатов и срыва выборов. К таким требованиям относятся:

1) голосовать имеют право только уполномоченные избиратели;
2) ни один из голосующих не может отдать более одного голоса;
3) ни один из участников процесса не может узнать, как проголосовал кто-то другой;
4) никто не может продублировать голос какого-то другого участника выборов;
5) конечный результат будет корректно подсчитан;
6) каждый из участников способен проверить, что результат подсчитан правильно;
7) протокол будет работать и в случае, когда некоторые из его участников нечестны [3, с. 347–348].

В Эстонии с осени 2005 г. муниципальные выборы проводятся через интернет, в Казахстане система электронного голосования «Сайлау», закупленная в Белоруссии, впервые испытывалась на 10 % избирательных участков на выборах депутатов в 2004 г. и с тех пор активно внедряется по всей республике. Внедряемые в России в рамках проекта «ГАС Выборы» двумерные считыватели заполненных бюллетеней КОИБ автоматизируют лишь процедуру подсчета результатов по участку и имеют высокую стоимость (около 70,0 тыс. руб.). 12 октября 2008 г. по инициативе Тульской областной избирательной комиссии, поддержанной Центральной избирательной комиссией (ЦИК) России, в порядке эксперимента было проведено электронное голосование, для которого использовались возможности интернет-сети. Для того чтобы принять участие в электронном голосовании, избирателю необходимо было получить специальный диск электронного опроса и воспользоваться любым компьютером с выходом в

интернет. Этой системой воспользовалось 5,4 % от общего количества граждан, принявших участие в выборах. Позже этот эксперимент был повторен 1 марта 2009 г. в Вологодской, Волгоградской и Томской областях, а также 11 октября 2009 г. в городе Кингисепп Ленинградской области. К возможности проголосовать с использованием диска электронного опроса добавились технологии голосования с использованием мобильного телефона и электронной социальной карты. Однако эти технологии не подходят, например, для выборов всероссийского масштаба, в первую очередь, потому, что задачей экспериментов являлось, прежде всего, изучение отношения избирателей к новым формам голосования, и поэтому выполнение перечисленных выше требований было далеко не самым важным. Таким образом, в России нет разработанной и готовой для внедрения системы электронного голосования, позволяющей осуществлять подачу голоса и его подсчет в электронном виде. Однако в опубликованном отчете о результатах проведения экспериментов обозначено, что российские избиратели очень активно поддержали идею проведения выборов в электронной форме, что говорит о перспективности разработок по данному направлению [1, 2, 4].

Рассмотрим требование 3: «Ни один из участников процесса не может узнать, как проголосовал кто-то другой». Если проводить выборы, используя средства компьютерных сетей, то в этом случае предъявляемое к используемой в этом процессе системе требование соблюдения тайны голосования будет одним из самых важных и труднореализуемых. Иными словами, никто из участников не должен иметь возможность узнать, как проголосовал любой из участников выборов. Для того, чтобы система, используемая при проведении выборов, удовлетворяла этому требованию, авторами статьи предлагается использовать протокол слепой подписи. В отличие от привычных цифровых подписей, важным свойством которых является знание подписывающим содержания подписываемого документа, в протоколах слепой подписи подписывающий не знает содержания подписываемого документа. Эту особенность протоколов слепой подписи и можно использовать для того, чтобы соблюсти требование тайны голосования.

Если провести аналогию между голосованием с использованием бумажных бюллетеней и электронным голосованием, то можно для электронного голосования использовать идею раздачи бюллетеней, используя которые участник голосования и будет подавать свой голос. Только в случае электронного голосования и бюллетени должны быть в электронном виде. При этом раздающий бюллетени не должен знать, кому и какой бюллетень им был выдан, чтобы в дальнейшем не было возможности связать его с участником голосования. Поэтому для соблюдения тайны голосования нужно каким-то образом выдать бюллетень избирателю, причем сделать это так, чтобы он был уверен в том, что раздающий бюллетени не знает, кому какой бюллетень он выдал. Для этих целей и может быть использован протокол слепой подписи.

