Украинская академия банковского дела

Национального банка Украины

Кафедра Економической кибернетики

**Контрольная работа**

**по дисциплине „Платежные системы”**

Сумы 2008

**„Методи захисту платежів в мережі інтернет”**

**План**

1. Методи захисту платежів у мережі Іntегnеt

2. Принципи побудови захисту електронних банківських документів

3. Криптографічний захист інформації

4. Захист інформації та вирішення питань безпеки у СЕП

Література

**1. Методи захисту платежів у мережі Іntегnеt**

Слабким місцем мережної інфраструктури є незахищені канали зв'язку, де існує можливість появи неіснуючих платежів, перехоплення та несанкціонованого використання платіжних даних, інших проявів шахрайства та зловживань. Такі випадки траплялися в Іntегnеt. Існують два шляхи захисту передачі інформації: ізолювання мережі, яка використовується для обробки платежів, тобто використання приватних мереж, і шифрування даних.

Загальновизнано, що асиметричні алгоритми шифрування забезпечують вищий рівень надійності та безпеки. Найбільш поширене шифрування за допомогою відкритих ключів. Для розшифрування використовуються таємні ключі. Кількість можливих комбінацій, придатних для розшифрування зашифрованої за допомогою відкритих ключів інформації, залежить від довжини ключа в бітах. Вживання довших послідовностей у ролі ключів дозволяє випереджати можливості сучасних комп'ютерів, забезпечуючи надійний захист найважливішої інформації. Донедавна в Іntегnеt для захисту інформації найчастіше застосовувалися ключі довжиною 40 біт. Але ці ключі були легко розкриті (слід зазначити, що використання такого ненадійного засобу було наслідком дуже жорстких обмежень на експорт зі США потужних шифрувальних засобів). Нині в Іntегnеt розповсюджені ключі довжиною 1024 біт або навіть довші, що робить практично неможливим їх розкриття.

У платіжних системах важливе завдання - ідентифікація учасників платежу (автентифікація). Це робиться для обмеження доступу до платіжних засобів, надаючи право на такий доступ лише їх власникам, та для забезпечення можливості одержувати повідомлення про платіжні операції лише тим, кому вони адресовані. Надійна автентифікація сприяє також підвищенню рівня взаємної довіри між учасниками електронної комерції. На поточний момент в Іntегnеt застосовуються різноманітні засоби автен-тифікації. До них належить персональний ідентифікаційний код (РIN-код), який потрібно ввести перед виконанням фінансової операції. Але незначна довжина таких кодів дозволяє шахраям досить легко долати такі методи захисту.

Для захисту більш вдалим виявилося використання комп'ютерних паролів, які мають більшу довжину і складнішу структуру, що робить важчим їх розгадування. Цей метод досить широко застосовується в Іntегnеt, оскільки в ньому доступ до локальних систем контролюється шляхом використання паролів, але надійний результат можна мати лише за умови пра­вильного використання.

