УДК 004.056(075)
Н 82

АНАЛИЗ СРЕДСТВ И МЕТОДОВ РЕАЛИЗАЦИИ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

В. В. Норик, магистрант;
И. В. Устенко, доц., канд. техн. наук

Национальный университет кораблестроения, г. Николаев

Аннотация. Описана методика реализации системы проведения электронного голосования с использованием современных средств защиты информации.

Ключевые слова: электронная подпись, шифрование, устойчивость.

Анотація. Описана методика реалізації системи проведення електронного голосування з використанням сучасних засобів захисту інформації.

Ключові слова: електронний підпис, шифрування, стійкість.

Abstract. The procedure of the electronic voting system realization using modern information safety measures is described.

Keywords: electronic signature, encryption, durability.

ПОСТАНОВКА ПРОБЛЕМЫ

Для участия в выборах или дискуссиях, для принятия коллегиальных решений в современном мире все чаще прибегают к системе электронного голосования. Главными достоинствами электронных выборов являются мобильность, возможность контроля подсчета голосов, скорость проведения голосования и обработки данных. Однако возникает и ряд проблем, основные из которых — обеспечение анонимности, конфиденциальности и защиты от фальсификаций. Решить перечисленные проблемы можно, используя криптографические методы защиты информации.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ

Рассматривая последние исследования и публикации, следует отметить большую заинтересованность стран Европы, США и России во внедрении надежной системы электронных выборов. Анализ подобных публикаций [1–4] позволил сделать вывод, что проблема обеспечения информационной безопасности электронного голосования весьма актуальна и важна в современном мире.

ЦЕЛЬ СТАТЬИ — анализ основных криптографических алгоритмов для дальнейшего использования выборов схемы при реализации электронного голосования, отвечающей разработанным требованиям.

ИЗЛОЖЕНИЕ ОСНОВНОГО МАТЕРИАЛА

Проанализировав основные подходы к реализации электронного голосования, можно сформулировать требования к схеме выборов:

анонимность;
контроль над избирателями;
индивидуальный контроль;
универсальный контроль;

устойчивость;

неподтверждаемость;

невозможность голосования за другого человека;

невозможность узнать промежуточные результаты.

Существуют различные механизмы, обеспечивающие удовлетворение указанных требований. Проведя анализ, остановимся на тех, которые в наибольшей мере решают эту проблему.

Для обеспечения анонимности целесообразно использовать «слепую» цифровую подпись как разновидность электронной цифровой подписи, особенностью которой является то, что подписывающая сторона не может точно знать содержимое подписываемого документа. При необходимости можно проверить, принадлежит ли подпись именно тому человеку, который об этом заявляет; поставлена ли подпись именно на этот документ (т. е. в документ не были внесены изменения или не был подложен другой документ).

Реализацию алгоритма «слепой» подписи можно осуществить с помощью асимметричных алгоритмов (RSA, DSA) [1, 4], так как, в отличие от блочных алгоритмов (DES, 3DES), в них отсутствует потребность в хранении и распределении ключей.

Анализ алгоритмов показал, что по быстродействию система DSA сравнима с RSA при формировании подписи, но существенно (в 10…40 раз) уступает ей при проверке подписи, что отображено в таблице. Поэтому алгоритм «слепой» цифровой подписи целесообразно реализовать, используя алгоритм RSA.

Algorithm	Key Generation* 1 (ms.)	Sign* 100 (ms.)	Verify*100 (ms.)
RSA 512	544.61	915	160
RSA 1024	1120.46	4188	263
DSA 512	6.62	634	988
DSA 1024	17.87	1775	3397

Рассмотрим схему, основанную на этом алгоритме. Избирателю (стороне А) нужно отправить серверу-распределителю (стороне В) ответ — свой голос (M′), подтвержденный цифровой подписью (рис. 1).

Алгоритм «слепой» электронной подписи:

1. Взять открытый текст M'.

2. Создать цифровую подпись σ с помощью своего секретного ключа (d, n) по формуле

$$\sigma = S_A(M') = M'^{d} \bmod n. \qquad (1)$$

3. Передать пару (M', σ), состоящую из сообщения и подписи.

4. Принять пару (M', σ).

5. Взять открытый ключ (e, n) стороны A.

6. Проверить подлинность подписи:

$$P_A(\sigma) = \sigma^{e} \bmod n \equiv M' \rightarrow \text{подпись верная.} \qquad (2)$$

Важное свойство цифровой подписи заключается в том, что ее может проверить каждый, кто имеет доступ к открытому ключу ее автора.

Так как исходное сообщение M' передается в открытом виде, то его нужно зашифровать, используя RSA (рис. 2) [2].

Алгоритм RSA :

1. Взять открытый ключ (e, n) стороны A.

