**\_\_\_\_\_Тернопільський національний технічний університет імені Івана Пулюя\_\_\_\_\_\_**

(повне найменування вищого навчального закладу)

Кафедра \_\_\_\_\_\_\_\_\_**кібербезпеки**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

\_\_**5.9 «Інформаційні банківські технології»**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(шифр і назва навчальної дисципліни)

напрям підготовки \_\_**6.170101 «Безпека інформаційних і комунікаційних систем»**

(шифр і назва напряму підготовки)

спеціальність **7.17010101 «Безпека інформаційних і комунікаційних систем»**\_\_\_\_\_\_\_\_

(шифр і назва спеціальності)

(назва спеціалізації)

факультет \_\_\_\_**комп’ютерно-інформаційних систем і програмної інженерії**\_\_\_\_\_\_\_\_\_

(назва інституту, факультету, відділення)

Тернопіль – 201\_\_ рік

Опорний конспект лекцій з дисципліни

**«Інформаційні банківські технології»**\_\_для студентів

(назва навчальної дисципліни)

за напрямом підготовки 6.170101 «Безпека інформаційних і комунікаційних систем», спеціальністю 7.17010101, 8.17010101 «Безпека інформаційних і комунікаційних систем».

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ року - 206 с.

Розробники:доц. Кареліна О. В.

Опорний конспект лекцій затверджений на засіданні кафедри кібербезпеки ТНТУ   
ім. І. Пулюя

Протокол від. "\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року № \_\_\_

Завідувач кафедри кібербезпеки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_Козак Р. О.\_\_\_)

(підпис) (прізвище та ініціали)

"\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року

Схвалено Методичною радою факультету комп’ютерно-інформаційних систем і програмної інженерії

Протокол від "\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року № \_\_\_

"\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року Голова \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_Осухівська Г.М. \_\_)

(підпис) (прізвище та ініціали)

© Кареліна О. В., 201\_\_ р.

© ТНТУ, 201\_\_ р.

**Лекція 1. Системи електронних платежів.**

# 1.   Становлення електронних платежів в україні.

# 2.   Система електронних міжбанківських платежів.

# 3. Положення про захист електронних банківських документів з використанням засобів захисту інформації національного банку України.

4.    Національна платіжна система "Український платіжний простір".

# 1.   СТАНОВЛЕННЯ ЕЛЕКТРОННИХ ПЛАТЕЖІВ В УКРАЇНІ.

У 1994 р. НБУ було прийняте стратегічне рішення щодо впровадження системи електронних міжбанківських розрахунків/платежів (СЕП). Ця державна платіжна система об’єднала засобами електронної пошти в єдиний інформаційний простір всі комерційні банки України. СЕП створювалась як багаторівнева безпаперова система.

Впровадження СЕП дало змогу відмовитись від використання поштових та телеграфних авізо, значно підвищити швидкість, якість і надійність виконання платежів, забезпечити безпеку та конфіденційність банківської інформації. Архітектура СЕП включає три рівні: комерційні банки (КБ), де функціонують програмно-технічні комплекси АРМ-3; обласний рівень НБУ, куди передаються платіжні повідомлення від КБ, представлений регіональними розрахунковими палатами (РРП) і відповідно комплексом АРМ-2; найвищий рівень — це центральна розрахункова палата (ЦРП) і комплекс АРМ-1, який проводить облік та контроль платежів у масштабі України в цілому. СЕП побудована і функціонує за міжнародними стандартами, виконуючи обробку та передачу повідомлень. Кожний комерційний банк є самостійним учасником СЕП і може вибрати одну з моделей обслуговування кореспондентського рахунку, яких налічується сім. Банки, які мають власні платіжні системи, виходять лише на рівень ЦРП із загальними консолідованими сумами. СЕП дає змогу НБУ щоденно на десяту годину ранку мати актуальний баланс банківської системи України за попередній день. За допомогою СЕП щодня опрацьовується більш як 300 тис. платіжних документів на суму близько одного мільярда доларів США.

Створення і впровадження такої системи дало змогу національній банківській системі України стати однією з досить ефективних і отримати схвальні відгуки фахівців. Безумовно, як будь-яка комп’ютерна система, СЕП не є чимось сталим; це — система, яка постійно удосконалюється й розвивається. Зокрема, великих змін та трансформацій СЕП зазнала у зв’язку з переходом на міжнародні стандарти бухгалтерського обліку.

В НБУ функціонує електронний депозитарій для управління державними цінними паперами. Створена національна платіжна система для автоматизації масових розрахунків на базі пластикових карток VISA, Master Card та ін.

Аналізуючи стан справ на рівні комерційних банків, слід зазначити, що рівень впровадження сучасних інформаційних технологій у комерційних банках України дуже різний. Це пов’язано з надто швидким зростанням кількості банківських установ та різним рівнем їх фінансових можливостей щодо впровадження комп’ютерних технологій. Тому є банки, які мають лише набір засобів для формування необхідної звітності та програмних продуктів, що дозволяють банкам, згідно з вимогами Національного банку України, бути учасниками СЕП. Поряд з такими банками, які характеризуються невисоким рівнем комп’ютеризації робіт, є банківські установи, котрі добре розуміють, що сучасні інформаційні технології є основним засобом підвищення конкурентоспроможності у боротьбі за пріоритетне становище на фінансовому ринку та залучення клієнтів. Тому в таких банках при виборі комп’ютерних систем перевагу надають технологіям, які розроблені з урахуванням міжнародних стандартів і відповідають вимогам відкритих систем, а також можуть легко переноситись з однієї платформи на іншу.

Для залучення нових клієнтів та створення зручностей щодо їхнього спілкування з банком у багатьох банківських установах впроваджена й успішно функціонує система «Клієнт-банк». Впровадження такої системи дає змогу клієнту спілкуватися з банком і виконувати платежі, не виходячи з свого офісу, що, безперечно, підвищує привабливість банку при виборі його клієнтом.

Деякі українські комерційні банки є учасниками міжнародної фінансової телекомунікаційної мережі SWIFT.

# 2.   СИСТЕМА ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ.

Відповідно до статті 11 Закону України "Про платіжні системи та переказ коштів в Україні" Національний банк України має право створювати системи міжбанківських розрахунків, системи роздрібних платежів та інші види платіжних систем. Національний банк України забезпечує безперервне, надійне та ефективне функціонування і розвиток створених ним платіжних систем. Створені Національним банком України платіжні системи є державними платіжними системами.

На сьогодні в Україні функціонують дві платіжні системи, платіжною організацією та розрахунковим банком яких є Національний банк України:

Cистема електронних платежів (СЕП);

Національна платіжна система «Український платіжнй Простір».

|  |
| --- |
|  |

### 2.1. СИСТЕМА ЕЛЕКТРОННИХ ПЛАТЕЖІВ (СЕП).

Система електронних платежів Національного банку (СЕП) – державна банківська платіжна система, що забезпечує проведення міжбанківського переказу через рахунки, відкриті в Національному банку України.

СЕП забезпечує здійснення розрахунків у межах України між банками як за дорученнями клієнтів банків, так і за зобов’язаннями банків та інших учасників системи. У СЕП виконуються міжбанківські перекази у файловому режимі та в режимі реального часу. Здійснення учасником початкових платежів у файловому режимі є обов’язковим, а в режимі реального часу – за його вибором. Крім того, учасник системи, який працює в СЕП у файловому режимі, має забезпечити приймання платежів, відправлених на його адресу іншими учасниками СЕП у режимі реального часу.

У файловому режимі обмін міжбанківськими електронними розрахунковими документами здійснюється шляхом приймання-передавання документів, згрупованих у файли. Тривалість технологічного циклу становить 15 – 20 хвилин. Кошти списуються з технічного рахунку учасника СЕП у момент приймання початкових платежів до Центру оброблення СЕП та зараховуються на технічний рахунок учасника-отримувача у момент надходження до Центру оброблення СЕП квитанції про успішне приймання файла платежів у відповідь.

У режимі реального часу кошти списуються з технічного рахунку учасника СЕП-платника і зараховуються на рахунок учасника-отримувача одночасно.

СЕП приймає початкові платежі від учасника системи в межах поточного значення його технічного рахунку. У СЕП немає пріоритетів оброблення платежів, крім черговості їх надходження.

СЕП визнана системно важливою платіжною системою в Україні. Системна важливість СЕП обумовлена тим, що вона забезпечує здійснення 97%% міжбанківських переказів у національній валюті в межах України.

СЕП є системою класу RTGS (Real-time gross settlement).

### **ПРАВОВА ОСНОВА ФУНКЦІОНУВАННЯ СЕП**

Базовим законом, що визначає загальні засади функціонування платіжних систем в Україні та загальний порядок проведення переказу коштів у межах України, є Закон України "Про платіжні системи та переказ коштів в Україні".

Цим Законом СЕП визначено державною системою міжбанківських розрахунків, а Національний банк України – платіжною організацією та розрахунковим банком СЕП.

### **Порядок функціонування СЕП визначається Національним банком України.**

### ПРАВИЛА СЕП

СЕП працює за правилами, що складаються з комплексу нормативно-правових актів Національного банку України та технологічної документації, а саме:

       щодо порядку ініціювання та здійснення переказу в СЕП, умов участі, порядку вступу та виходу із системи, оформлення електронних розрахункових документів:

•         Інструкції про міжбанківський переказ коштів в Україні в національній валюті, затвердженої постановою Правління Національного банку України від 16.08.2006 № 320, зареєстрованої в Міністерстві юстиції України 06.09.2006 за № 1035/12909 (зі змінами);

•        • Інструкції про безготівкові розрахунки в Україні в національній валюті, затвердженої постановою Правління Національного банку України від 21.01.2004 № 22 (зі змінами);

       щодо захисту інформації та вирішення спорів між учасниками системи – постанови Правління Національного банку України від 26.11.2015 № 829 "Про затвердження нормативно-правових актів з питань інформаційної безпеки";

       щодо забезпечення безперервного функціонування СЕП:

•        Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 № 265 (зі змінами);

•        Інструкції щодо організації роботи банківської системи в надзвичайному режимі, затвердженої постановою Правління Національного банку України від 22.07.2014 № 435 (зі змінами);

•        Положення про міжбанківський переказ коштів в Україні в національній валюті в особливий період, затвердженого постановою Правління Національного банку України від 23.12.2003 № 576, зареєстрованого в Міністерстві юстиції України 14.01.2004 за № 39/8638;

•        Положення про функціонування інформаційних систем Національного банку України та банків в особливий період, затвердженого постановою Правління Національного банку України від 21.04.2004 № 175, зареєстрованого у Міністерстві юстиції України 17.05.2004 за № 618/9217 (зі змінами);

       щодо регламенту та технології роботи СЕП:

•        Технологічного регламенту роботи системи електронних платежів Національного банку України;

•        Опису інтерфейсу між системою автоматизації банку і СЕП НБУ;

       щодо плати за послуги СЕП – Тарифів на послуги (операції), що надаються (здійснюються) Національним банком України в системі електронних платежів та у сфері розрахунково-касового обслуговування, затверджених постановою Правління Національного банку України від 12.08.2003 № 333 (зі змінами).