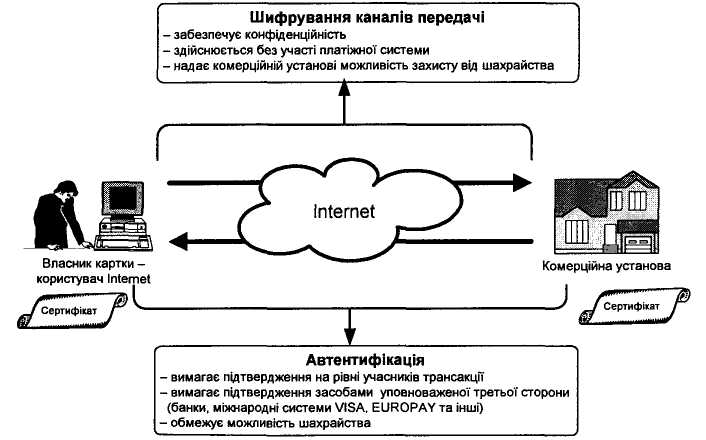


Рис. 1. Призначення цифрових сертифікатів

Дуже ефективним засобом захисту є електронний підпис. Його застосування передбачає наявність у того, хто цей підпис перевіряє, відкритого ключа, що відповідає застосованому особистому ключу (підпису) відправника електронного документа. Однак, при отриманні такого відкритого ключа не виключено шахрайство, внаслідок якого буде передано підроблений відкритий ключ, який автентифікуватиме підроблені повідомлення. Щоб запобігти цьому, застосовується практика сертифікування (підтвердження) відкритих ключів з боку уповноваженої на це і заслуговуючої довіри установи або організації (рис. 1). Таку установу чи організацію називають сертифікуючою, і вона ставить свій електронний підпис на відкритих ключах, які надаються користувачам платіжної системи. Відкритий ключ сертифікуючої установи повинен надаватися з використанням надійно захищених каналів. Ця установа сертифікує відкриті ключі учасників системи лише після перевірки їх тотожності з використанням захищених каналів або інших методів, що забезпечують достатній рівень безпеки, і лише підтверджені нею відкриті ключі вважаються чинними.

**2. Принципи побудови захисту електронних банківських документів**

Система захисту електронних банківських документів складається з комплексу апаратно-програмних засобів криптографічного захисту та ключової системи до них, технологічних і організаційних заходів щодо захисту інформації.

Система захисту електронних банківських документів в інформаційній мережі (далі - система захисту) включає:

а) усі етапи розроблення, упровадження та експлуатації програмно-технічного забезпечення в банківських установах, підключених до інформаційної мережі;

б) технологічні, апаратні, програмні засоби та організаційні заходи захисту;

в) чіткий розподіл відповідальності на кожному етапі підготовки, оброблення та виконання електронних банківських документів на всіх рівнях.

Система захисту забезпечує:

а) захист від несанкціонованого розшифрування та викривлення електронних банківських документів, появи фальсифікованих електронних банківських документів на будь-якому етапі оброблення;

б) автоматичне ведення протоколу оброблення електронних банківських документів з метою локалізації джерел появи порушень роботи програмно-технічних комплексів в інформаційній мережі;

в) захист від технічних порушень та збоїв апаратури {у тому числі збоїв та псування апаратних і програмних засобів, перешкод у каналах зв'язку);

г) належні умови для роботи програмно-технічних комплексів в інформаційній мережі, за яких фахівці банків - учасників СЕМП та Національного банку не можуть утручатись в оброблення електронних банківських документів після їх формування, та автоматичний контроль на кожному етапі їх оброблення.

Система захисту є єдиною для всіх інформаційних задач Національного банку і СЕМП. Для підвищення ступеня захисту міжбанківських електронних розрахункових документів у СЕМП використовуються додаткові засоби, уключаючи технологічний контроль. Технологічні та криптографічні засоби безпеки використовуються не лише в СЕМП, а й у всіх інформаційних задачах Національного банку.

**3. Криптографічний захист інформації**

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.

Криптографічний захист Інформації має охоплювати всі етапи оброблення електронних банківських документів, починаючи з часу їх створення до зберігання в архівах банку. Використання різних криптографічних алгоритмів на різних етапах оброблення електронних банківських документів дає змогу забезпечити безперервний захист інформації в інформаційній мережі, а також відокремлене оброблення інформації стосовно різних задач інформатизації Національного банку.

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.

Кожна банківська установа з точки зору захисту інформації має трибайтний ідентифікатор, перший знак якого є літерою відповідної території, на якій розташована ця банківська установа; другий та третій знаки є унікальним ідентифікатором банківської установи в межах цієї території. Ці ідентифікатори узгоджені з адресами системи ЕП і є унікальними в межах банківської системи України.

