УДК 336.711.008(477)

***І.Д. Горбенко**, д-р техн. наук, проф., **О.В. Потій**, канд. техн. наук, доц., ЗАТ "ІІТ"*

# КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО СТВОРЕННЯ, ВПРОВАДЖЕННЯ ТА ФУНКЦІОНУВАННЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

*Автор досліджує важливі концептуальні елементи створення інфраструктури відкритих ключів Національного банку України (ІВК НБУ): мету і завдання створення, основні завдання та вимоги до ІВК, структуру і основні завдання засвідчувального центру НБУ.*

*Ключові слова: інфраструктура відкритих ключів НБУ, цілісність інформації, електронний цифровий підпис, засвідчувальний центр НБУ.*

**Постановка проблеми**. На сьогоднішній день актуальною є проблема створення, впровадження, безпечного та надійного функціонування інфраструктури відкритих ключів Національного банку України (ІВК НБУ). Першочерговим завданням ІВК НБУ є надання банківським та фінансовим установам, органам державної влади, місцевого самоврядування, юридичним та фізичним особам послуг із забезпечення цілісності і справжності інформації та різноманітних даних, що представлені в електронному вигляді, електронних документів та повідомлень, програмного забезпечення, що ними використовуються.

**Виклад основного матеріалу.** Відповідно до існуючих міжнародних норм та вимог усім користувачам мають надаватися послуги з забезпечення цілісності та справжності інформації, а в деяких випадках також і конфіденційності, на всіх етапах її життєвого циклу, тобто при обробці. Під обробкою інформації розуміється виконання однієї або декількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрування, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних та/або програмних засобів.

Одним із основних та комплексних засобів забезпечення надання вказаних послуг є застосування електронного цифрового підпису (ЕЦП). На світовому рівні та в усіх технологічно розвинутих державах застосування цифрового підпису під час обробки інформації є усталеною практикою. Для розв'язання цих завдань у технологічно розвинутих державах створені інфраструктури відкритих ключів. Україна зробила в цьому напрямку ряд дуже важливих кроків. Прийнято закони "Про електронні документи та електронний документообіг", "Про електронний цифровий підпис", ряд постанов Кабінету Міністрів та наказів ДСТСЗІ СБ України. Крім того, введено у дію національний стандарт України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002). У даній статті наведений концептуальний підхід до побудови ІВК НБУ.

*Мета та завдання створення інфраструктури відкритих ключів НБУ*

Головною метою ІВК НБУ є надання фізичним та юридичним особам, банківським та фінансовим установам, органам місцевого самоврядування та іншим суб'єктам послуг щодо забезпечення цілісності та справжності інформації, документів, повідомлень та програмного забезпечення, які представлені в електронному вигляді та використовуються суб'єктами на усіх етапах життєвого циклу за допомогою використання сертифікатів відкритих ключів. Використання сертифікатів відкритих ключів забезпечує надійний зв'язок відкритих ключів з користувачами, дозволяє іншим користувачам перевірити наявність цього зв'язку та одержати необхідні послуги з управління ключовими даними. У рамках ІВК НБУ забезпечується підтвердження цілісності інформації, що підписується особистим ключем користувача та ідентифікація підписувача (підтвердження справжності інформації, яка ним підписана). ІВК НБУ має інтегрувати сертифікати відкритих ключів, криптографічні перетворення з відкритими ключами та уповноважені на сертифікацію органи в єдину організаційно-технічну структуру.

Інтеграція ІВК НБУ, у тому числі систем ЕЦП, з інформаційно-телекомунікаційними системами банківських та фінансових установ дозволяє розв'язати такі завдання:

- реєстрація користувачів;
- реєстрація сертифікатів відкритих ключів користувачів;

- реалізація процедури обслуговування сертифікатів, тобто формування та засвідчення чинності відкритого ключа, видача (випуск), розповсюдження, скасування, блокування, поновлення, облік чинних сертифікатів, перевірка статусу сертифікатів та зберігання (архівування) сертифікатів;
- об'єднання сертифікатів відкритих ключів у спеціальні довідники сертифікатів та їх обслуговування;
- взаємодія з іншими уповноваженими органами системи ЕЦП, у тому числі з відповідними уповноваженими органами інших країн;
- надання інших додаткових послуг щодо управління ключовими даними та сертифікатами, в тому числі в частині асиметричного (направленого) шифрування та надання послуг з управління привілеями.