### ТЕРМІНОЛОГІЯ СЕП

**Банківський день** у системі електронних платежів Національного банку (далі - банківський день) - позначений календарною датою проміжок часу, протягом якого виконуються технологічні операції, пов'язані з проведенням міжбанківських електронних розрахункових документів через систему електронних платежів Національного банку (далі - СЕП), за умови, що підсумки розрахунків за цими документами відображаються на кореспондентських рахунках банків у Національному банку на ту саму дату;

**Внутрішньобанківська міжфілійна платіжна система** (далі - ВМПС) - платіжна система банку, яка забезпечує проведення переказу коштів між його філіями та взаємодію із СЕП для виконання міжбанківського переказу коштів філіями банку, що працює за моделлю 3 обслуговування консолідованого кореспондентського рахунку;

внутрішньобанківський переказ коштів через ВМПС (далі - внутрішньобанківський переказ) - переказ коштів між банком та його філіями або між філіями банку, що здійснюється засобами ВМПС;

**Електронний технологічний довідник банків України** та інших установ - систематизований перелік банків, філій, інших установ, що є складовою частиною інформаційної мережі Національного банку і використовується під час роботи всіх її програмно-технічних комплексів;

**електронне розрахункове повідомлення** - електронний документ, який несе інформацію щодо переказу коштів, має такий самий формат, реквізити, порядок формування і технологію оброблення в СЕП, як і міжбанківський електронний розрахунковий документ, але не супроводжується рухом коштів;

**електронний банківський документ** - електронний документ, що використовується в банківській діяльності, формат, обов'язкові реквізити і засоби захисту якого відповідають вимогам законодавства;

**заблоковані кошти** - кошти, заблоковані Національним банком на кореспондентському рахунку банку, відкритому в Національному банку, у розмірі наданого банку кредиту овернайт без забезпечення (далі - кредит овернайт бланковий) та процентів за користування ним відповідно до нормативно-правового акта Національного банку про регулювання ліквідності банків України;

**інформаційна мережа Національного банку** (далі - інформаційна мережа) - комплекс апаратно-програмних засобів та організаційних заходів, що призначені для забезпечення функціонування власних задач автоматизації банківських і господарсько-фінансових операцій Національного банку, а також взаємодії з телекомунікаційними мережами та інформаційними системами банків, фінансових і державних інституцій України;

**інформаційно-пошукова система СЕП** (далі - ІПС) - складова СЕП що призначена для надання учасникам СЕП інформації про переказ коштів, виконаний ними через СЕП;

**код банку** - умовна шестизначна числова ознака, що ідентифікує банк, філію, іншу установу, розраховується Національним банком і є обов'язковим реквізитом Електронного технологічного довідника банків України та інших установ і Довідника учасників СЕП;

**кореспондентський рахунок** - рахунок, що відкривається одним банком іншому банку філії іноземного банку для здійснення міжбанківського переказу коштів;

**ліміт початкових оборотів** - сума, що визначає максимальний обсяг початкових платежів, які банк (філія) може виконати за певний період;

**ліміт технічного рахунку** - сума, що визначає мінімальний залишок коштів на технічному рахунку банку (філії);

**міжбанківський електронний розрахунковий документ** - електронний документ на переказ коштів, сформований банком (філією) на підставі власних розрахункових документів, розрахункових документів клієнтів і стягувачів, документів на переказ готівки для виконання міжбанківського переказу коштів;

**міжбанківський переказ коштів** (далі - міжбанківський переказ) - переказ коштів між банками в безготівковій формі, що обумовлений потребою виконання платежів клієнтів або власних зобов'язань банків;

**міжбанківський переказ у СЕП у режимі реального часу** - міжбанківський переказ, що здійснюється з індивідуальним обробленням міжбанківського електронного розрахункового документа, за яким списання коштів з технічного рахунку учасника СЕП (платника) та зарахування коштів на технічний рахунок учасника СЕП (отримувача) виконується одночасно;

**міжбанківський переказ у СЕП у файловому режимі** - міжбанківський переказ, що здійснюється з індивідуальним обробленням міжбанківського електронного розрахункового документа, за яким між списанням коштів з технічного рахунку учасника СЕП (платника) та зарахуванням коштів на технічний рахунок учасника СЕП (отримувача) є певний проміжок часу;

**модель обслуговування консолідованого кореспондентського рахунку в СЕП** (далі - модель) - сукупність механізмів і правил роботи СЕП, банку та його філій, згідно з якими виконується міжбанківський переказ через консолідований кореспондентський рахунок;

**операційні правила** - система логічних та операційних обмежень у відповідній моделі, що встановлюються банком для філій на переказ коштів через СЕП, а також на переказ коштів та інші банківські операції філій у системі автоматизації банку;

**пакет-відповідь** - одиниця обміну інформацією в СЕП у режимі реального часу, формується засобами центру оброблення СЕП (далі - ЦОСЕП) у відповідь на пакет-запит від системи автоматизації банку (далі - САБ) відправника;

**пакет-запит** - одиниця обміну інформацією в СЕП у режимі реального часу, формується засобами САБ відправника і надсилається до ЦОСЕП;

**система автоматизації банку** (САБ) - програмне забезпечення, що обслуговує поточну внутрішньобанківську діяльність (бухгалтерський облік, обслуговування рахунків клієнтів тощо);

**система електронних платежів Національного банку (СЕП)** - державна банківська платіжна система, що забезпечує проведення міжбанківського переказу через кореспондентські рахунки банків - резидентів у Національному банку із застосуванням електронних засобів приймання, оброблення, передавання та захисту інформації у файловому режимі або режимі реального часу. Функціонування СЕП забезпечується такими програмно-технічними комплексами:

ЦОСЕП - розміщений у Центральній розрахунковій палаті ЦОСЕП;

АРМ-СЕП - автоматизоване робоче місце учасника СЕП;

**система захисту електронних банківських документів** - сукупність методів та засобів, що включає апаратно-програмні, програмні засоби захисту, ключову інформацію та систему розподілу ключової інформації, технологічні засоби контролю та організаційні заходи щодо захисту інформації;

**система резервування і відновлення функціонування СЕП** - це процедури, програмно-технічні комплекси та компоненти програмного забезпечення СЕП, що призначені забезпечити функціонування СЕП у разі порушення функціонування програмно-технічних комплексів ЦОСЕП, АРМ-СЕП внаслідок фізичного пошкодження комп'ютерного та телекомунікаційного обладнання, каналів зв'язку, втрати або пошкодження баз даних тощо;

**технічний рахунок у ЦОСЕП** (далі - технічний рахунок) - інформація в електронній формі, що зберігається в ЦОСЕП, поновлюється під час оброблення міжбанківських електронних розрахункових документів і відображає стан кореспондентського рахунку учасника СЕП безпосереднього на певний час або обороти учасника СЕП безпосереднього, що не має кореспондентського рахунку, на певний час;

**учасник СЕП опосередкований** - філія банку, що не має технічного рахунку в ЦОСЕП і виконує міжбанківський переказ через СЕП з використанням ВМПС та АРМ-СЕП банку;

**файл СЕП** - одиниця обміну інформацією в СЕП у файловому режимі, що позначається однією літерою відповідно до технології роботи СЕП, зокрема:

A - файл, сформований засобами САБ відправника і надісланий до ЦОСЕП (файл початкових документів);

B - файл, сформований засобами ЦОСЕП і надісланий до САБ отримувача (файл відповідних документів);

L - інформація від САБ структурного підрозділу Національного банку про стан кореспондентських рахунків учасників СЕП та встановлення обмеження на їх роботу в СЕП;

**Центральна розрахункова палата Національного банку (ЦРП)** - структурна одиниця Національного банку, яка забезпечує функціонування СЕП.

### ЗАГАЛЬНІ ВИМОГИ ЩОДО ВИКОНАННЯ МІЖБАНКІВСЬКОГО ПЕРЕКАЗУ

Банки (філії) здійснюють міжбанківський переказ за міжбанківськими електронними розрахунковими документами, що формуються ними на підставі:

паперових розрахункових документів клієнтів;

паперових розрахункових документів банку (філії);

електронних розрахункових документів, отриманих засобами автоматизованих систем від клієнта - ініціатора переказу;

електронних розрахункових документів, отриманих засобами ВМПС від філії банку;

електронних розрахункових документів, автоматично сформованих САБ за умовами договорів або згідно з потребою банку (філії);

електронних розрахункових документів, отриманих засобами інших платіжних систем, телекомунікаційних систем, інших засобів зв'язку за умови забезпечення цілісності та конфіденційності інформації тощо.

Міжбанківський електронний розрахунковий документ має обов'язково містити реквізити документа, на підставі якого він сформований, а саме:

назву та номер;

дату складання (число, місяць, рік);

дату надходження до банку платника;

ознаку дебет/кредит;

суму;

код платника, назву платника, рахунок платника;

код банку платника;

код отримувача, назву отримувача, рахунок отримувача;

код банку отримувача;

призначення платежу.

Міжбанківський електронний розрахунковий документ має обов'язково містити електронний цифровий підпис (далі - ЕЦП) та технологічні реквізити (ідентифікатор ключа ЕЦП, відмітку про час оброблення документа тощо).

Міжбанківський переказ виконується банками в строк, визначений правилами платіжної системи, який не може перевищувати трьох операційних днів відповідно до Закону України "Про платіжні системи та переказ коштів в Україні".

Взаємовідносини в системі міжбанківських розрахунків між її учасниками регулюються договорами, укладеними відповідно до законодавства.

### ВИКОНАННЯ МІЖБАНКІВСЬКОГО ПЕРЕКАЗУ ЧЕРЕЗ КОРЕСПОНДЕНТСЬКІ РАХУНКИ, ЩО ВІДКРИВАЮТЬСЯ БАНКАМИ В НАЦІОНАЛЬНОМУ БАНКУ

Відкриття/закриття кореспондентського рахунку банку в Національному банку

Національний банк відкриває кореспондентський рахунок банку на підставі укладеного договору про кореспондентський рахунок у Національному банку України та за умови подання керівником банку, головним бухгалтером банку належним чином оформлених документів.

Підставою для закриття кореспондентського рахунку банку є розірвання договору, що здійснюється за заявою власника кореспондентського рахунку або за ініціативою Національного банку, або уповноваженої особи Фонду гарантування вкладів фізичних осіб у випадках, передбачених законодавством України.

У разі закриття кореспондентського рахунку банку залишок коштів за кореспондентським рахунком має бути перерахований на рахунок, визначений його власником або уповноваженою особою Фонду гарантування вкладів фізичних осіб відповідно до законодавства України.

### ЕЛЕКТРОННИЙ ТЕХНОЛОГІЧНИЙ ДОВІДНИК БАНКІВ УКРАЇНИ ТА ІНШИХ УСТАНОВ

Департамент інформаційних технологій формує Електронний технологічний довідник банків України та інших установ на підставі інформації, що міститься в електронній формі Державного реєстру банків (далі - електронний реєстр).

Електронний технологічний довідник банків України та інших установ має обов'язково містити такі реквізити:

"назва банку (технологічна)" - зазначається найменування банку (філії), яке за потреби може скорочуватися [за умови, що в скороченому найменуванні міститиметься інформація, достатня для однозначної ідентифікації банку (філії)]. Банк (філія) використовує цей реквізит у разі роздрукування міжбанківського електронного розрахункового документа засобами САБ;

"адреса електронної пошти в мережі Інтернет АРМ-СЕП" і "адреса електронної пошти в мережі Інтернет АРМ-СЕП-інформаційного" - призначені для забезпечення безперервного функціонування АРМ-СЕП і АРМ-СЕП-інформаційного в разі виникнення надзвичайних ситуацій.