Трибайтні ідентифікатори є основою для ідентифікації робочих місць у банківських установах та ідентифікаторів ключі її для всіх робочих місць банківської установи. Ідентифікатор ключів робочих місць складається з шести символів, з яких три перших є ідентифікаторами банківської установи, четвертий символ визначає тип робочого місця (операцїоніст, бухгалтер тощо), п'ятий та шостий символи - ідентифікатор конкретного робочого місця (тобто службової особи, яка відповідає за оброблення платіжної інформації на цьому робочому місці). Трибайтний ідентифікатор банківської установи вбудований у програму генерації ключів і не може бути змінений у банківській установі, що забезпечує захист від підроблення ключів від імені інших банківських установ.

Відповідні ідентифікатори ключів записуються в електронні картки, які є носіями ключової інформації для апаратного шифрування.

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. Під час формування файла міжбанківських електронних розрахункових документів на робочому місці бухгалтера накладається ЕЦП на цей файл, що забезпечує захист від модифікації файла в цілому. Сформований таким чином платіжний файл обробляється АРМ-НБУ, де виконується перевірка ЕЦП операціоніста на кожному міжбанківському електронному розрахунковому документі та накладається ЕЦП АРМ-НБУ, який можуть перевірити всі банківські установи - учасники СЕП. Під час оброблення платіжних файлів на АРМ-2 виконується перевірка підписів на файлі в цілому та після формування файлів відповідних платежів накладається ЕЦП на файл у цілому за допомогою таємного ключа АРМ-2.

**4. Захист інформації та вирішення питань безпеки у СЕП**

Система захисту СЕП НБУ розроблялася разом з технологією та бухгалтерською моделлю. Під час експлуатації СЕП вона постійно аналізувалась і зміцнювалась. Захист електронних платіжних документів є невід'ємною частиною програмно-апаратних комплексів СЕП, він не може бути виключений або змінений. Усі учасники електронних розрахунків у СЕП повинні мати відповідний дозвіл Національного банку України та дотримуватися всіх вимог безпеки. Крім того, кожний банк-учасник мусить мати систему захисту внутрішньобанківських розрахунків.

При розробці системи захисту були виділені такі завдання:

* захист від злочинних дій (несанкціоноване розшифрування та викривлення платіжних повідомлень, поява фальсифікованих платежів на будь-якому етапі обробки - від клієнта банку до АРМ-1);
* автоматичне ведення протоколу використання банківської мережі для локалізації джерел появи порушень роботи СЕП;
* захист від технічних порушень апаратури: збоїв та псування апаратних і програмних засобів, перешкод у каналах зв'язку;
* створення умов роботи СЕП, при яких фахівці банків - учасників СЕП та Національного банку практично не мають змоги втручатися в обробку платіжних документів після їх формування;
* забезпечення контролю на кожному етапі обробки.

Система захисту СЕП включає технологічні, апаратні, програмні засоби та організаційні заходи захисту, забезпечує чіткий розподіл відповідальності на кожному етапі підготовки, обробки та виконання платежів на всіх рівнях - від клієнта банку до АРМ-1.

З урахуванням завдань банківської безпеки у СЕП була створена Служба захисту інформації на двох рівнях: у Національному банку та в регіональних розрахункових палатах, через які здійснюються міжрегіональні та внут-рішньорегіональні платежі.

Служба захисту інформації НБУ здійснює свою діяльність відповідно до Законів України «Про банки і банківську діяльність», «Про захист інформації в автоматизованих системах» та нормативних актів Національного банку.

Служба захисту інформації на рівні Національного банку вирішує питання, що пов'язані з:

* розробкою загальної політики безпеки електронних платежів в Україні;
* постійним аналізом системи захисту та її вдосконаленням;
* розробкою, підготовкою та сертифікацією апаратних і програмних засобів захисту;
* генерацією та розподілом програм криптографічного захисту та ключової інформації;
* наданням консультацій та навчанням персоналу служб захисту інформації регіональних розрахункових палат;
* аналізом збоїв у функціонуванні СЕП та спроб несанкціонованого доступу до СЕП (далі - НСД).