2. Взять открытый текст M.

3. Передать шифрованное сообщение

$$P_A(M) = M^{e} \bmod n.$$

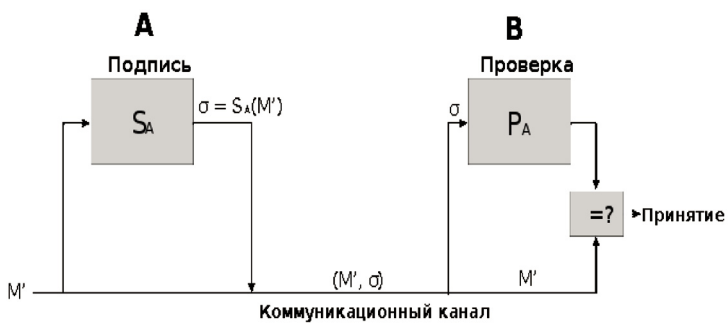

Рис. 1. Схема «слепой» электронной подписи

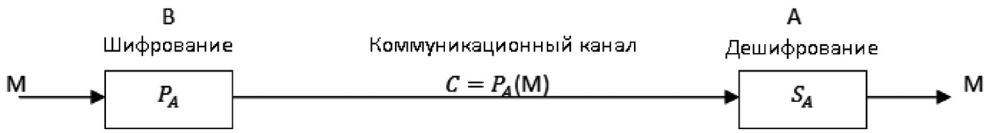

Рис. 2. Схема шифрования алгоритмом RSA

4. Принять зашифрованное сообщение C.

5. Применить свой секретный ключ (d, n) для расшифровки сообщения

$$S_A(C) = C^d \ mod \ n.$$

Сообщением являются целые числа, лежащие в диапазоне от 0 до $n - 1$, т. е.

$$M \in D = Z^n.$$

Уравнения (1) и (2), на которых основана схема RSA, определяют взаимно обратные преобразования.

Для обеспечения тайны голосования можно использовать несколько разных подходов. Первый заключается в том, что все видят голос, но никто не знает, чей он. Еще одним подходом может быть такой: все знают, кому принадлежит данный выбор, но никто не может его расшифровать.

При первом подходе в качестве инструмента для обеспечения тайны голосования выступает использование анонимного канала. Для решения проблемы контроля за избирателями (контроль над тем, кто пытается проголосовать два раза) целесообразно использовать специальные сообщения — псевдонимы.

Рис. 3. Алгоритм проведения электронных выборов

Во время первой фазы выборов избиратель, общаясь с организаторами, создает псевдоним. Он может создать лишь один псевдоним. Организаторы не знают псевдонимы избирателей. Они могут проконтролировать избирателей, составив список участвующих в выборах псевдонимов. Во второй фазе происходит голосование. Избиратель посылает по анонимному каналу пару, состоящую из псевдонима и голоса. Организаторы, суммируя соответствующие корректным псевдонимам голоса, могут проконтролировать, сколько различных избирателей приняло участие в выборах. Избиратель, в свою очередь, может проконтролировать, что его пара была включена в список.

При втором подходе для получения шифротекста всех бюллетней можно использовать гомоморфное шифрование. Расшифровав этот объединенный шифротекст, получают сумму всех голосов:

$$F(E(x_1),E(x_2),...,E(x_n)) = \mathrm{E}(x_1 + x_2 + ... + x_n).$$

Применение этого подхода предполагает абсолютную честность независимых организаторов выборов. Поскольку опираться на это нецелесообразно, для обеспечения тайны голосования остановимся на первом подходе.

Проанализировав все сказанное, можно составить алгоритм проведения электронных выборов (рис. 3).

ВЫВОД

Использование предложенного алгоритма позволит удовлетворить следующие требования, предъявляемые к проведению электронного голосования: контроль над избирателями; тайна голоса; индивидуальный контроль; невозможность узнать промежуточные результаты. Для проверки, имеет ли избиратель право голоса, он должен предъявить раздающему свою электронную подпись (аналог паспорта).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

[1] *Гундарь, К. Ю.* Защита информации в компьютерных систе-мах [Текст] / К. Ю. Гундарь. — К. : Корнийчук, 2000. – 151 с.

[2] *Иванов, М. А.* Криптографические методы защиты информации в компьютерных системах и сетях [Текст] / М. А. Иванов. — М. : КУДИЦ-ОБРАЗ, 2001. — 368 с.

[3] *Лифшиц, Ю. А.* Электронные выборы [эл. изд.] / Ю. А. Лифшиц. – http://yury.name/crypto/03cryptonote.pdf.

[4] *Мао, В.* Современная криптография [Текст] / В. Мао. — М. : Вильямс, 2005. — 763 с.