Центральна розрахункова палата наприкінці кожного робочого дня розсилає оновлену версію Електронного технологічного довідника банків України та інших установ по всій інформаційній мережі засобами системи електронної пошти Національного банку (далі - система ЕП).

Необхідною умовою для виключення банку (філії) з Довідника учасників СЕП є розірвання договору про розрахунково-інформаційне обслуговування в системі електронних платежів Національного банку України та надання послуг системою електронної пошти Національного банку України.

Структурний підрозділ Національного банку інформує засобами системи ЕП Департамент безпеки про ініціювання банком (філією) унесення інформації до Довідника учасників СЕП.

ЦРП зобов'язана внести зміни до Довідника учасників СЕП згідно з отриманим від структурного підрозділу Національного банку повідомленням і надіслати їх учасникам СЕП наприкінці робочого дня, що передує дню, з якого зміни набирають чинності.

Учасники СЕП зобов'язані внести зміни до Довідника учасників СЕП після закінчення банківського дня, у якому надійшла ця інформація, але до початку наступного банківського дня на всіх робочих місцях САБ, де використовується цей довідник.

ЦРП вносить інформацію до Довідника учасників СЕП щодо включення нового учасника СЕП (безпосереднього) або зміни ідентифікатора учасника СЕП (безпосереднього) за умови, що цей учасник надіслав відкриті ключі АРМ-СЕП на сертифікацію до 13 години дня, що передує дню внесення інформації до Довідника учасників СЕП.

ЦРП зобов'язана на початку першого банківського дня після включення банку до Довідника учасників СЕП засобами ЦОСЕП привести значення технічного рахунку банку (філії) у відповідність до стану його кореспондентського рахунку на підставі файла L.00, отриманого від відповідного структурного підрозділу Національного банку. Після цього банк може здійснювати міжбанківський переказ через СЕП.

Під час виключення з учасників СЕП банку значення його технічного рахунку має дорівнювати нулю. Банк для виконання цієї вимоги наприкінці останнього робочого дня в СЕП після виконання вимоги пункту 10 цієї глави зобов'язаний перерахувати засобами СЕП суму коштів, що дорівнює залишку на його технічному рахунку, на рахунок, визначений у договорі.

### ЗАГАЛЬНІ УМОВИ ФУНКЦІОНУВАННЯ СЕП ЩОДО ПРОВЕДЕННЯ МІЖБАНКІВСЬКОГО ПЕРЕКАЗУ

Національний банк визначає технологію роботи СЕП, має право змінювати технологічну структуру цієї системи та шляхи програмно-технічної реалізації її компонентів і вимагати від учасників СЕП відповідної адаптації їх програмно-технічних засобів САБ та ВМПС до технології роботи СЕП. Строк інформування учасників СЕП про внесення змін до програмно-технічного забезпечення визначається Національним банком і не може бути меншим, ніж за п'ять робочих днів до часу їх унесення. Зміна програмно-технічних засобів і технології роботи СЕП відбувається за вказівками Національного банку.

Технологічний регламент роботи СЕП визначається Національним банком і надсилається засобами системи ЕП усім учасникам СЕП для виконання.

Учасник СЕП забезпечує формування, передавання, приймання міжбанківських електронних розрахункових документів, службових повідомлень СЕП та електронних розрахункових повідомлень з використанням апаратно-програмних засобів криптографічного захисту інформації відповідно до нормативно-правового акта Національного банку з питань інформаційної безпеки.

ЦОСЕП здійснює оброблення міжбанківських електронних розрахункових документів, службових повідомлень СЕП та електронних розрахункових повідомлень у порядку їх надходження до СЕП. Міжбанківський електронний розрахунковий документ, прийнятий СЕП, не може бути відкликаний. Результати оброблення міжбанківських електронних розрахункових документів у СЕП відображаються на технічному рахунку банку (філії).

Початкові платежі від банку (філії) приймаються в межах поточного значення його технічного рахунку.

Міжбанківський електронний розрахунковий документ уважається виконаним у СЕП з часу відображення його суми за технічним рахунком учасника СЕП-отримувача, за винятком випадків, передбачених процедурою відновлення функціонування СЕП у разі порушення її роботи або виникнення надзвичайних ситуацій.

У кінці банківського дня ЦОСЕП передає до структурного підрозділу Національного банку інформацію про розрахунки, що здійснені через СЕП, для їх відображення на кореспондентських рахунках учасників СЕП та інших рахунках у САБ структурного підрозділу Національного банку.

Кожний учасник СЕП веде журнал обліку встановлення та заміни програмно-технічних засобів, що використовуються для роботи в СЕП, у якому зазначаються дата та час їх установлення (заміни), а також компоненти, що замінюються, їх назва, підстава для заміни, нова версія, прізвище, ініціали та підпис виконавця.

Обов'язковій реєстрації в журналі підлягають установлення та заміна таких компонентів:

прикладного програмного забезпечення СЕП, системи ЕП;

комп'ютера та його компонентів;

мережевої плати та/або мережевого клієнта;

системного програмного забезпечення;

апаратних засобів захисту інформації, а також настройка комп'ютера.

Кожен учасник СЕП зобов'язаний забезпечити наявність внутрішнього документа, що регламентує порядок відновлення роботи в СЕП у разі порушення роботи в системі або виникнення надзвичайних ситуацій та його виконання.

Якщо учасник СЕП порушує технологію роботи, не виконує вимоги щодо захисту банківської інформації, то Національний банк має право зупинити початкові платежі цього учасника в СЕП. Учасник СЕП продовжує роботу в системі після службового розслідування, проведеного Національним банком у максимально короткий строк. Учасник СЕП зобов'язаний усунути недоліки, виявлені під час проведення службового розслідування.

Учасник СЕП має забезпечити створення шифрованого архіву оброблених платежів і технологічної інформації.

Учасник СЕП має право на підставі файла-запиту ІПС одержувати інформацію про проходження сформованих ним міжбанківських електронних розрахункових документів. Відповідь на запит ІПС надає протягом одного робочого дня, не враховуючи день отримання запиту.

### 

### ФУНКЦІОНУВАННЯ СЕП У ФАЙЛОВОМУ РЕЖИМІ

ЦОСЕП на початку банківського дня отримує від САБ структурного підрозділу Національного банку файл L.00 і на його підставі перевіряє відповідність значень технічних рахунків учасників СЕП стану їх кореспондентських рахунків та в разі потреби приводить значення технічних рахунків у ЦОСЕП у відповідність до значень кореспондентських рахунків у файлі L.00. Від ЦОСЕП інформація про стан технічних рахунків надсилається їх власникам.

Обмін файлами через СЕП здійснюється засобами системи ЕП.

Оброблення файлів у СЕП здійснюється в циклічному режимі. Цикл оброблення файлів складається з двох частин:

приймання інформації;

передавання інформації.

Під час приймання інформації ЦОСЕП отримує від учасника СЕП файл A і перевіряє його на відповідність вимогам СЕП.

ЦОСЕП надсилає за результатами оброблення файла A на адресу відправника квитанцію про результати його приймання. ЦОСЕП приймає або не приймає файл A у цілому. Відправник файла A несе відповідальність за склад міжбанківських електронних розрахункових документів, уключених до цього файла.

Під час передавання інформації міжбанківські електронні розрахункові документи, прийняті ЦОСЕП у файловому режимі, групуються за адресами і надсилаються отримувачам (зокрема файли B).

Файл B уважається одержаним і його сума відображається за технічним рахунком отримувача в ЦОСЕП за умови надходження від отримувача квитанції, що підтверджує успішне прийняття файла B.

У кінці банківського дня ЦОСЕП надає учасникам СЕП інформацію про стан їх технічних рахунків на початок і кінець банківського дня, а також перелік усіх міжбанківських електронних розрахункових документів, що оброблялися ними протягом цього дня.

Необхідною умовою завершення банківського дня учасником СЕП є:

надання інформації за підсумками банківського дня до ЦОСЕП, якщо інше не передбачено регламентом роботи СЕП;

звіряння інформації САБ з даними ЦОСЕП;

відображення на рахунках у САБ у цей банківський день міжбанківських електронних розрахункових документів, здійснених у режимі реального часу, що надійшли від ЦОСЕП у підсумкових файлах дня.

Суми міжбанківських електронних розрахункових документів, здійснених у файловому режимі, що не були підтверджені отримувачем за станом на кінець банківського дня, мають обліковуватися на транзитних рахунках структурного підрозділу Національного банку.

### 

### ФУНКЦІОНУВАННЯ СЕП У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Учасник СЕП у режимі реального часу має право:

а) виконувати міжбанківські перекази;

б) установлювати в ЦОСЕП ліміти технічних рахунків, початкових оборотів підпорядкованих йому філій;

в) одержувати довідкову інформацію про:

стан власного технічного рахунку і про стан технічних рахунків своїх філій;

власні міжбанківські перекази;

міжбанківські перекази своїх філій тощо.

Структурний підрозділ Національного банку має право в режимі реального часу встановлювати обмеження щодо виконання початкових платежів банку відповідно до нормативно-правових актів Національного банку.

Обмін інформацією в режимі реального часу здійснюється пакетами за протоколом TCP/IP.

Учасник СЕП формує засобами САБ пакет-запит і надсилає його до ЦОСЕП. За підсумками оброблення пакета-запиту ЦОСЕП готує та відправляє учаснику СЕП пакет-відповідь, що містить інформацію про виконання чи невиконання пакета-запиту.

### 

### МОДЕЛІ ОБСЛУГОВУВАННЯ КОНСОЛІДОВАНОГО КОРЕСПОНДЕНТСЬКОГО РАХУНКУ В СЕП

Банк та його філії мають право працювати в СЕП з використанням відповідної моделі обслуговування консолідованого кореспондентського рахунку.

У разі роботи за моделлю 3 банк зобов'язаний мати консолідований кореспондентський рахунок у структурному підрозділі Національного банку і технічний рахунок у ЦОСЕП. Філії банку не можуть мати технічних рахунків у ЦОСЕП. Банк повинен мати власну ВМПС для виконання внутрішньобанківського переказу.

Філії банку є опосередкованими учасниками СЕП і обмінюються міжбанківськими електронними розрахунковими документами з СЕП засобами ВМПС через АРМ-СЕП банку з відображенням результатів розрахунків на технічному рахунку банку.

У разі роботи за моделлю 4 банк зобов'язаний мати консолідований кореспондентський рахунок у структурному підрозділі Національного банку і технічний рахунок у ЦОСЕП. Його філії мають технічні рахунки в ЦОСЕП.

Банк і філії зобов'язані мати програмно-технічні комплекси АРМ-СЕП, засоби захисту інформації СЕП, обмінюватися міжбанківськими електронними розрахунковими документами із СЕП незалежно один від одного. Розрахунки філії мають відображатися на технічних рахунках філії та банку.

Банк має право протягом операційного дня встановлювати ліміти технічних рахунків і початкових оборотів філій, отримувати від СЕП підсумкову технологічну інформацію про їх роботу.

У разі роботи за моделлю 7 банк зобов'язаний мати консолідований кореспондентський рахунок у структурному підрозділі Національного банку і технічний рахунок в ЦОСЕП. Його філії мають технічні рахунки в ЦОСЕП.