Впровадження послуг ЕЦП у банківську діяльність дозволить:

- впровадити новітні інформаційні технології електронного документообігу у практику повсякденної діяльності банківських установ усіх форм власності;
- розширити можливість інтеграції української банківської системи у міжнародну;
- підвищити конкурентоспроможність українських банків у цілому;
- забезпечити цілісність та справжність (автентичність) інформації, представленої в електронному вигляді, а також неспростовність (причетність) суб'єктів інформаційних відносин;
- при затвердженні правових норм використання ЕЦП дозволяє забезпечувати легітимний електронний документообіг та реалізувати правові відносини, такі як при використанні традиційних паперових документів.

Впровадження в ІВК НБУ сертифікатів управління привілеями (сертифікації атрибутів) дозволить зв'язати такі атрибути користувача як права доступу, категорії допуску, належність до певної групи, платіжну спроможність тощо з особою власника сертифіката. Як правило, така інформація має менший термін дії ніж сертифікат відкритого ключа. Атрибут сертифікатів використовується разом із сертифікатом відкритого ключа. В цьому випадку автентифікація суб'єкта здійснюється за допомогою сертифіката відкритого ключа, а зв'язування атрибутів із суб'єктом – за допомогою сертифіката атрибутів.

*Основні проблемні завдання та напрямки створення ІВК НБУ*

В Україні роботи щодо створення та застосування засобів ЕЦП розпочато ще в 1991-1992 рр. саме у банківський системі. В результаті їх виконання в 1994-1996 рр. у різних банках були впроваджені системи криптографічного захисту інформації, перш за все ЕЦП, в електронні платіжні системи та електронну пошту. Зацікавленість банків в наявності безпечних систем ЕЦП дозволила створити достатньо надійні прообрази сучасних інфраструктур відкритих ключів. Наприклад, в Укрсоцбанку створена та функціонує універсальна інфраструктура відкритих ключів, що забезпечує три основні функції: електронний цифровий підпис, направлене шифрування та управління привілеями.

Роботи щодо створення системи ЕЦП в масштабах держави по суті почалися з прийняттям національного стандарту на ЕЦП – ДСТУ 4145-2002. Планомірний характер вони одержали з прийняттям у 2003 р. законів України "Про електронні документи та електронний документообіг", а також "Про електронний цифровий підпис". Ці документи визначають організаційно-правові основи використання електронних документів і електронних підписів, в тому числі цифрових, в Україні. В них також визначено умови та вимоги, при дотриманні та виконанні яких електронний цифровий підпис з використанням особистого ключа прирівнюється до власноручного підпису, штампу, печатки тощо на паперовому документі.

Попередній аналіз та дослідження стану створення, впровадження та застосування системи ЕЦП в банківський сфері дозволяє виділити як найбільш проблемні такі завдання:

1) створення засвідчувального центру НБУ (ЗЦ НБУ) як основного уповноваженого органу ІВК у банківській сфері, основними функціями якого є реєстрація та акредитація центрів сертифікації ключів, формування кореневих сертифікатів відкритих ключів та управління їх життєвим циклом;
2) створення, дослідження та впровадження програмно-технічного комплексу ЗЦ НБУ;
3) створення, випробування, акредитація та впровадження акредитованих центрів сертифікації ключів банківських та фінансових установ;
4) створення, дослідження та випробування програмних та програмно-апаратних засобів виконання основних функцій ЕЦП користувачами;

