

Электронная цифровая подпись

Химичева О.В., Волосевич И.Н.

Научный руководитель - преподаватель Ковалькова И.А.

Белорусский национальный технический университет

Цель: определить цели применения электронной цифровой подписи в таможенных органах Республики Беларусь, а также ее преимущества и недостатки.

Электронная цифровая подпись (далее ЭЦП) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП.

ЭЦП предназначена для аутентификации лица, подписавшего электронный документ, а также позволяет осуществлять: контроль целостности передаваемых документов; защиту от изменений или подделки документа; доказательное подтверждение авторства документа.

ЭЦП строится на основе алгоритмов симметричного (зашифрование и расшифрование производится закрытым ключом) и асимметричного (зашифровывается закрытым ключом, а расшифровывается открытым ключом) шифрования.

В таможенных органах Республики Беларусь используется асимметричный алгоритм шифрования, поэтому основной проблемой является защита открытых ключей от подмены злоумышленником и организация отзыва ключа в случае его компрометации. В настоящее время защита ключей от подмены осуществляется с помощью сертификатов. Сертификат позволяет удостоверить заключенные в нем данные о владельце и его открытый ключ подписью какого-либо доверенного лица. Существуют две системы сертификатов: централизованные (используются центры сертификации) и децентрализованные (пользователем ключа строится «сеть доверия»).

В таможенных органах ЭЦП нашла свое применение в системе электронного декларирования, благодаря высокой степени надежности и легкости использования. ЭЦП – эффективность и практичность минус две проблемы сразу.