Банк та філії зобов'язані мати програмно-технічні комплекси АРМ-СЕП, засоби захисту інформації СЕП, обмінюватися міжбанківськими електронними розрахунковими документами із СЕП незалежно один від одного. Розрахунки філії мають відображатися на технічних рахунках філії та банку.

Банк має право протягом операційного дня встановлювати ліміти технічних рахунків і початкових оборотів філій, виконувати початкові платежі від їх імені та отримувати від СЕП підсумкову технологічну інформацію про їх роботу, а також обмежувати повноваження філій щодо виконання розрахункових та інших операцій за допомогою операційних правил САБ.

Під час роботи за моделлю 7 банк має право використовувати програмно-технічні засоби, що забезпечують обмін внутрішньобанківськими повідомленнями між ним та його філіями без виходу в СЕП. Структура і зміст внутрішньобанківських повідомлень визначаються банком.

У разі роботи за моделлю 8 банк зобов'язаний мати консолідований кореспондентський рахунок у структурному підрозділі Національного банку і технічний рахунок у ЦОСЕП. Його філії мають технічні рахунки в ЦОСЕП.

Банк і філії зобов'язані мати програмно-технічні комплекси АРМ-СЕП, засоби захисту інформації СЕП, обмінюватися міжбанківськими електронними розрахунковими документами із СЕП незалежно один від одного. Розрахунки філії мають відображатися на технічних рахунках філії та банку. Банк має право протягом операційного дня встановлювати ліміти технічних рахунків і початкових оборотів філій.

СЕП надає банку технологічну інформацію про роботу філій та обороти за їх технічними рахунками лише за підсумками банківського дня, але банк може отримувати технологічну інформацію про роботу філій протягом банківського дня в режимі реального часу.

2. Для одержання дозволу банк подає до Національного банку (на ім'я посадової особи, до обов'язків якої належить регулювання питань щодо функціонування СЕП) викладені державною мовою документи, що підтверджують організаційну, функціональну та технологічну готовність банку до роботи в СЕП за відповідною моделлю, а саме:

У разі використання банком під час роботи за моделлю 7 внутрішньобанківських повідомлень, якими обмінюються банк і його філії без виходу в СЕП, у правилах здійснення банком та його філіями переказу коштів за моделлю 7 має бути опис структури, змісту цих повідомлень і порядок їх захисту від підроблення та викривлення.

Національний банк у місячний строк із дня отримання від банку документів, що мають відповідати вимогам пунктів 2 - 4 цієї глави, може надати йому дозвіл на роботу в СЕП за відповідною моделлю або в разі невідповідності правил вимогам цієї глави відмовити в наданні дозволу.

Банк у разі потреби заміни діючого програмного забезпечення та/або системи захисту інформації на програмний продукт іншого розробника або на нову версію програмного продукту того самого розробника подає документи згідно з пунктами 2 - 4 цієї глави для отримання на це дозволу Національного банку. У разі надання банку дозволу попередній дозвіл втрачає чинність з дня переходу банку на роботу з використанням програмного продукту іншого розробника або нової версії програмного продукту того самого розробника.

### 

### ЗАГАЛЬНІ УМОВИ ВЕДЕННЯ УЧАСНИКАМИ СЕП АРХІВУ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ДОКУМЕНТІВ

Банки та їх філії, структурні підрозділи Національного банку, ЦРП (далі в тексті - учасники СЕП) кожного робочого дня формують на зовнішніх носіях, придатних для тривалого зберігання та зчитування інформації (далі - зовнішні носії), архів електронних міжбанківських документів для забезпечення довгострокового зберігання цієї інформації для оперативного її використання у випадках, визначених законодавством та технологією функціонування СЕП.

Архів електронних міжбанківських документів має зберігатися на зовнішніх носіях у формі, що дає змогу перевірити цілісність електронних міжбанківських документів на цих носіях.

2. Архів електронних міжбанківських документів має, зокрема, містити:

а) на рівні банків та їх філій:

усі відправлені та отримані міжбанківські електронні розрахункові документи та електронні розрахункові повідомлення;

протокол роботи САБ;

архів системи ЕП;

архів АРМ-СЕП (шифровані арбітражні журнали апаратного і програмного шифрування та захищений від модифікації протокол роботи АРМ-СЕП);

б) на рівні структурних підрозділів Національного банку:

протокол роботи САБ;

архів АРМ-СЕП (шифровані арбітражні журнали апаратного і програмного шифрування та захищений від модифікації протокол роботи АРМ-СЕП);

в) на рівні ЦРП:

протокол роботи САБ;

архів АРМ-СЕП (шифровані арбітражні журнали апаратного і програмного шифрування та захищений від модифікації протокол роботи АРМ-СЕП);

повний архів роботи ЦОСЕП;

архів баз даних ІПС;

архів системи ЕП.

Архів електронних міжбанківських документів має формуватися згідно із затвердженою номенклатурою справ учасника СЕП, створюватися у відповідних структурних підрозділах, переноситися на електронні носії з метою подальшого зберігання в цьому підрозділі або передаватися для зберігання до відповідного уповноваженого структурного підрозділу.

Архів електронних міжбанківських документів має зберігатися відповідно до нормативно-правового акта Національного банку щодо порядку формування, зберігання та знищення електронних архівів.

Доступ до архіву повинні мати посадові особи, які згідно з наказом керівника установи призначені для роботи з архівом.

Строки зберігання архівів електронних міжбанківських документів установлюються нормативно-правовим актом Національного банку, що визначає перелік документів, що утворюються в діяльності Національного банку та банків України.

Інформацію на електронних носіях, строки зберігання якої закінчилися, учасники СЕП мають знищувати на підставі оформлених належним чином актів. Електронні носії, на яких зберігалася інформація, можуть використовуватися повторно залежно від їх стану, який визначається згідно з паспортним строком експлуатації. Інформацію, строки зберігання якої перевищують паспортний строк експлуатації електронного носія, на якому вона розміщена, учасник СЕП має перенести на інший електронний носій з обов'язковим виконанням перевірки її цілісності на цьому носії.

### 

### ЗАГАЛЬНІ УМОВИ ВИКОНАННЯ МІЖБАНКІВСЬКОГО ПЕРЕКАЗУ ЧЕРЕЗ КОРЕСПОНДЕНТСЬКІ РАХУНКИ, ЩО ВІДКРИВАЮТЬСЯ БАНКАМИ В РОЗРАХУНКОВОМУ БАНКУ ПЛАТІЖНОЇ СИСТЕМИ

Переказ коштів через кореспондентські рахунки банків - членів платіжної системи в розрахунковому банку може виконуватися на підставі клірингової вимоги, сформованої в платіжній системі за результатами взаємозаліку на підставі клірингу або за кожним документом на переказ коштів окремо.

Для зведення результатів клірингу на балансі розрахункового банку відкривається кліринговий рахунок.

Функції розрахункового банку визначаються внутрішнім положенням банку, що регулює проведення міжбанківського переказу з урахуванням вимог законодавства та правил платіжної системи і, зокрема, має визначати:

технологію, регламент проведення розрахунків і порядок обміну інформацією з учасниками розрахунків;

порядок урегулювання неплатоспроможності та інших випадків невиконання членами платіжної системи своїх зобов'язань;

порядок формування та умови використання страхового фонду з покриття ризиків неплатежів членів платіжної системи (далі - страховий фонд), якщо відповідно до договору з платіжною організацією розрахунковий банк здійснює облік і контроль за формуванням членами платіжної системи страхового фонду.

У разі надання платіжною організацією розрахунковому банку повноважень здійснювати контроль за формуванням членами платіжної системи коштів страхового фонду їх облік і використання здійснюються відповідно до нормативно-правових актів Національного банку та умов договорів з платіжною організацією та членами платіжної системи.

Рішення щодо виконання функцій розрахункового банку приймається Національним банком на підставі розгляду документів, що подаються від імені платіжної організації платіжної системи, а саме:

письмового звернення платіжної організації платіжної системи щодо укладення договору про виконання Національним банком функцій розрахункового банку цієї платіжної системи;

загальних відомостей про платіжну систему, зокрема щодо платіжної організації та клірингової установи, що уповноважена платіжною організацією виконувати кліринг;

опису технології функціонування платіжної системи;

переліку її членів;

видів платіжних інструментів;

способів покриття можливих ризиків та управління безпекою в системі.

Національний банк має право отримати від платіжної організації додаткову інформацію, потрібну для прийняття остаточного рішення.

ВМПС має використовувати програмно-технічне забезпечення, систему захисту інформації та телекомунікаційні канали зв'язку, що забезпечують:

а) надійний багаторівневий захист інформації від несанкціонованого доступу, використання, модифікації на різних етапах її формування, оброблення, передавання та приймання;

б) контроль за достовірністю інформації на всіх етапах її оброблення;

в) процедури та механізми, які після збоїв чи інших порушень роботи ВМПС дають змогу відновити роботу без послаблення вимог щодо захисту інформації;

г) фіксування спроб несанкціонованого доступу до системи розрахунків (з негайним інформуванням про це банком - власником ВМПС Національного банку);

ґ) автоматичне ведення протоколу найкритичніших моментів роботи (вхід, формування міжбанківських електронних розрахункових документів тощо) та забезпечення його захисту від модифікації, формування архіву цього протоколу під час закриття робочого дня;

д) формування і зберігання архівів електронних банківських документів відповідно до вимог законодавства;

е) надійне резервування для підтримки безперебійного функціонування ВМПС і відновлення її діяльності в разі порушення її роботи або виникнення надзвичайних ситуацій.

Транспортні потреби ВМПС забезпечуються засобами системи ЕП або власними чи загального користування засобами телекомунікації тощо. Програмні засоби вузла системи ЕП передаються банку та філії на підставі договору про надання послуг системою електронної пошти Національного банку України.

## ПОРЯДОК РЕЗЕРВУВАННЯ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ СЕП

### **ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ РЕЗЕРВУВАННЯ СЕП**

Для підтримання системи резервування СЕП у належному стані Департамент інформаційних технологій, Департамент безпеки, ЦРП, учасники СЕП зобов'язані виконувати підготовчі роботи, перелік яких наведений далі.

Департамент інформаційних технологій зобов'язаний вести довідник оповіщення учасників СЕП (далі - довідник оповіщення), у якому зазначені контактні телефони, у тому числі стільникового зв'язку, та адреси електронної пошти, що використовуються Національним банком для оповіщення учасників СЕП у разі порушення роботи ЦОСЕП або виникнення надзвичайних ситуацій. ЦРП має надавати Департаменту інформаційних технологій інформацію для внесення змін до довідника оповіщення. Учасник СЕП зобов'язаний на запит Департаменту інформаційних технологій, ЦРП повідомити реквізити, за якими проводитиметься оповіщення, для включення цих реквізитів до довідника оповіщення. Учасник СЕП має протягом трьох робочих днів повідомити ЦРП про зміни реквізитів довідника оповіщення.

Збереження баз даних ЦОСЕП та іншої інформації СЕП, потрібної для безперебійного її функціонування, забезпечується шляхом використання двох центрів зберігання даних інформаційної мережі, географічно віддалених один від одного, які мають забезпечувати резервування один одного.