5) визначення переліку та розроблення нормативних документів, а також стандартів з управління ключовими даними та сертифікації ключів;
6) проектування, виготовлення, дослідження та впровадження захищених носіїв ключових даних, у тому числі особистих ключів ЕЦП, та уніфікованих засобів виконання криптографічних перетворень, в першу чергу ЕЦП;
7) розроблення, узгодження та затвердження технічних завдань та техноробочих проектів на програмно-технічні комплекси ЗЦ НБУ та АЦСК, а також на захищені системи ведення архівів електронних документів та сертифікатів відкритих ключів;
8) створення матеріально-технічної бази та підготовка спеціалістів ЗЦ НБУ.

Роботу щодо створення ІВК НБУ уже сьогодні доцільно вести у таких напрямках:

1. *Створення нормативно-правової бази ІВК НБУ*, яке спрямоване на вдосконалення та подальший розвиток правових засад функціонування ІВК НБУ, розвиток правових відносин суб'єктів у сфері послуг ІВК. Нормативно-правова база має розвиватися у декількох напрямках:

- удосконалення нормативно-правової бази щодо використання електронного документообігу та ЕЦП банківськими та фінансовими установами усіх форм власності;
- удосконалення нормативно-правової бази щодо створення та забезпечення функціонування організаційно-технічної складової ІВК НБУ;
- удосконалення нормативно-правової бази щодо технологій, які використовуються під час реалізації та надання послуг ЕЦП, а у перспективі – послуг інфраструктури відкритих ключів та інфраструктури управління привілеями.

2. *Створення організаційно-технічної складової ІВК НБУ*. Чинним законодавством визначена ієрархічна структура уповноважених органів із сертифікації. На сьогоднішній день першочерговим завданням є забезпечення організаційно-технічних умов створення реальної структури уповноважених органів із сертифікації ключів у банківській сфері.

Основними напрямками вирішення цих завдань є:

- створення засвідчувального центру НБУ та забезпечення технологічних умов реалізації його основних функцій відповідно до чинного законодавства. Важливою технічною задачею є створення програмно-технічного комплексу сертифікації ключів із забезпеченням високого рівня захисту особистого ключа ЗЦ НБУ;
- створення типових програмно-технічних комплексів акредитованих центрів сертифікації ключів банківських та фінансових установ. Важливо визначити функціональну структуру центрів сертифікації та сформувати вимоги безпеки. У цьому напрямку необхідно враховувати досвід розвинутих країн, а також вимоги міжнародних стандартів щодо центрів сертифікації, їх архітектури та функцій;
- розробка політики застосування сертифікатів ЗЦ НБУ. Вирішення цієї задачі є суттєвим та дуже важливим, оскільки по суті це відомча політика застосування сертифікатів, яка має суттєвий вплив на функціонування всієї ІВК НБУ у цілому, а також на взаємодію з національною ІВК, з ІВК інших відомств. Вимоги політики застосування сертифікатів ЗЦ НБУ безпосередньо трансформуються та впливають на вимоги політик застосування сертифікатів, центрів сертифікації та акредитованих центрів сертифікації. Узгодження та відображення цих політик є важливим чинником організації взаємодії об'єктів та суб'єктів ІВК НБУ;
- нарешті, важливою є розробка регламентів надання послуг ЗЦ НБУ та центрами сертифікації банківських та фінансових установ. При створені регламенту ЗЦ НБУ важливо враховувати досвід інших країн світу.

3. *Підготовка кадрів.* Практичний досвід впровадження систем ЕЦП та ІВК у США, Канаді, Європейському союзі вказує, що недостатній рівень підготовленості персоналу є суттєвим чинником стримування ефективного впровадження технологій ІВК у повсякденну практику. Недостатній рівень популяризації знань про електронний документообіг та послуги ІВК серед державних службовців, персоналу об'єктів господарювання та населення суттєво зменшує ефективність використання цих новітніх технологій.

