Про організацію захищеного електронного документообігу

Правилами зберігання, захисту, використання та розкриття банківської таємниці, затвердженими постановою Правління Національного банку України від 14.07.2006 № 267 (зі змінами), установлено вимоги, згідно з якими передавання інформації, що містить банківську таємницю, електронною поштою або в режимі онлайн здійснюється лише в захищеному (зашифрованому) вигляді з контролем цілісності та з обов'язковим наданням підтвердження про її надходження з електронним підписом отримувача з використанням засобів захисту.

З метою виконання зазначених вимог в інформаційних задачах Національного банку використовується АРМ-НБУ інформаційний.

Якщо банк підключається до інформаційної системи державного органу, у якій передбачено оброблення інформації з обмеженим доступом, то банк має право для передавання інформації, яка містить банківську таємницю, використовувати засоби захисту інформації зазначеної інформаційної системи.

В інших випадках банк самостійно визначає та узгоджує із стороною інформаційної взаємодії засоби захисту, що будуть використовуватись для захищеного обміну інформацією.

Окремо зазначимо, що Законом України "Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації" на законодавчому рівні визнається кваліфікована довірча послуга з видачі та обслуговування кваліфікованого сертифікату шифрування.

У зв'язку з цим Національний банк пропонує банкам розглянути як один з варіантів організації захищеного обміну інформацією, що містить банківську таємницю, можливість використання кваліфікованих сертифікатів шифрування в такому порядку:

1) контрагент у відкритій формі надсилає на офіційну електронну поштову скриньку банку запит на отримання інформації, підписаний кваліфікованим електронним підписом, а також додає свій кваліфікований сертифікат шифрування та адресу електронної пошти, на яку банк має відправити підтвердження про отримання запиту;

2) банк надсилає на визначену електронну поштову скриньку контрагента інформацію, що містить банківську таємницю, зашифровану з використанням кваліфікованого сертифіката шифрування контрагента та особистого ключа шифрування уповноваженої особи банку. До електронного листа із зашифрованою інформацією додається кваліфікований сертифікат шифрування уповноваженої особи банку;

3) контрагент розшифровує отриману інформацію після чого направляє банку підтвердження про її отримання, підписане кваліфікованим електронним підписом (без шифрування).

Що стосується обміну інформацією, яка містить таємницю надавача платіжних послуг, то вищезазначена технологія для передавання інформації від надавача платіжних послуг до державних органів уже визначена в пункті 29 Правил зберігання, захисту, використання та розкриття таємниці надавача платіжних послуг, затверджених постановою Правління Національного банку України від 14.07.2022 року № 147, де зазначено, що передавання такої інформації в електронній формі здійснюється шляхом її шифрування з використанням кваліфікованих сертифікатів шифрування та/або захищеними каналами зв’язку, що відповідають вимогам законодавства у сфері криптографічного та технічного захисту інформації та/або нормативно-правових актів Національного банку з питань інформаційної безпеки.

Аналогічний підхід до організації захищеного передавання інформації, що містить таємницю надавача платіжних послуг, застосовується в інших випадках.