Департамент інформаційних технологій розробляє, погоджує з ЦРП, Департаментом безпеки і надає учасникам СЕП технологічну документацію щодо відновлення роботи ЦОСЕП. У разі відновлення функціонування СЕП її учасники мають дотримуватися вимог технологічної документації, розпоряджень ЦРП, Департаменту інформаційних технологій і Департаменту безпеки. Департамент безпеки підтримує систему захисту СЕП для її використання під час відновлення функціонування ЦОСЕП згідно з технологічною документацією. Національний банк забезпечує потрібну кількість комп'ютерного обладнання для відновлення роботи ЦОСЕП.

Усі працівники, які беруть участь в обробленні електронних платежів, мають бути ознайомлені з порядком резервування та відновлення функціонування СЕП і технологічною документацією щодо відновлення роботи ЦОСЕП.

Учасник СЕП зобов'язаний забезпечити належний рівень резервування загальносистемних і програмно-технічних комплексів, необхідних для забезпечення його роботи в СЕП, відповідного серверного та телекомунікаційного обладнання, систем електроживлення, кондиціонування, каналів зв'язку та підтримку схем швидкого відновлення їх функціонування.

### РІВНІ РЕЗЕРВУВАННЯ ЦОСЕП

1. Резервування ЦОСЕП залежно від ступеня та локалізації порушення його функціонування здійснюється за трьома рівнями:

перший рівень - резервування з метою відновлення роботи ЦОСЕП у ЦРП за умови, що бази даних ЦОСЕП не пошкоджені;

другий рівень - резервування з метою відновлення роботи ЦОСЕП в іншій будівлі Національного банку в місті Києві (далі - інша будівля) за умови, що бази даних ЦОСЕП не пошкоджені;

третій рівень - резервування з метою відновлення роботи ЦОСЕП або в ЦРП, або в іншій будівлі, або у віддаленому резервному пункті за умови, що бази даних ЦОСЕП утрачені або пошкоджені.

Рішення про відновлення функціонування ЦОСЕП за схемою першого рівня приймається в ЦРП відповідальною особою, до функціональних обов'язків якої належить обґрунтування рішення про неможливість функціонування ЦОСЕП та про необхідність відновлення його функціонування, або особами, до функціональних обов'язків яких належить приймання такого рішення в разі відсутності відповідальної особи.

Рішення про відновлення функціонування ЦОСЕП за схемою другого або третього рівня приймається посадовою особою Національного банку, до обов'язків якої належить регулювання питань щодо функціонування СЕП.

Якщо для відновлення функціонування ЦОСЕП недостатньо заходів, що передбачені цим розділом, то Департамент інформаційних технологій розробляє потрібні заходи відповідно до ситуації, що склалася, та узгоджує їх з ЦРП і Департаментом безпеки.

Відновлення функціонування ЦОСЕП за другим або третім рівнем може бути викликано перешкодами у функціонуванні вузла інформаційної мережі в ЦРП, у тому числі головного вузла системи ЕП. У цьому разі одночасно з відновленням функціонування ЦОСЕП учасники СЕП зобов'язані вносити зміни до організації їх роботи з інформаційною мережею відповідно до вимог нормативно-правових актів Національного банку з питань забезпечення безперервного функціонування інформаційних систем Національного банку та банків України.

У разі відновлення функціонування ЦОСЕП за другим або третім рівнем резервування надання інформації засобами ІПС щодо проходження міжбанківських електронних розрахункових документів припиняється до повного відновлення функціонування ЦОСЕП.

### 

### ВИКОРИСТАННЯ ПЕРШОГО РІВНЯ РЕЗЕРВУВАННЯ

Відновлення функціонування ЦОСЕП за першим рівнем резервування застосовується в разі виходу з ладу або пошкодження сервера бази даних (на якому функціонує система управління базами даних), серверів застосувань, робочих станцій ЦОСЕП або повної чи часткової втрати інформації, що зберігається в них, за умови збереження баз даних ЦОСЕП.

Перший рівень резервування ЦОСЕП забезпечується в ЦРП на резервному комп'ютерному обладнанні, на якому встановлено відповідне програмне забезпечення ЦОСЕП і резервні апаратно-програмні засоби захисту інформації, що дублюють основні засоби захисту ЦОСЕП. Параметри настроювання резервного комп'ютерного обладнання мають відповідати параметрам настроювання основного комп'ютерного обладнання, на якому функціонують відповідні складові ЦОСЕП.

У разі неможливості функціонування одного чи кількох комп'ютерів, на яких установлено компоненти програмного забезпечення ЦОСЕП, забезпечується переведення ЦОСЕП на резервне комп'ютерне обладнання. На час виконання цих дій функціонування ЦОСЕП може бути зупинено, про що ЦРП надсилає учасникам СЕП повідомлення засобами системи ЕП. 4. Після відновлення функціонування ЦОСЕП ЦРП надсилає учасникам СЕП інформаційне повідомлення від ЦОСЕП про роботу СЕП у штатному режимі.

Учасникам СЕП уживати додаткових заходів для переналагодження своєї роботи в СЕП не потрібно.

### 

### ВИКОРИСТАННЯ ДРУГОГО РІВНЯ РЕЗЕРВУВАННЯ

Відновлення функціонування ЦОСЕП за другим рівнем резервування застосовується в разі пошкодження або знищення інформації, руйнування обладнання чи будівлі ЦРП, коли в строк до шести годин неможливо відновити функціонування ЦОСЕП у ЦРП. Відновлення функціонування ЦОСЕП здійснюється в іншій будівлі.

Другий рівень резервування ЦОСЕП забезпечується в іншій будівлі на резервному комп'ютерному обладнанні, на якому встановлено відповідне програмне забезпечення ЦОСЕП і резервні програмні засоби криптографічного захисту інформації, що дублюють основні засоби захисту ЦОСЕП. Параметри настроювання резервного комп'ютерного обладнання мають відповідати параметрам настроювання основного комп'ютерного обладнання, на якому функціонують відповідні складові ЦОСЕП.

Департамент інформаційних технологій для відновлення функціонування ЦОСЕП за другим рівнем резервування засобами системи ЕП або засобами оповіщення зобов'язує учасників СЕП зупинити функціонування АРМ-СЕП. Учасники СЕП зупиняють функціонування АРМ-СЕП до отримання подальших розпоряджень від Департаменту інформаційних технологій.

Якщо відновити функціонування ЦОСЕП з використанням апаратних засобів криптографічного захисту інформації неможливо, то ЦОСЕП і учасники СЕП переводяться на використання програмних засобів захисту інформації.

Після відновлення функціонування ЦОСЕП у іншій будівлі ЦРП надсилає учасникам СЕП засобами системи ЕП інформаційне повідомлення про відновлення роботи за другим рівнем резервування.

Відновлення роботи ЦОСЕП у ЦРП має розпочинатися після закінчення одного банківського дня та до початку наступного банківського дня. ЦРП надсилає учасникам СЕП інформаційне повідомлення від ЦОСЕП про відновлення роботи ЦОСЕП у ЦРП.

### 

### ВИКОРИСТАННЯ ТРЕТЬОГО РІВНЯ РЕЗЕРВУВАННЯ

Відновлення функціонування ЦОСЕП з використанням третього рівня резервування застосовується в разі пошкодження або знищення інформації, обладнання чи будівлі в ЦРП і іншої будівлі з втратою інформації бази даних ЦОСЕП. Таке відновлення передбачає забезпечення функціонування ЦОСЕП або в ЦРП, або в іншій будівлі, або у віддаленому резервному пункті з використанням відновлених з мінімальною втратою інформації баз даних ЦОСЕП.

Пошкодження зазначеного рівня можуть бути підставою для тимчасового зупинення обслуговування учасників СЕП. Залежно від рівня пошкоджень Національний банк може оголосити про настання форс-мажорних обставин відповідно до умов договорів з учасниками СЕП.

Для відновлення функціонування ЦОСЕП за третім рівнем резервування ЦОСЕП формує і відправляє до іншої будівлі та/або до віддаленого резервного пункту файли, які містять:

за підсумками кожного банківського дня - нормативно-довідкову інформацію (Довідник учасників СЕП тощо), інформацію про стан технічних рахунків учасників СЕП тощо;

за підсумками кожного циклу оброблення інформації - інформацію про оброблені протягом циклу платежі та технологічну інформацію, потрібну для відновлення роботи ЦОСЕП.

ЦРП або Департамент інформаційних технологій засобами системи ЕП або засобами оповіщення зобов'язує учасників СЕП зупинити функціонування АРМ-СЕП у зв'язку з відновленням роботи ЦОСЕП за третім рівнем резервування. Учасники СЕП зупиняють функціонування АРМ-СЕП до отримання подальших розпоряджень від ЦРП або Департаменту інформаційних технологій.

ЦРП або віддалений резервний пункт у разі відновлення роботи ЦОСЕП у ньому виконує відновлення баз даних ЦОСЕП. Якщо пошкодження ЦОСЕП відбулося між банківськими днями, то робочий день у СЕП після відновлення функціонування ЦОСЕП розпочинається у звичайному режимі. 6. Якщо пошкодження ЦОСЕП відбулося протягом банківського дня, то під час відновлення його функціонування може бути втрачена інформація про міжбанківські електронні розрахункові документи, що була оброблена ЦОСЕП протягом циклу, у якому відбулося пошкодження.

Після завершення відновлення функціонування ЦОСЕП його робота продовжується за місцем відновлення. Департамент інформаційних технологій та ЦРП визначають технологічні особливості функціонування СЕП і засобами системи ЕП надсилають учасникам СЕП інформаційне повідомлення про:

відновлення роботи СЕП;

особливості продовження функціонування СЕП.

У разі відновлення роботи ЦОСЕП у віддаленому резервному пункті учасники СЕП змінюють параметри настроювання АРМ-СЕП у зв'язку зі зміною місцезнаходження ЦОСЕП.

Подальші зміни щодо функціонування СЕП та її технологічний регламент визначаються посадовою особою Національного банку, до обов'язків якої належить регулювання питань щодо функціонування СЕП, і доводяться до відома учасників СЕП.

Якщо пошкодження ЦОСЕП відбулося протягом банківського дня, то після відновлення баз даних ЦОСЕП учасникам СЕП надсилається технологічна інформація про відновлені файли, пакети електронних розрахункових документів та інформаційних повідомлень і відновлену службову інформацію СЕП із зазначенням номера сеансу, до якого (уключно) була відновлена інформація. На підставі цієї інформації учасники СЕП зобов'язані вжити заходів щодо з'ясування стану з відправленими та прийнятими ними (до пошкодження ЦОСЕП) міжбанківськими електронними розрахунковими документами, інформаційними повідомленнями та службовими повідомленнями СЕП.

Усі розрахункові документи та електронні розрахункові повідомлення, що надійшли учасникові СЕП у файловому режимі та в режимі реального часу і не були відновлені в ЦОСЕП, слід вилучити із САБ з відповідним виправленням проводок, що були виконані в САБ.

Квитанції, що були сформовані на файли B та відправлені, - нічні та з номерами сеансу від 1 до номера сеансу, до якого (уключно) була відновлена інформація, слід повторно відправити до ЦОСЕП.