Допустим, избиратель хочет получить бюллетень для проведения голосования. Для этого применяя протокол слепой подписи, можно действовать по следующему плану [5].

1. Избиратель формирует бюллетень в виде электронного документа. Для того, чтобы он был уникальным, ему присваивается некоторый идентификатор, достаточно большой, чтобы считаться уникальным.

2. Избиратель умножает полученный бюллетень на некоторое случайное число. Это случайное число называется маскирующим множителем.

3. Избиратель посылает замаскированный бюллетень организаторам выборов. Организаторы подписывают замаскированный документ.

4. Избиратель получает подписанный документ, удаляет маскирующий множитель и получает оригинальный бюллетень, подписанный организаторами.

Этот протокол работает только, если функции подписи и умножения на маскирующий множитель коммутативны.

В случае если маскирующий множитель действительно случаен и делает замаскированный документ действительно случайным, то организаторы выборов не могут получить никакую информацию о том, что подписывают.

Этот протокол обладает следующими свойствами.

1. Подпись организаторов выборов на бюллетене правильна и служит доказательством того, что этот бюллетень был действительно выдан организаторами, т.е. фактически они дали разрешение на участие в выборах конкретному лицу, получившему этот бюллетень. Подпись убедит организаторов в том, что именно они дали какому-то лицу разрешение на участие в выборах.

2. Организаторы не могут связать подписанный бюллетень с полученными ранее замаскированными бюллетенями. Даже хранение у организаторов информации обо всех выданных ими бюллетенях не поможет им определить, когда он подписал конкретный замаскированный бюллетень и от кого он был получен.

Для реализации подобной идеи можно использовать, например, алгоритм RSA.

Допустим, у организаторов есть открытый ключ e, закрытый ключ d и открытый модуль n. Избиратель хочет, чтобы организаторы подписали его бюллетень и при этом в дальнейшем не могли связать этот бюллетень с ним. Пусть m – это бюллетень. Тогда последовательность действий будет следующей.

1. Избиратель выбирает случайное число k из диапазона от 1 до n. Затем он маскирует бюллетень m, вычисляя $t = mk^e \pmod n$.

2. Организаторы подписывают t, вычисляя $t^d = (mk^e)^d \pmod n$.

3. Избиратель снимает маскировку с t^d, вычисляя $s = t^d/k \pmod n$.

4. Подписанным документом является s, так как $s = m^d \pmod n$. Это можно легко показать: $t^d \equiv (mk^e)^d \equiv m^d k \pmod n$, поэтому $t^d/k = m^d k/k \equiv m^d \pmod n$.

Пусть, например, $e = 37$, $d = 13$, $n = 77$. Возьмем бюллетень $m = 31$, где последняя цифра числа – вариант выбора в проходящем голосовании, а первая цифра – уникальный идентификатор бюллетеня. Для примера возьмем маскирующий множитель $k = 12$. Далее проводим вычисления в соответствии с изложенной выше последовательностью действий.

1. Вычисляем замаскированный бюллетень $t = mk^e \pmod n = 31*12^{37} \pmod{77} = 64$.

2. Организаторы подписывают замаскированный бюллетень, вычисляя $t^d \pmod n = 64^{13} \pmod{77} = 36$.

3. Избиратель снимает маскировку с t^d, вычисляя $s = t^d/k \pmod n = 36/12 \pmod{77} = 3$. Число *3* и есть подпись бюллетеня $m = 31$.

Если вычислить $m^d \pmod n$, т.е. если бы подпись ставили на незамаскированном бюллетене, то получили бы $31^{13} \pmod{77} = 3$. Подпись на замаскированном бюллетене совпадает с подписью на незамаскированном и, следовательно, является верной.

В результате мы получаем протокол, который позволяет раздавать бюллетени избирателям, при этом не нарушает принцип тайны голосования. Стойкость протокола от взлома зависит от стойкости выбранной криптографической функции и случайности выбранных для реализации протокола элементов – открытых и закрытых ключей, а также маскирующего множителя.

