УДК 681.324

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В СИСТЕМЕ ОРГАНИЗАЦИИ ТЕНДЕРНЫХ ТОРГОВ

Студент гр. 113024 Короткевич О.С.,
кандидат техн. наук, доцент В.А. Артамонов
Белорусский национальный технический университет

Создание системы электронных конкурсных торгов предполагает адекватную техническую реализацию правовых отношений между заказчиками и поставщиками товаров и услуг. Техническая реализация некоторых специфических моментов правовых отношений, основана на использовании инфраструктуры открытого ключа (PKI).

Защита информации в PKI (public key infrastructure) основана на методе асимметричного шифрования с использованием пары ключей: открытого и закрытого, и их использовании в механизме электронной цифровой подписи (ЭЦП). ЭЦП — это реквизит электронного документа, который с высокой степенью достоверности свидетельствует о неизменности подписанного документа, гарантирует его аутентичность и неотрекаемость от подписи.

Опираясь на специально созданный профиль защиты электронной тендерной площадки, учитывающий разнообразные предположения угрозы безопасности системы, была разработана защищенная электронная система организации конкурсных торгов. Система представляет собой связанную совокупность программных средств, в которую входят:

- интернет площадка проведения торгов (web-портал, размещенный в интернет и свободно доступный для использования);
- клиентское криптографическое приложение (программа, предназначенная для генерации ключевой информации и выполнения функций ассиметричного шифрования, создания и верификации цифровой подписи);
- система администрирования (web-приложение с ограниченным доступом, предназначенное для конфигурации и управления системой, выступающее в качестве удостоверяющего центра PKI).

Основной интерес представляет предлагаемая подсистема безопасности, построенная на основе архитектуры PKI и обеспечивающая информационную безопасность проведения торгов. Разработанная система является универсальной, т.е. реализует как технологию ЭЦП, так и конфиденциальную передачу информации, а так же имеет собственный способ генерации ключевой пары и включает свой набор криптоалгоритмов на основе RSA (ЭЦП и ассиметричное шифрование), MD5 (хэширование) и AES(Rijndael) (симметричное шифрование).