Файли A і пакети-запити, які цього банківського дня були відправлені до ЦОСЕП, але не відображені в переліку відновленої інформації, слід отримати з архівів САБ у сформованому вигляді (не переформовувати і не змінювати їх найменування) і відправити до ЦОСЕП. Одержуючи квитанції на ці файли (пакети-запити), слід переконатися, що стан проходження файлів у САБ відповідає стану їх проходження в СЕП. Якщо неможливо повторно відправити ці файли (пакети-запити), то платежам, що містилися в цих файлах (пакетах-запитах), слід надати статус невідправлених до СЕП та внести відповідні виправлення в бухгалтерські проводки, що були виконані за цими платежами.

Банк, який керує філіями за допомогою встановлення лімітів, має проаналізувати поточний стан лімітів і в разі потреби встановити нові їх значення.

Учасник СЕП має привести зміст бази даних САБ у відповідність до стану технічного рахунку в ЦОСЕП.

Якщо відновлення функціонування ЦОСЕП за третім рівнем резервування здійснювалося в іншій будівлі або у віддаленому резервному пункті, то відновлення роботи ЦОСЕП у ЦРП має розпочинатися після закінчення одного банківського дня та до початку наступного банківського дня. ЦРП надсилає учасникам СЕП інформаційне повідомлення від ЦОСЕП про відновлення роботи ЦОСЕП у ЦРП.

Використання резервних засобів криптографічного захисту інформації ЦОСЕП

У ЦРП і іншій будівлі забезпечується наявність і підтримання в актуальному стані достатньої кількості резервних програмних та апаратно-програмних засобів захисту інформації, а також відповідної ключової інформації.

У разі пошкодження апаратно-програмних засобів захисту інформації апаратура, що вийшла з ладу, замінюється на резервну і функціонування відповідної складової ЦОСЕП продовжується без її переналагодження. Учасникам СЕП уживати додаткових заходів для переналагодження своєї роботи в СЕП не потрібно.

У разі пошкодження апаратно-програмних засобів захисту інформації, за якого унеможливлюється використання апаратури захисту взагалі, функціонування ЦОСЕП відновлюється з використанням програмних засобів криптографічного захисту. Усім учасникам СЕП надсилається інформаційне повідомлення від ЦОСЕП, а також засобами системи ЕП про потребу налагодження АРМ-СЕП на роботу з використанням програмних засобів захисту.

Повернення ЦОСЕП до роботи з апаратно-програмними засобами захисту інформації здійснюється лише після закінчення одного банківського дня та до початку наступного банківського дня. Учасникам СЕП надсилається інформаційне повідомлення від ЦОСЕП про потребу налагодження АРМ-СЕП на той засіб криптографічного захисту, який використовувався ними до переходу ЦОСЕП на використання програмного захисту.

### 

### ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ АРМ-СЕП

Учасник СЕП зобов'язаний мати резервний комп'ютер для забезпечення роботи АРМ-СЕП у разі виходу з ладу основного комп'ютера, на якому розгорнута діюча версія АРМ-СЕП, з актуальними таблицями відкритих ключів, файлами конфігурації та допоміжними файлами.

У разі пошкодження комп'ютера, на якому функціонує АРМ-СЕП, учасник СЕП має підключити до резервного комп'ютера апаратуру захисту інформації і продовжувати функціонування АРМ-СЕП на резервному комп'ютері.

Учасник СЕП має зробити копію шифрованого архіву АРМ-СЕП з пошкодженого комп'ютера, якщо рівень пошкодження дає змогу це зробити, і зберігати її надалі разом з архівом банківського дня, що створюватиметься АРМ-СЕП на резервному комп'ютері.

Учасник СЕП зобов'язаний засобами системи ЕП повідомити Департамент безпеки Національного банку про відновлення функціонування АРМ-СЕП на резервному комп'ютері.

У разі виходу з ладу апаратури криптографічного захисту інформації учасник СЕП має надіслати до ЦРП засобами системи ЕП повідомлення про переведення його на роботу в програмному режимі криптографічного захисту. Отримавши таке повідомлення від учасника СЕП, ЦРП засобами ЦОСЕП установлює відповідні параметри роботи ЦОСЕП з цим учасником. Учасник СЕП установлює відповідні параметри роботи АРМ-СЕП.

Файли, що були сформовані в ЦРП для учасника СЕП з використанням апаратури криптографічного захисту інформації, за клопотанням учасника СЕП перешифровуються за допомогою програмних засобів і надаються йому повторно.

Для відновлення функціонування апаратури криптографічного захисту інформації учасник СЕП звертається до Департаменту безпеки Національного банку. Повернення АРМ-СЕП учасника СЕП до роботи з апаратурою криптографічного захисту інформації здійснюється після закінчення одного банківського дня та до початку наступного банківського дня.

Перенесення АРМ-СЕП на інший комп'ютер у випадках, не обумовлених потребою негайного відновлення його функціонування, дозволяється тільки після закінчення одного банківського дня та до початку наступного банківського дня.

# 3. ПОЛОЖЕННЯ ПРО ЗАХИСТ ЕЛЕКТРОННИХ БАНКІВСЬКИХ ДОКУМЕНТІВ З ВИКОРИСТАННЯМ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

Положення розроблено відповідно до [статей 7](http://zakon3.rada.gov.ua/laws/show/679-14/paran109#n109), [56](http://zakon3.rada.gov.ua/laws/show/679-14/paran632#n632) Закону України "Про Національний банк України", [статті 66](http://zakon3.rada.gov.ua/laws/show/2121-14/paran1096#n1096) Закону України "Про банки і банківську діяльність", Законів України ["Про платіжні системи та переказ коштів в Україні"](http://zakon3.rada.gov.ua/laws/show/2346-14), ["Про захист інформації в інформаційно-телекомунікаційних системах"](http://zakon3.rada.gov.ua/laws/show/80/94-%25%D0%25%B2%25%D1%25%80) і нормативно-правових актів Національного банку України у сфері інформаційної безпеки.

У тексті Положення терміни та скорочення вживаються в такому значенні:

1) **адміністратор інформаційної безпеки** - фахівець з питань інформаційної безпеки, призначений внутрішнім документом організації для забезпечення впровадження та підтримки роботи засобів захисту інформації Національного банку України в цій організації;

2) **АКЗІ** - апаратура криптографічного захисту інформації, яка є власністю Національного банку України;

3) **АРМ бухгалтера САБ** - автоматизоване робоче місце системи автоматизації банку, на якому здійснюється формування файлів/онлайнових пакетів, які містять початкові платежі системи електронних платежів Національного банку України;

4) **АРМ-НБУ-інф** - програмне забезпечення "Автоматизоване робоче місце обміну неплатіжною інформацією" Національного банку України, призначене для обміну інформацією між системою автоматизації банку та інформаційними задачами;

5) **ВК** - відкритий ключ;

6) **ЕЦП** - електронний цифровий підпис;

7) **ЗЗІ** - засоби захисту інформації Національного банку України, які використовуються в системі електронних платежів Національного банку України та інформаційних задачах;

8) **інформаційні задачі** - програмно-технічні комплекси автоматизації банківської діяльності, які забезпечують оброблення та передавання інформації, що не належить до платіжної та технологічної інформації системи електронних платежів Національного банку України, з використанням засобів захисту інформації Національного банку України між банківськими та іншими установами і Національним банком України;

9) **криптобібліотеки** - бібліотеки криптографічних функцій - накладання та перевірки електронного цифрового підпису, шифрування та дешифрування інформації;

10) **організація** - банківська або інша установа, яка є безпосереднім учасником системи електронних платежів Національного банку України та/або інформаційних задач і використовує засоби захисту інформації Національного банку України;

11) **організація-замовник** - банківська або інша установа, яка укладає договір про використання засобів захисту інформації Національного банку України з Національним банком України, у тому числі за свої філії;

12) **ПМГК** - програмний модуль генерації ключів, який є власністю Національного банку України;

13) **САБ** - система автоматизації банку;

14) **система захисту інформації** - сукупність методів і засобів, що включає апаратно-програмні, програмні засоби захисту інформації Національного банку України, ключову інформацію та систему розподілу ключової інформації, технологічні засоби контролю та організаційні заходи, які забезпечують захист електронних банківських документів;

15) **СЕП** - система електронних платежів Національного банку України;

16) **СК** - смарт-картка;

17) **сувора автентифікація** - ідентифікація кожного користувача за ознакою володіння своїм секретним ключем;

18) **ТВК** - таблиця відкритих ключів;

19) **ТК** - таємний ключ.

Положення визначає принципи побудови системи захисту інформації та порядок отримання і повернення ЗЗІ організаціями. **Безпосередні учасники СЕП отримують ЗЗІ для використання в СЕП та інформаційних задачах** незалежно від моделі обслуговування консолідованого кореспондентського рахунку банку в СЕП. Опосередковані учасники СЕП та організації, які не є учасниками СЕП, отримують ЗЗІ для використання їх в інформаційних задачах Національного банку України (далі - Національний банк).

Організації **взаємодіють за всіма поточними питаннями роботи із ЗЗІ з Департаментом інформаційної безпеки** Національного банку України (далі - Департамент інформаційної безпеки) та отримують ЗЗІ в територіальних управліннях Національного банку України (далі - територіальні управління) за місцем їх розташування. Організації міста Києва і Київської області отримують ЗЗІ в Департаменті інформаційної безпеки.

Організації, які використовують ЗЗІ, зобов'язані виконувати організаційні заходи інформаційної безпеки щодо використання, зберігання, обліку ЗЗІ згідно з [Правилами організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України](http://zakon3.rada.gov.ua/laws/show/v0829500-15#n160), затвердженими постановою Правління Національного банку від 26 листопада 2015 року № 829 (далі - Правила).

Департамент інформаційної безпеки здійснює перевірку дотримання вимог Правил в організаціях відповідно до [Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran464#n464), затвердженого постановою Правління Національного банку від 26 листопада 2015 року № 829 (далі - Положення про порядок перевірки).

Організація зобов'язана узгоджувати з Департаментом інформаційної безпеки питання, які можуть виникати під час роботи із ЗЗІ і які не передбачені Правилами.

Керівник організації забезпечує дотримання вимог щодо інформаційної безпеки в ній, визначених цим Положенням.

### ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Система захисту інформації створена для забезпечення конфіденційності та цілісності інформації в електронній формі на будь-якому етапі її оброблення, а також суворої автентифікації учасників СЕП, учасників інформаційних задач і фахівців організацій, які беруть участь у підготовці й обробленні електронних документів. Для забезпечення цілісності інформації, суворої автентифікації та безперервного захисту електронних банківських документів з часу їх формування система захисту інформації використовує механізми формування (перевірки) ЕЦП на базі несиметричних алгоритмів RSA та ДСТУ 4145-2002.

Організація для забезпечення захисту інформації зобов'язана мати трибайтний унікальний ідентифікатор (далі - унікальний ідентифікатор), перший символ якого є літерою на позначення відповідної території, на якій вона розташована, другий і третій символи утворюють унікальний ідентифікатор організації в межах цієї території.

Унікальний ідентифікатор має бути узгоджений з адресою організації в системі електронної пошти Національного банку. Унікальний ідентифікатор записується в ПМГК та АКЗІ, які надаються організації, та не може бути нею змінений, що забезпечує захист від підроблення ключової інформації від імені іншої організації.

Ідентифікатори ключів криптографічного захисту, що використовуються організацією, складаються з шести символів, з яких перші три є унікальним ідентифікатором організації, четвертий символ визначає тип робочого місця учасника СЕП (операціоніст, бухгалтер тощо) або тип інформаційної задачі, п'ятий і шостий - ідентифікатор робочого місця або відповідальної особи.