Однако, если использовать протокол слепой подписи в представленном виде, может случиться ситуация, когда организаторы подписали бюллетень, содержащий ошибку. Например, из-за плохой связи изменился один бит замаскированного сообщения, либо избиратель специально отправил бюллетень с ошибкой, чтобы потом обвинить организаторов в попытке сорвать выборы. В результате избиратель не сможет воспользоваться этим бюллетенем, потому что организаторы, получившие ошибочный бюллетень, не могут быть уверены, что голосующий отправляя бюллетень, содержащий ошибку, не пытается смошенничать.

Для того, чтобы избежать подобных ситуаций, организатор должен быть уверен в правильности формата подписываемого бюллетеня.

Чтобы обеспечить это, можно поступить следующим образом [5].

1. Избиратель готовит n бюллетеней, в каждом из которых различные идентификаторы и для маскировки каждого из них используется свой маскирующий множитель.

2. Избиратель отправляет замаскированные бюллетени организаторам выборов. Организаторы выбирают n-1 бюллетень и просят прислать маскирующие множители для этих бюллетеней.

3. Избиратель отправляет маскирующие множители, и организаторы открывают замаскированные бюллетени, убеждаясь, что они сформированы правильно.

4. Организаторы выборов подписывают оставшийся нераскрытым бюллетень и отправляют его избирателю.

5. Избиратель снимает маскировку и получает бюллетень, подписанный организаторами выборов.

Теперь вероятность того, что организатор подпишет неправильно сформированный бюллетень, равна $1/n$. Изменяя значение n можно свести к минимуму вероятность подписания ошибочного бюллетеня.

Представленный протокол является вариантом интерактивного протокола доказательства с нулевым разглашением. Используя этот протокол доказывающий убеждает проверяющего в том, что переданная им информация (бюллетень в нашем случае) верна, при этом не раскрывая самой информации. Однако он может быть и неинтерактивным, – это протокол, не требующий в своей работе непосредственно взаимодействия участвующих в нем сторон. Например, вместо того чтобы организаторы выбирали наборы, которые избиратель должен раскрыть, избиратель может использовать однонаправленную хэш-функцию от всего опубликованного набора для определения тех наборов, которые надо раскрыть, т.е. избиратель вычисляет хэш-функцию от публикуемого им набора бюллетеней и на основе нее раскрывает n-1 публикуемых бюллетеней. Идея здесь состоит в том, что доказывающий не может угадать значение хэш-функции перед тем, как открывать наборы значений, поскольку для этого нужно было бы инвертировать хэш-функцию.

Таким образом, используя описанный способ, можно распределять избирательные бюллетени между избирателями, при этом гарантируя анонимность избирателя и тем самым обеспечивая требование соблюдения тайны голосования. На данный момент слепые подписи широко используются при осуществлении платежей в электронной форме, т.е. механизм слепых подписей широко изучен и опробован. Авторы предлагают использовать описанную схему в разработке протокола электронного голосования.

Библиографический список

1. Механизм народовластия / Национальная избирательная комиссия Эстонии – Обзор Системы электронного голосования. – Режим доступа: http://mexnap.info/index.php, свободный. – Заглавие с экрана. – Яз. рус.

2. Результаты апробирования технологий и систем электронного голосования / Национальная академия наук Беларуси, Объединенный институт проблем информатики ; В. Ю. Липень, М. А. Воронецкий, Д. В. Липень. – Режим доступа: http://uiip.bas-net.by, свободный. – Заглавие с экрана. – Яз. рус.

3. Смарт, Н. Мир программирования. Криптография / Н. Смарт. – М. : Техносфера, 2005.

4. Экспериментальный электронный опрос избирателей с использованием сети интернет / Центральная избирательная комиссия России. – Режим доступа: http://www.cikrf.ru, свободный. – Заглавие с экрана. – Яз. рус.

5. Шнайер, Б. Прикладная криптография / Б. Шнайер. – 2-е изд. – М. : Триумф, 2002.