Методы обеспечения целостности информации контрольная работа

ФИО преподавателя: А.Ю. Ермакова

Электронные торги

Рассмотрим, для примера, протокол организации электронных торгов.
Свойства ЭЦП:

«неподделываемость»

и

«неотказуемость»

Электронные торги

Как известно, любые торги организуются, по следующей схеме:

1) организатор торгов объявляет условия торгов, критерии определения победителей и срок приема заявок от участников;

2) участник торгов в установленный срок направляет организатору свою заявку с предложениями в соответствии с объявленными условиями;

Электронные торги

3) организатор торгов, закончив прием заявок от всех участников, сравнивает их предложения между собой и объявляет победите-ля, который предложил лучшие условия в соответствии с заранее объявленными в условиях торгов критериям

Электронные торги

Приведенный ниже протокол основан опять-таки на схеме RSA.

а) Организатор торгов создает стандартную схему RSA с открытым ключом (m, e) и закрытым ключом (m, d).

Открытый ключ публикуется, с тем чтобы он стал известен всем участникам торгов, закрытый ключ остается известен только организатору.

б) Каждый участник торгов V_i **(i=1, 2, …, N)** формирует свое исходное предложение s_i и направляет организатору зашифрованное предложение f_i, определяемое по формуле

$$f_i = (s_i)^e \bmod m.$$

в) Организатор торгов по истечении срока поступления заявок публикует реестр участников, принявших участие в торгах, и их зашифрованные предложения fi. Это нужно для того, чтобы каждый участник имел возможность проверить правильность получения организатором своего зашифрованного предложения и для возможности осуществления последующего контроля.

г) После публикации реестра зашифрованных предложений организатор осуществляет вычисление исходных заявок участников по формуле

$$s_i = (f_i)^d \bmod m,$$

публикует исходные заявки, сравнивает предложения участников
и объявляет победителя.

Замечание 1. Сравнивая приведенный протокол электронных торгов с протоколом ЭЦП, можно увидеть, что зашифрованные заявки — это фактически ЭЦП исходных заявок. Это позволяет перенести на протокол электронных торгов все результаты, относящиеся к ЭЦП, в частности, **«неподделываемость» и «неотказуемость».**

Замечание 2. Замена исходной заявки ее цифровой подписью является криптографическим аналогом упомянутого конверта, в который запечатывается исходная заявка с целью сохранения ее конфиденциальности.

Убедимся, что приведенный протокол решает все задачи организации торгов.

В самом деле:

— до момента подведения результатов сохраняется конфиденциальность исходных заявок участников, поскольку провести расшифровку опубликованных зашифрованных заявок можно только с использованием закрытого ключа, а он известен только организатору;

— после того как опубликован реестр зашифрованных заявок, в силу действия «принципа неотказуемости» невозможно даже по сговору с организатором подменить ни одну из исходных заявок таким образом, чтобы сохранить без изменения зашифрованную заявку;

— и наконец, после объявления победителя и публикации его исходной заявки любой участник торгов может осуществить проверку факта получения организатором именно этой заявки до начала процедуры подведения итогов торгов. Для этого он должен взять опубликованную исходную заявку победителя (обозначим ее $s_{r'}$), повторить процедуру шифрования, т. е. вычислить $f_{r'} = (s_{r'})^e \bmod m$, и сравнить с зашифрованной заявкой f_r из реестра, опубликованного организатором. Равенство $f_{r'} = f_r$ возможно только в случае $s_{r'} = s_r$, а это и будет означать, что организатор при подведении итогов рассматривал ту самую заявку, которую получил на первом этапе конкурса.

Литература

1. Ермакова А.Ю., Криптографические методы защиты информации.– М.: РТУ-МИРЭА, 2021. – 267 с.
2. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации.– М.: Юрайт, 2019. – 474 с.