Організація забезпечує захист електронних банківських документів, шифрування/дешифрування і накладання/перевірку ЕЦП за допомогою таких криптографічних ЗЗІ:

1) апаратно-програмних ЗЗІ, до складу яких входять АКЗІ, СК, програмне забезпечення керування АКЗІ, що вбудоване в АРМ-СЕП і не може бути вилучене або використане окремо, з відповідними ТВК та криптобібліотеками;

2) програмних ЗЗІ, до складу яких входять програмний модуль для шифрування, вбудований в АРМ-СЕП, ПМГК з незаповненими ТВК, носіїв ТК, відповідними ТВК та криптобібліотеками.

Національний банк забезпечує побудову ключової системи криптографічного захисту для СЕП та інформаційних задач. Ця система складається з ключів програмних ЗЗІ, що генеруються в організаціях за допомогою наданих ПМГК, і ключів апаратних ЗЗІ, які генеруються безпосередньо АРМ-СЕП за допомогою АКЗІ.

Основними ЗЗІ в АРМ-СЕП є АКЗІ.

Адміністратор АРМ-СЕП здійснює генерацію ключової пари (ТК та ВК) для АКЗІ на комп'ютері, де розміщується АРМ-СЕП, за допомогою програмного забезпечення керування АКЗІ, що вбудоване в АРМ-СЕП. Генерація здійснюється відповідно до алгоритму, визначеного в національному стандарті України ДСТУ 4145-2002. Для забезпечення безперебійної роботи АРМ-СЕП з апаратурою захисту адміністратор АРМ-СЕП повинен записувати ТК на дві СК (основну та резервну). Ключова інформація під час роботи АКЗІ використовується виключно на рівні АКЗІ, що унеможливлює підроблення та перехоплення ключової інформації. У разі виходу з ладу АКЗІ адміністратор АРМ-СЕП здійснює перехід до роботи з програмними ЗЗІ.

За допомогою ПМГК організація має право генерувати ключову пару (ТК та ВК) відповідно до несиметричного алгоритму RSA для всіх робочих місць, де працюють з електронними банківськими документами. Кожен ТК робочого місця захищений особистим паролем відповідальної особи, яка працює з цим ключем.

Для забезпечення захисту ключової інформації від несанкціонованої модифікації адміністратор інформаційної безпеки надсилає ВК до Департаменту інформаційної безпеки для сертифікації (крім ВК для робочих місць операціоністів, що використовуються лише в САБ).

Департамент інформаційної безпеки здійснює сертифікацію ВК та надсилає засобами системи електронної пошти Національного банку на адресу організації відповідні сертифікати ВК. Організація вживає заходів щодо своєчасного оновлення ТВК відповідно до експлуатаційної документації для АРМ-СЕП, АРМ-НБУ-інф, САБ та інформаційних задач.

Департамент інформаційної безпеки надає криптобібліотеки безкоштовно всім організаціям, які використовують ЗЗІ, для вбудовування в програмне забезпечення САБ або інше відповідне програмне забезпечення.

**В організації використовуються такі ЗЗІ:**

|  |  |  |
| --- | --- | --- |
| № з/п | Назва ЗЗІ | Кількість |
| 1 | АКЗІ (для безпосереднього учасника СЕП) | 1 |
| 2 | СК (для безпосереднього учасника СЕП) | 2 |
| 3 | ПМГК | 1 |
| 4 | Копія ПМГК | 1 |
| 5 | ТКАРМ-СЕП (для безпосереднього учасника СЕП) | 1 + копія |
| 6 | ТК АРМ-НБУ-інф | 1 + копія |
| 7 | ТК АРМ бухгалтера САБ (для безпосереднього учасника СЕП) | За кількістю відповідальних осіб, але не більше 5 |
| 8 | ТК технолога (для безпосереднього учасника СЕП) | За кількістю відповідальних осіб, але не більше 5 |
| 9 | ТК операціоністів (для безпосереднього учасника СЕП) | За кількістю відповідальних осіб |
| 10 | ТК інших робочих та технологічних місць для інформаційних задач | За вказівками Національного банку |

Центральна розрахункова палата Національного банку надає консультації щодо супроводження АРМ-СЕП/АРМ-НБУ-інф, а також технологічного процесу проходження електронних платежів у СЕП та електронних документів в інформаційних задачах.

### ЗАХОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СЕП

Технологічні засоби контролю, вбудовані в програмно-технічні комплекси СЕП, не можуть бути відключені. У разі виявлення нестандартної ситуації, яка може свідчити про підозру щодо несанкціонованого доступу до СЕП від імені певного учасника СЕП, ЦОСЕП автоматично припиняє приймання початкових електронних розрахункових документів та повідомлень від цього учасника.

Основним засобом шифрування файлів (пакетів) СЕП є АКЗІ. Робота АКЗІ контролюється вбудованими в ЦОСЕП і АРМ-СЕП програмними ЗЗІ і забезпечує апаратне шифрування (розшифрування) інформації за алгоритмом, визначеним у національному стандарті України ДСТУ ГОСТ 28147:2009. Як резервний засіб шифрування в СЕП використовується вбудована в ЦОСЕП і АРМ-СЕП функція програмного шифрування.

Засоби шифрування ЦОСЕП і АРМ-СЕП (як АКЗІ, так і програмне шифрування) забезпечують сувору автентифікацію відправника та отримувача електронного банківського документа, цілісність кожного документа в результаті неможливості його підроблення або несанкціонованого модифікування в шифрованому вигляді. АРМ-СЕП і ЦОСЕП у режимі реального часу забезпечують додаткову сувору взаємну автентифікацію під час установлення сеансу зв'язку.

Під час роботи АРМ-СЕП створює журнали програмного та апаратного шифрування і захищений від модифікації протокол роботи АРМ-СЕП, у якому фіксуються всі дії, що ним виконуються, із зазначенням дати та часу оброблення електронних банківських документів. Наприкінці банківського дня журнали програмного та апаратного шифрування і протокол роботи АРМ-СЕП підлягають обов'язковому збереженню в архіві.

Департамент інформаційної безпеки надає банкам (філіям) інформаційні послуги щодо достовірності інформації за електронними банківськими документами в разі виникнення спорів на основі копії архіву роботи АРМ-СЕП за відповідний банківський день.

Департамент інформаційної безпеки розшифровує копію цього архіву та визначає:

1) ідентифікатор банку - учасника СЕП, який надіслав (зашифрував) електронний банківський документ;

2) ідентифікатор банку - учасника СЕП, якому адресовано електронний банківський документ;

3) дату, годину та хвилину виконання шифрування електронного банківського документа;

4) дату, годину та хвилину розшифрування електронного банківського документа;

5) відповідність усіх електронних цифрових підписів, якими був захищений від модифікації електронний банківський документ.

Під час використання АКЗІ додатково визначаються:

1) номер АКЗІ, на якій виконувалося шифрування або розшифрування електронного банківського документа;

2) номер СК, якою користувалися під час шифрування або розшифрування електронного банківського документа.

Департамент інформаційної безпеки надає послуги щодо розшифрування інформації за електронними банківськими документами, якщо між учасниками СЕП виникли спори з питань, пов'язаних з електронними банківськими документами, у разі:

1) невиконання автентифікації або розшифрування електронного банківського документа;

2) відмови від факту одержання електронного банківського документа;

3) відмови від факту формування та надсилання електронного банківського документа;

4) ствердження, що одержувачу надійшов електронний банківський документ, а насправді він не надсилався;

5) ствердження, що електронний банківський документ був сформований та надісланий, а він не формувався або було надіслане інше повідомлення;

6) виникнення спору щодо змісту одного й того самого електронного банківського документа, сформованого та надісланого відправником і одержаного та правильно автентифікованого одержувачем;

7) роботи з архівом роботи АРМ-СЕП під час проведення ревізій тощо.

Департамент інформаційної безпеки надає учасникам СЕП письмові відповіді щодо порушених питань.

V. Внутрішній контроль за станом інформаційної безпеки в організації

Організація зобов'язана інформувати Департамент інформаційної безпеки впродовж одного робочого дня телефоном та протягом трьох робочих днів листом засобами системи електронної пошти Національного банку в таких випадках:

1) виконання (спроби виконання) фіктивного платіжного документа;

2) компрометація ЗЗІ;

3) пошкодження ЗЗІ;

4) несанкціоноване проникнення в приміщення з АРМ-СЕП/АРМ-НБУ-інф (пошкодження вхідних дверей, ґрат на вікнах, спрацювання сигналізації за нез'ясованих обставин тощо);

5) проведення правоохоронними органами та іншими органами державної влади перевірки діяльності організації, унаслідок якої створюються умови для компрометації ЗЗІ;

6) виникнення інших аварійних або надзвичайних ситуацій, що створюють передумови до розкрадання, втрати, пошкодження тощо ЗЗІ.

Внутрішній контроль за станом інформаційної безпеки відповідно до вимог нормативно-правових актів Національного банку в діяльності організації забезпечують:

керівник організації (особа, яка виконує його обов'язки);

заступник керівника організації або особа, яка за своїми службовими обов'язками чи за окремим внутрішнім документом організації призначена відповідальною особою за організацію інформаційної безпеки.

Адміністратор інформаційної безпеки забезпечує поточний контроль за дотриманням вимог інформаційної безпеки під час використання та зберігання ЗЗІ в організації.

Службові особи організації, які відповідають за інформаційну безпеку, зобов'язані надавати письмові або усні відомості про стан ЗЗІ та їх використання, стан захисту інформації в програмному забезпеченні САБ та інших системах, на які поширюються вимоги Національного банку щодо інформаційної безпеки, технологію оброблення електронних банківських документів в організації та систему захисту інформації під час їх оброблення на вимогу Департаменту інформаційної безпеки.

# 3. ПРАВИЛА ОРГАНІЗАЦІЇ ЗАХИСТУ ЕЛЕКТРОННИХ БАНКІВСЬКИХ ДОКУМЕНТІВ З ВИКОРИСТАННЯМ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

Правила розроблені відповідно до [статей 7](http://zakon3.rada.gov.ua/laws/show/679-14/paran109#n109), [56](http://zakon3.rada.gov.ua/laws/show/679-14/paran632#n632) Закону України "Про Національний банк України", [статті 66](http://zakon3.rada.gov.ua/laws/show/2121-14/paran1096#n1096) Закону України "Про банки і банківську діяльність", Законів України ["Про платіжні системи та переказ коштів в Україні"](http://zakon3.rada.gov.ua/laws/show/2346-14), ["Про захист інформації в інформаційно-телекомунікаційних системах"](http://zakon3.rada.gov.ua/laws/show/80/94-%25%D0%25%B2%25%D1%25%80) і нормативно-правових актів Національного банку України у сфері інформаційної безпеки.

2. У цих Правилах терміни та скорочення вживаються в такому значенні:

1) ГМД - гнучкий магнітний диск;

2) захищений носій ТК - носій таємного ключа, обладнаний вбудованими апаратними засобами криптозахисту (Touch Memory, токени тощо);

3) незахищений носій ТК - носій таємного ключа, необладнаний вбудованими засобами криптозахисту (ГМД, флеш-носії тощо);

4) носій ТК - носій таємного ключа (захищений або незахищений).