Важливими напрямками діяльності ЗЦ НБУ є участь у формуванні змісту стандартів освіти, замовлення та контроль підготовки фахівців відповідної кваліфікації.

*Основні вимоги до інфраструктури відкритих ключів Національного банку України*

ІВК НБУ має створюватися з урахуванням таких основних вимог:

- *довірчість*. Інфраструктура відкритих ключів Національного банку в цілому та її окремі компоненти мають бути довіреними об'єктами;

- *легкість, прозорість та зручність використання.* Впровадження послуг ЕЦП та інших послуг обслуговування сертифікатів, впровадження відповідних апаратних, програмних та програмно-апаратних засобів не мають призводити до суттєвого ускладнення функціонування існуючих систем та змін ділових та управлінських процесів;
- *інтероперабельність.* Корпоративні ІВК банківських установ мають задовольняти вимогу інтероперабельності та взаємодіяти між собою;
- *узгодженість імен.* ІВК НБУ має здійснювати узгодженість імен, з метою забезпечення унікальності імені для кожного суб'єкта (об'єкта);
- *масштабованість.* Архітектура ІВК НБУ має задовольняти вимоги масштабованості для забезпечення ефективного нарощування потужності під час зростання кількості користувачів ІВК НБУ та пов'язаних з ними сертифікатів;
- *гнучкість.* ІВК НБУ має задовольняти вимоги гнучкості з метою забезпечення можливості сумісної роботи різних додатків, платформ і технологій та врахування об'єктивних змін сучасних інформаційних технологій;
- *відповідність вимогам стандартів.* Об'єкти та компоненти ІВК НБУ мають відповідати вимогам міжнародних, національних, галузевих стандартів та нормативних документів;
- *архівування електронних документів.* ІВК НБУ має забезпечити можливість довгострокового зберігання (архівування) електронних документів, ключових даних, сертифікатів, списків скасування сертифікатів та інших даних. При цьому необхідно забезпечити представлення даних, що зберігаються, у єдиному форматі, або в такий спосіб, що забезпечує можливість надійного відновлення даних протягом встановлених строків зберігання.

*Основні вимоги до системи управління ключовими даними*

Система управління ключовими даними є найбільш критичною підсистемою ІВК НБУ. Високий рівень критичності даних, їх суттєвий вплив на захищеність та надійність ІВК НБУ визначають необхідність висування спеціальних вимог до управління ключовими даними.

Для функціонування ІВК НБУ та надання послуг з обслуговування сертифікатів необхідно використовувати різні типи ключових даних. Генерування ключових даних має здійснюватися відповідно до вимог чинного законодавства та нормативних документів. Об'єкти ІВК НБУ мають підтримувати генерування секретних (симетричних) ключів, особистих ключів та відкритих ключів відповідно до встановленого регламенту.

Незалежно від того, хто здійснює генерування та розподіл ключів, всі дії з управління ключовими даними мають виконуватися з дотриманням вимог конфіденційності, цілісності та доступності.

*Ключова структура ІВК НБУ* має складатися з трьох груп ключових даних:

І група. Спеціальні ключі ЗЦ НБУ (АЦСК). До першої групи входять особисті ключі та секретні симетричні ключі посадових осіб ЗЦ НБУ (АЦСК). Ці ключові дані призначені для здійснення встановлених операцій (дій) посадових осіб ЗЦ НБУ (АЦСК).

ІІ група. Робочі ключі ЗЦ НБУ (АЦСК). До другої групи входять особисті та відповідний йому відкритий ключ ЗЦ НБУ (АЦСК), які використовуються для формування сертифікатів відкритих ключів та підписання інформації про статус сертифіката.

ІІІ група. Особисті ключі підписувачів (фізичних та юридичних осіб), які відповідають відкритим ключам, що містяться у сертифікатах.

