А. В. Жарков (Ульяновск, УлГУ)**. Реализация криптографического протокола электронного голосования.**

Любой приемлемый протокол on-line голосования должен обладать следующими свойствами: голосовать могут только те, кто имеет на это право; голосование происходит анонимно; никто не может узнать, за кого проголосовал конкретный избиратель (тайность); никто не может тайно изменить чей-то голос; каждый голосующий может проверить, что его голос учитывался при подведении итогов голосования. Разумеется, в каких-то случаях могут потребоваться и иные свойства. Несмотря на то, что эти требования противоречивы, использование двухключевой асимметричной криптографии позволяет составить подходящую реализацию. Опишем систему электронного голосования, разработанную в Ульяновском госуниверситете.

За основу реализации взята криптосистема RSA, основанная на трудности разложения большого натурального числа на два простых множителя. В нашем случае используются числа N, состоящие из 256 бит (75 десятичных цифр), что обеспечивает приемлемую криптостойкость. Центр голосования объявляет дату, анкету с вопросами и список голосующих. Так как это конкретные студенты, то они либо уже имеют пару ключей (пусть это числа p и t, причем t — открытый ключ хранится в базе данных участников голосования, p — секретный ключ участника), либо могут получить ее в Центре. Центр генерирует собственную пару ключей: e — открытый, он выставляется на сайте Центра, и d — секретный ключ.

В основе протокола электронного голосования лежит известный протокол «слепой» подписи Чаума [1]. Первый шаг протокола — регистрация участника. Участник самостоятельно выбирает числа n и r (меньшие N), и вычисляет (с помощью специальной клиентской программы) число $q = H(n)r^e \pmod N$, где $H(n)$ — значение стандартной хэш-функции (в нашем случае RC5). Зайдя на сайт Центра голосования, участник под своей фамилией шифрует на своем открытом ключе некоторое специальное (открытое) число Центра и передает ему результат, а также число $q^p \pmod N$. Анонимности пока нет.

Центр восстанавливает собственное число, расшифровывая его на ключе t, (тем самым подтверждая право участника на голосование), и вычисляет число $z = q^{td} \pmod N$, где d — секретный ключ Центра. Число z передается участнику, который вычисляет число $s = zr^{-1} \pmod N$. С этого момента пара чисел $(n; s)$ является анонимным «открепительным талоном», дающим право на голосование.

Теперь участник, зайдя на сайт Центра, анонимно заполняет анкету с вопросами и передает результат вместе с парой чисел $(n; s)$. Центр проверяет подлинность талона, вычисляя, истинно ли равенство $H(n) = s^e \pmod N$. Если это так, то анкета заносится в базу данных результатов. Тайность голосования обеспечивается тем, что Центр не знает числа r, использовавшегося при подготовке талона.

СПИСОК ЛИТЕРАТУРЫ

1. *Молдовян Н.А., Молдовян А.А.* Введение в криптосистемы с открытым ключом. СПб.: БХВ–Петербург, 2005, 288 с.