У разі необхідності Служба захисту інформації НБУ надає арбітражні послуги банкам - учасникам системи електронних платежів. Відділи захисту інформації на другому рівні забезпечують:

* впровадження розробленої політики безпеки;
* впровадження апаратних та програмних засобів захисту всіма уча­сниками системи електронних платежів;
* проведення консультацій та навчання персоналу банків, які беруть участь у СЕП;
* нагляд за виконанням вимог банківської безпеки учасниками СЕП;
* підготовку інформації для аналізу збоїв роботи СЕП та НСД.

З досвіду експлуатації системи можна зробити висновок, що Служба захисту інформації НБУ, побудована на основі вищезазначених принципів, забезпечує достатній рівень безпеки у СЕП.

Система безпеки СЕП є багаторівневою. Вона включає не лише засоби шифрування інформації, які, беззаперечно, є дуже важливими та надають можливість отримати достовірну інформацію на різних рівнях, а й цілий комплекс технологічних та бухгалтерських засобів контролю за проходженням платежів у СЕП. Такий технологічний та бухгалтерський контроль забезпечується програмним забезпеченням на всіх рівнях, що дозволяє персоналу РРП та ЦРП, учасникам розрахунків відстежувати порядок проходження платежів як протягом дня, так і за підсумками дня.

Технологічні засоби контролю включають:

* механізм обміну квитанціями в режимі реального часу, який дозволяє однозначно ідентифікувати отримання адресатом конкретного пакета документів та достовірність інформації, що в ньому міститься;
* механізм інформування банку - учасника СЕП про поточний стан його коррахунку за підсумками технологічних сеансів у РРП, який
* дозволяє банку відстежувати відповідність змін коррахунку та при­ймання/передачі пакетів платіжних документів;
* взаємообмін між банком та РРП підсумковими документами на кі­нець банківського дня, програмну звірку підсумкових документів як у РРП, так і в банку;
* програмний комплекс самодіагностики, який дозволяє виявити по­рушення цілісності та неузгодженість баз даних АРМ-2, що може виникнути внаслідок збою в функціонуванні системи, спроб несанкціонованого доступу до баз даних АРМ-2 або фізичного їх псування;
* взаємообмін між АРМ-2 та АРМ-1 повідомленнями звітного харак­теру про функціонування СЕП у цілому; : • механізм контролю програмних засобів для виявлення несанкціонованої модифікації модулів програмного забезпечення. Усі технологічні засоби контролю вбудовані у програмне забезпечення, їх не можна вилучити, а в разі виникнення нестандартної ситуації або підозри на несанкціонований доступ вони негайно інформують працівників РРП та ЦРП, що дає можливість оперативно втручатися у таку ситуацію. Бухгалтерські засоби контролю включають:
* комплект звітних документів, які отримуються в АРМ-2, містить повну технологічну та бухгалтерську інформацію, перехресні посилання та аналіз балансу;
* комплект звітних форм АРМ-1, які містять бухгалтерську інформацію про стан СЕП в Україні;
* засоби звірки взаємодії РРП в АРМ-1, які дозволяють виявити розбіжності в звітній інформації, що надає РРП;
* засоби аналізу причин відсутності балансу в масштабах України. Однак, застосування тільки технологічних та бухгалтерських засобів контролю у СЕП недостатньо, щоб забезпечити захист від зловживань при передачі платіжних документів у СЕП. До того ж, автоматичне ведення протоколу виконуваних дій у системі платежів має супроводжуватися також захистом цього протоколу від підробки та модифікації. Всі ці вимоги можуть бути виконані тільки за допомогою програмних та апаратних засобів шифрування.