*Ключова структура уповноважених на сертифікацію.* З метою зниження ризику компрометації ключових даних, порушення конфіденційності, цілісності та доступності службової та іншої інформації у ЗЦ НБУ (АЦСК) можуть бути встановлені різні категорії ключових даних за призначенням:

- ключові дані підпису сертифікатів та інформації про статус сертифікатів;
- ключові дані забезпечення цілісності даних;
- ключові дані загальної авторизації об'єктів (суб'єктів);
- довгострокові ключі захисту ключів;
- довгострокові ключові дані забезпечення конфіденційності;
- короткострокові ключі захисту ключів;
- короткострокові ключові дані забезпечення конфіденційності.

*Основними складовими (об'єктами) ІВК НБУ* є:

- засвідчувальний центр НБУ;
- акредитовані центри сертифікації ключів банківських та фінансових установ (АЦСК);
- незалежні АЦСК, що надають послуги з обслуговування сертифікатів для банківських установ та акредитовані у ЗЦ НБУ;

- користувачі з клієнтськими засобами (КЗ) генерації ключів.

*Засвідчувальний центр НБУ* є найбільш важливим елементом ІВК НБУ. Він здійснює загальне управління та забезпечує ефективне функціонування ІВК НБУ у цілому, забезпечує взаємодію ІВК НБУ з національною ІВК. З метою забезпечення надійного функціонування ІВК НБУ у цілому до складу ЗЦ НБУ мають входити:

- постійно діюча комісія з питань акредитації центрів у ІВК НБУ;
- служба захисту інформації;
- програмно-технічний комплекс ЗЦ НБУ;
- служба архівування та резервування;
- служба перспективного планування та розвитку ІВК НБУ.

Пропозиції відносно організаційної структури та основних завдань ЗЦ НБУ наведено на рис. 1.


*Рис. 1. Організаційна структура та основні завдання ЗЦ НБУ*

Засвідчувальний центр НБУ виконує такі функції:

- публікує свою ідентифікаційну та іншу інформацію та надає її до центрального засвідчувального органу (ЦЗО);
- публікує ідентифікаційну та іншу інформацію про АЦСК, для яких він випускає сертифікати відкритих ключів;
- публікує перспективні плани обслуговування;
- публікує та надсилає у ЦЗО або у відповідні довідники положення своєї політики щодо застосування сертифікатів:
- здійснює ідентифікацію та автентифікацію підпорядкованих центрів сертифікації (у тому числі акредитованого);
- формує та здійснює управління сертифікатами центрів сертифікації;
- розповсюджує посилений сертифікат власного відкритого ключа;
- визначає процедури та зміст інформації, що необхідна для перевірки списку скасованих сертифікатів;
- отримує та здійснює автентифікацію запитів на скасування, поновлення та блокування сертифікатів, що були випущені ЗЦ;
- формує списки скасованих сертифікатів для всіх сертифікатів, що були випущені ЗЦНБУ;
- здійснює архівування сертифікатів, списків скасованих сертифікатів та іншої службової інформації;
- надсилає сертифікати та списки скасованих сертифікатів у відповідні довідники.

**Висновки.** В даній роботі розглянуто важливі концептуальні елементи створення інфраструктури відкритих ключів НБУ. В процесі розробки

цієї технології необхідно врахувати практичний досвід інших країн світу. На наш погляд розглянуті положення допоможуть вирішити актуальні проблеми та завдання, що стають перед НБУ на сучасному етапі впровадження цифрових технологій в усі види банківської діяльності. Викладені погляди можуть бути використані для розробки Концепції ІВК НБУ.

*Summary*

The author studies important conceptual elements for the formation of the infrastructure of open keys of the National Bank of Ukraine: goals and tasks, major requirements, structure and major functions of the specialized center of the National Bank of Ukraine.

Отримано 16.03.2006

Горбенко, І. Д. Концептуальні підходи до створення, впровадження та функціонування інфраструктури відкритих ключів Національного банку України [Текст] / І. Д. Горбенко // Вісник Української академії банківської справи. - 2006. - N 1. - С. 95 – 100.