КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

ст. викладач А.І. Пасько, студенти О.С. Бакар, А.Д. Полянський,
Університет імені Альфреда Нобеля, м. Дніпропетровськ

Апаратно-програмні засоби криптографічного захисту інформації в СЕП забезпечують автентифікацію адресата та відправника міжбанківських електронних розрахункових документів і службових повідомлень СЕП, гарантують їх достовірність та цілісність у результаті неможливості підроблення або викривлення документів у шифрованому вигляді або за наявності ЕЦП.

Основною метою криптографічного захисту інформації є забезпечення конфіденційності та цілісності електронної банківської інформації, а також суворої автентифікації учасників СЕП і фахівців банківських установ, які беруть участь у підготовці та обробленні електронних банківських документів. Для забезпечення розв'язання завдань суворої автентифікації банківських установ, підключених до інформаційної мережі, розроблено систему ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту.

Для забезпечення захисту інформації від модифікації з одночасною суворою автентифікацією та безперервного захисту платіжної інформації з часу її формування система захисту СЕП та інших інформаційних задач включає механізми формування/перевірки ЕЦП на базі несиметричного алгоритму RSA. Для забезпечення роботи цього алгоритму кожна банківська установа отримує від служб захисту інформації територіальних управлінь персональний генератор ключів із вбудованим ідентифікатором цієї банківської установи. За допомогою цього генератора ключів банківська установа має змогу генерувати ключі для всіх робочих місць, які працюють з електронними банківськими документами. Для забезпечення захисту ключової інформації (а саме відкритих ключів) від викривлення та підроблення відкриті ключі ЕЦП мають надсилатися до служби захисту Інформації Національного банку для сертифікації (крім ключів для робочих місць операціоністів та інших, що використовуються лише в САБ).

Технологія накладання/перевірки ЕЦП у СЕП створена таким чином, щоб одна службова особа не мала змоги відіслати міжбанківський електронний розрахунковий документ. Під час формування міжбанківського електронного розрахункового документа на робочому місці операціоніста службова особа, яка формує цей документ, має накладати ЕЦП на документ за допомогою свого таємного ключа.