Система захисту банківської інформації у СЕП включає комплекс заходів шифрування інформації, яка циркулює у платіжній системі. Шифруванню підлягають усі файли, що передаються між АРМ СЕП: як пакети початкових та відповідних платіжних документів, так і квитанції на них, всі інші технологічні файли.

Усі платіжні документи СЕП перед відправкою з банківської установи обробляються апаратними або програмними засобами захисту інформації, які забезпечують виконання ряду вимог безпеки інформації у СЕП, а саме:

* закритість інформації, яка пересилається (повідомлення не може бути прочитане ніким, крім адресата);
* цілісність (будь-яке, випадкове або зловмисне, викривлення пові­домлення на етапі передавання буде виявлене при прийманні);
* аутентичність відправника (при прийманні однозначно визначаєть­ся, хто відправив конкретне повідомлення).

Крім цих основних вимог, виконується ряд додаткових, що дозволяє детальніше аналізувати можливі нестандартні ситуації:

* засобами захисту інформації ведеться шифрований арбітражний журнал, який містить протокол обробки інформації, а також зміст оброблених файлів;
* у шифроване повідомлення включені реквізити дати та часу обробки.

В основу роботи засобів захисту інформації у СЕП покладений алгоритм шифрування із закритими симетричними ключами за ГОСТ 28147-89. Згаданий метод характеризується високою стійкістю до дешифрування, але одночасно висуває високі вимоги до процедури транспортування та зберігання закритих ключів, секретність яких і визначає реальну стійкість системи шифрування в цілому. Щоб забезпечити секретність ключів при їх транспортуванні, зберіганні та використанні, застосовується комплекс тех­нологічних і організаційних заходів.

Основними засобами захисту інформації у СЕП є апаратні засоби. В них секретність ключів забезпечується технологічно:

* ключі зберігаються в спеціальній електронній картці, їх зчитування можливе лише у пам'яті спеціального блоку («шифроблоку»), який здійснює процес шифрування інформації. Зчитування ключів іншими засобами не можливе;
* електронна картка видається конкретному банку з попередньою прив'язкою її до конкретного шифроблоку цього ж банку; якщо картку загублено або викрадено, то вона не буде працювати в іншому шифроблоці (наприклад, в апаратурі іншого банку);
* на випадок викрадення одночасно блоку і картки у конкретного банку передбачений режим виключення цієї апаратури із списку користувачів СЕП; банк зможе продовжувати роботу у СЕП шляхом отримання нового комплекту, після вирішення юридичних та фінансових питань, пов'язаних із втратою апаратури.

Резервним засобом захисту у СЕП є програмне шифрування, яке реалізує такий самий алгоритм шифрування. Програмні засоби шифрування є невід'ємною частиною програмного забезпечення АРМ-1, АРМ-2, АРМ-3 СЕП.

Зберігання та використання засобів захисту повинно відповідати вимогам, які висуваються до інформації з грифом «Банківська таємниця». Задоволення цих вимог забезпечується організаційними заходами.

При роботі засобів криптування банківської інформації ведеться шифрований архів банківських платежів, де зберігаються всі зашифровані та відправлені, а також одержані та дешифровані платежі. Дешифрування повідомлень архіву можливе лише за наявності ключа, який знаходиться в Службі захисту електронних банківських документів Національного банку. Наприкінці робочого дня цей шифрований архів треба обов'язково переписати на гнучкі магнітні носії. Він використовується для надання інформаційно-арбітражних послуг, які надає Служба захисту електронних банківських документів Національного банку відповідно до «Положення про інформаційно-арбітражні послуги служби захисту електронних банківських документів у СЕП».

Арбітражна версія апаратно-програмного комплексу криптографічного захисту дає змогу Службі захисту електронних банківських документів Національного банку при наявності копій шифрованого архіву банківської установи - учасника СЕП дешифрувати всі повідомлення з цього архіву та з абсолютною достовірністю визначати:

* ім'я абонента, який відправив (зашифрував) електронний платіжний документ;
* ім'я абонента, якому адресовано електронний платіжний документ;
* дату, годину та хвилину, коли виконувалося шифрування електронного платіжного документа;
* дату, годину та хвилину, коли та ким виконувалося дешифрування електронного платіжного документа.

При використанні апаратних засобів захисту додатково визначається:

* номер апаратури захисту, на якій виконувалось шифрування (дешифрування) електронного платіжного документа;
* номер електронної картки, якою користувались під час шифрування (дешифрування) електронного платіжного документа.

Журнали реєстрації надходжень електронної пошти дають змогу володіти інформацією про шлях та час проходження електронного платіжного документа від однієї банківської установи до іншої через усі пункти мережі телекомунікації СЕП.

Апаратні та програмні засоби шифрування, які надає Служба захисту інформації НБУ, отримали позитивну експертну оцінку Служби безпеки України та рекомендовані для застосування з дотриманням деяких організаційних та технологічних запобіжних заходів.

Додатково для захисту інформації у СЕП використовуються апаратні засоби шифрування в каналах телекомунікаційного зв'язку - апаратура захисту банківських даних (АЗБД). Ця апаратура забезпечує гарантований захист банківських електронних повідомлень від перехоплення, нав'язування, підробки та викривлення їх унаслідок зовнішнього впливу, підтримує абсолютну достовірність повідомлень, використовуючи електронні картки як носії ключової інформації. Такі засоби захисту «прозорі» для телекомунікаційних систем, сумісні зі стандартними протоколами зв'язку та працюють в автоматичному режимі.

З перших місяців роботи СЕП Службою захисту банківської інформації НБУ ведеться аналіз усіх порушень функціонування системи як з погляду надійності її роботи (апаратно-програмні збої, випадкові порушення технології тощо), так і з погляду безпеки (можливість «НСД»).

Кожному банку - учаснику СЕП Службою захисту інформації НБУ надається програмне забезпечення, яке складається з трьох модулів:

Власне модуля накладання/перевірки електронного цифрового підпису у вигляді бібліотеки об'єктних модулів, яка може бути вбудована в програмний комплекс «Операційний день банку» на будь-якому робочому місці підготовки платіжних документів.

Модуля генерації ключів для банку - учасника СЕП. Модуль генерації ключів надається у вигляді виконуваного модуля і виготовляється особисто для кожної установи — учасника СЕП. За допомогою такого генератора ключів учасник СЕП сам генерує пари таємного та відкритого ключів для всіх робочих місць підготовки платежів.

Модуля поновлення таблиці відкритих ключів та незаповнених таблиць відкритих ключів на кожне робоче місце, який виконує коректне поновлення таблиць відкритих ключів, створює їх резервні копії і веде протокол виконаних дій.

При генерації ключів таємний ключ записується на дискету або на touch-memory. Відкриті ключі, які використовуються всередині банку (наприклад, ключі операціоністів), записуються до згаданого каталогу у вигляді файлів змін таблиці відкритих ключів. Відкриті ключі робочих місць, електронний цифровий підпис яких перевіряється у СЕП, а саме - відкриті ключі АРМ-3 та АРМ бухгалтера, записуються у вигляді файлів сертифікації до каталогу, який задається. Ці файли надсилаються до Служби захисту інформації НБУ для виконання їх сертифікації, що дає можливість перед розповсюдженням їх через СЕП переконатися в тому, що вони належать саме цьому учаснику СЕП, а не були згенеровані кимось іншим від імені цього учасника, і що для них виконані всі вимоги, які висуваються до відкритих ключів алгоритму RSA. Після успішного проходження сертифікації відкриті ключі учасника СЕП розсилаються у вигляді файлів змін таблиць відкритих ключів на робочі місця, обумовлені технологією перевірки електронного цифрового підпису (АРМ-3 та АРМ-2).

Правові основи та нормативні документи НБУ повинні забезпечити правове середовище для захисту електронних міжбанківських розрахунків із визначенням юридичних та фізичних осіб, які несуть відповідальність за виконання операцій в системі, прав і обов'язків учасників системи, гарантують виконання фінансових трансакцій та дотримання конфіденційності інформації, що циркулює в системі. Особлива увага в нормативних документах НБУ та підзаконних актах приділяється розгляду спірних питань і порядку ведення арбітражних справ між учасниками системи електронних міжбанківських розрахунків, опису обов'язків учасників системи щодо збереження та своєчасного надання арбітражної інформації, яка створюється засобами криптозахисту програмних комплексів системи та зберігається зашифрованою.

Нормативними документами НБУ визначається комплекс адміністративних заходів, спрямованих на забезпечення захисту підготовки, передачі, обробки та зберігання у кожного учасника системи інформації про електронні фінансові трансакції; визначені правила доступу і фізичного захисту вузлів збирання, обробки та зберігання інформації. Нормативні документи НБУ регламентують також порядок генерації, транспортування, розподілу, оновлення і використання ключів криптографічного захисту в системі. Спеціальні інструкції НБУ суворо регламентують порядок роботи фахівців банківських установ із засобами захисту, використання та зберігання криптографічних ключів, розподіл повноважень щодо питань захисту інформації в банківській установі.

У головних вузлах збору, обробки та зберігання інформації в системі (Центральна розрахункова палата, регіональні розрахункові палати тощо) повинні вживатися заходи для захисту інформації від витоку технічними каналами. В усіх приміщеннях, де розташовані сервери системи, включаючи телекомунікаційні, постійно ведеться контроль за дотриманням визначеного комплексу організаційно-технічних заходів щодо порядку обстеження цих приміщень для контролю за витіканням інформації технічними каналами (лінії живлення, заземлення, допоміжні технічні засоби, електромагнітне випромінювання обчислювальних машин). Спеціальні вимоги щодо дотримання режимних умов у приміщеннях банківських установ -учасників СЕП, де обробляються, працюють та зберігаються засоби захисту, зазначені у «Положенні про міжбанківські розрахунки в Україні» і обов'язкові для усіх банківських установ. Усі службові особи, які виконують електронні розрахунки, зобов'язані суворо дотримуватися цих вимог. Відповідальність за виконання вищезгаданих вимог покладено на керівників банківських установ.

**ЛІТЕРАТУРА**

1. "Інструкція про міжбанківський переказ грошей в Україні в національній валюті", затверджена Постановою Правління Національного банку України 17.03.2004 р. № ПО, зареєстрована в Міністерстві юстиції України 15.04.2004р. за №483/9082.
2. "Персональні ЕОМ в інженерній практиці", Т.З.Кренкель, А.Г.Коган, А.М.Тараторин, вид. Москва "Радіо і звязок", 1989р.
3. А.Н.Романов, Б.Е.Одинцов „Советующие информационные системы в экономике „ ЮНИТИ, Москва, 2000 г.
4. Алан Нейбауэр „Access 2000 для занятых», перевод с английского, Питер, 2001, - 288 с.
5. В.М.Гужва „Інформаційні системи і технології на підприємствах”, навчальний посібник, Київ, 2001 р.
6. В.Ф.Ситник, Т.А.Писаревська, Н.В.Єрьоміна, О.С.Краєва „Основи інформаційних систем”, навчальний посібник, Київ, 2001 р.
7. І.Ф.Рогач, М.А.Сендзюк, В.А.Антонюк „Інформаційні системи у фінансово-кредитних установах”, навчальний посібник, Київ, 1999 р.
8. Под ред. Д.є.н. професора В.В.Евдокимова «Экономическая информатика», Учебник для вузов, Питер, 1997, - 592 с.
9. Титоренко Е.М. Автоматизированные информационные технологии в экономике. М., 1998 г.
10. Титоренко Е.М. Компьютеризация банковской деятельности, М., 1997 г.