Інші терміни та скорочення, що вживаються в цих Правилах, використовуються в значеннях, визначених [Законом України](http://zakon3.rada.gov.ua/laws/show/851-15) "Про електронні документи та електронний документообіг", [Положенням про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України](http://zakon3.rada.gov.ua/laws/show/v0829500-15#n17), затвердженим постановою Правління Національного банку України від 26 листопада 2015 року № 829 (далі - Положення про захист), стандартами з управління інформаційною безпекою в банківській системі України, затвердженими постановою Правління Національного банку України від 28 жовтня 2010 року [№ 474](http://zakon3.rada.gov.ua/laws/show/v0474500-10), [Інструкцією про міжбанківський переказ коштів в Україні в національній валюті](http://zakon3.rada.gov.ua/laws/show/z1035-06/paran15#n15), затвердженою постановою Правління Національного банку України від 16 серпня 2006 року № 320, зареєстрованою в Міністерстві юстиції України 06 вересня 2006 року за № 1035/12909 (із змінами).

Правила регламентують порядок використання, зберігання, передавання та облік ЗЗІ організаціями, які отримали ці ЗЗІ відповідно до Положення про захист. Департамент інформаційної безпеки Національного банку України (далі - Департамент інформаційної безпеки) перевіряє виконання цих Правил в організаціях відповідно до [Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran464#n464), затвердженого постановою Правління Національного банку України від 26 листопада 2015 року № 829.

### ПРИЗНАЧЕННЯ ВІДПОВІДАЛЬНИХ ОСІБ ЗА РОБОТУ ІЗ ЗЗІ

Організація зобов'язана призначити відповідальних за роботу із ЗЗІ осіб (далі - відповідальна особа) та осіб, які виконуватимуть обов'язки в разі відсутності відповідальних осіб, а саме:

1) адміністратора інформаційної безпеки;

2) адміністратора АРМ-СЕП/АРМ-НБУ-інф;

3) оператора АРМ бухгалтера САБ;

4) технолога САБ;

5) операціоніста САБ;

6) операторів робочих і технологічних місць САБ та інформаційних задач.

Адміністратор інформаційної безпеки реєструє відповідальних осіб у [розділі I](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran421#n421) журналу обліку адміністратора інформаційної безпеки (додаток 1).

**ЖУРНАЛ обліку адміністратора інформаційної безпеки**

Розділ I. Перелік відповідальних за роботу із засобами захисту інформації Національного банку України осіб:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № з/п | Прізвище, ініціали відповідальної особи | Функціональні обов'язки | Дата і номер документа про призначення | Дата і номер документа про звільнення від функціональних обов'язків | Причина звільнення |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

Розділ II. Перелік засобів захисту інформації Національного банку України:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № з/п | Дата отримання (копіювання) | Назва | Дата і підпис відповідальної особи про отримання | Дата і підпис відповідальної особи про повернення | Примітки |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

Призначення відповідальних осіб в АРМ-СЕП та САБ стосується тільки безпосередніх учасників СЕП.

Організація зобов'язана подавати до Департаменту інформаційної безпеки копію документа або виписку з нього в електронній або паперовій формі:

1) про призначення відповідальних осіб протягом трьох робочих днів з часу їх призначення;

2) про покладання обов'язків/звільнення від виконання відповідних обов'язків в організації, зокрема покладання інших обов'язків, адміністраторів інформаційної безпеки, адміністраторів АРМ- СЕП/АРМ-НБУ-інф і операторів АРМ бухгалтера САБ протягом трьох робочих днів із часу їх призначення/звільнення.

Адміністратор інформаційної безпеки зобов'язаний ознайомитися з нормативно-правовими актами Національного банку України (далі - Національний банк) з питань інформаційної безпеки та підписати зобов'язання адміністратора інформаційної безпеки ([додаток 2](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran443#n443)).

Представник Департаменту інформаційної безпеки зобов'язаний перевірити знання адміністратором інформаційної безпеки своїх функціональних обов'язків та відповідних нормативно-правових актів Національного банку, зробити на зобов'язанні відмітку про проведення цієї перевірки і зберігати копію цього зобов'язання.

Адміністратор інформаційної безпеки має право дати дозвіл на роботу на АРМ-СЕП/АРМ-НБУ-інф, робочих і технологічних місцях САБ та інформаційних задач відповідальним особам після їх ознайомлення з нормативно-правовими актами Національного банку, іншими документами з питань інформаційної безпеки.

Адміністратор інформаційної безпеки зобов'язаний ознайомити відповідальних осіб з правилами роботи та зберігання ТК.

Відповідальна особа зобов'язана підписати відповідне зобов'язання ([додаток 3](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran446#n446)).

Департамент інформаційної безпеки має право звернутися до керівника організації з пропозицією призначити нового адміністратора інформаційної безпеки в разі неналежного виконання ним своїх обов'язків.

Організація зобов'язана забезпечити відповідальних осіб особистими печатками (штампами, пломбіраторами тощо) для опечатування ЗЗІ, сейфів (для зберігання незахищених носіїв ТК) і приміщення з АРМ-СЕП/АРМ-НБУ-інф.

Адміністратор інформаційної безпеки зобов'язаний зареєструвати печатки (штампи, пломбіратори) у [розділі VI](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran432#n432) журналу обліку адміністратора інформаційної безпеки (додаток 1).

Відповідальні особи не мають права передавати один одному печатки (штампи, пломбіратори) для тимчасового користування.

### ФУНКЦІОНАЛЬНІ ОБОВ'ЯЗКИ ВІДПОВІДАЛЬНИХ ОСІБ

Адміністратор інформаційної безпеки зобов'язаний:

1) знати нормативно-правові акти Національного банку з питань інформаційної безпеки і використовувати їх у роботі;

2) виконувати вимоги щодо інформаційної безпеки в організації та підписати зобов'язання адміністратора інформаційної безпеки;

3) забезпечувати конфіденційність системи захисту інформації в організації;

4) отримувати ЗЗІ і проводити їх заміну в територіальному управлінні Національного банку;

5) здійснювати тестування ПМГК та брати участь у тестуванні інших ЗЗІ;

6) здійснювати листування з Департаментом інформаційної безпеки з питань інформаційної безпеки;

7) ознайомлювати відповідальних осіб організації з нормативно-правовими актами Національного банку з питань інформаційної безпеки та перевіряти знання правил використання і зберігання ТК й інших ЗЗІ;

8) забезпечувати відповідальних осіб ЗЗІ;

9) вести облік ЗЗІ і здійснювати контроль за їх прийманням-передаванням;

10) вести справу адміністратора інформаційної безпеки і забезпечувати її збереження;

11) надавати допомогу відповідальним особам в генерації ТК;

12) забезпечувати належне зберігання ЗЗІ, їх передавання іншому адміністратору інформаційної безпеки в разі двозмінної роботи або у зв'язку з тимчасовою відсутністю на роботі - відпусткою, навчанням, хворобою тощо;

13) забезпечувати відправлення на сертифікацію ВК, що потребують сертифікації;

14) вести архів ВК операціоністів;

15) здійснювати копіювання ПМГК та знищення копій ПМГК у встановленому порядку;

ТАБЛИЦЯ суміщення функціональних обов'язків

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № з/п | Функціональні обов'язки | Адміністратор інформаційної безпеки | Адміністратор АРМ-СЕП/ АРМ-НБУ-інф | Оператор АРМ бухгалтера (ключ типу B) | Оператор АРМ технолога (ключ типу A) | Операціоніст САБ | Оператор АРМ інформаційних задач | Адміністратор САБ | Відповідальний за розроблення САБ | Адміністратор локальної мережі | Адміністратор електронної пошти |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | Адміністрратор інформаційної безпеки | - | Х | Х | Х | Х | Х | В | Х | В | В |
| 2 | Адміністратор АРМ-СЕП/АРМ-НБУ-інф | Х | - | Х | В | Д | Д | Х | Х | В | В |
| 3 | Оператор АРМ бухгалтера (ключ типу В) | Х | Х | - | Х | Х | Д | Х | Х | В | В |
| 4 | Оператор АРМ технолога (ключ типу А) | Х | В | Х | - | Х | Д | Д | Х | В | В |
| 5 | Операціоніст САБ | Х | Д | Х | Х | - | Д | Х | Х | В | В |
| 6 | Оператор АРМ інформаційних задач | Х | Д | Д | Д | Д | - | Д | Д | Д | Д |
| 7 | Адміністратор САБ | В | Х | Х | Д | Х | Д | - | В | Д | Д |
| 8 | Відповідальний за розроблення САБ | Х | Х | Х | Х | Х | Д | В | - | Х | Х |
| 9 | Адміністратор локальної мережі | В | В | В | В | В | Д | Д | Х | - | Д |
| 10 | Адміністратор електронної пошти | В | В | В | В | В | Д | Д | Х | Д | - |

16) здійснювати контроль за дотриманням відповідальними особами правил інформаційної безпеки під час роботи із ЗЗІ та їх зберігання;

17) здійснювати контроль за своєчасною заміною ТК відповідальними особами;

18) здійснювати контроль за змінами ТВК у разі необхідності;

19) здійснювати контроль за правильним і своєчасним знищенням відповідальними особами ТК та їх копій;

20) забезпечувати вилучення відповідного ВК з ТВК шляхом генерації ТК на видалення в разі звільнення від обов'язків відповідальних осіб або компрометації ТК;

21) виконувати заміну криптобібліотек і ТВК у САБ та інформаційних задачах, якщо Національний банк ініціює їх заміну;

22) здійснювати перевірки відповідності приміщень з АРМ-СЕП/АРМ-НБУ-інф і сейфів, у яких зберігаються ЗЗІ, вимогам інформаційної безпеки;

23) знати експлуатаційну документацію на АРМ-СЕП/АРМ-НБУ-інф з питань роботи системи захисту інформації;

24) виконувати налаштування операційної системи комп'ютера з АРМ-СЕП/АРМ-НБУ-інф відповідно до вимог та рекомендацій Національного банку щодо усунення вразливостей операційної системи;

25) не рідше одного разу на квартал проводити планові перевірки використання ЗЗІ відповідальними особами організації;

26) під час перевірки звертати увагу на наявність ЗЗІ, ключів від сейфів, у яких зберігаються ЗЗІ, облікових даних, дотримання вимог інформаційної безпеки під час зберігання та використання ЗЗІ, обмеження доступу до приміщення з АРМ-СЕП/АРМ-НБУ-інф, знання відповідальними особами нормативно-правових актів Національного банку з питань інформаційної безпеки, правильне і своєчасне заповнення журналів обліку;

27) після закінчення перевірки зробити відповідні записи в [розділі IX](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran440#n440) журналу обліку адміністратора інформаційної безпеки (додаток 1);

28) інформувати керівника організації і Департамент інформаційної безпеки про виявлені недоліки, що можуть загрожувати безпеці електронної банківської інформації;

29) брати участь (за письмовим або усним розпорядженням керівника організації) у розгляді фактів порушення правил інформаційної безпеки в організації.

**Адміністратор АРМ-СЕП/АРМ-НБУ-інф організації зобов'язаний:**

1) знати нормативно-правові акти Національного банку з питань інформаційної безпеки, що стосуються його функцій, і використовувати їх у роботі;

2) забезпечувати конфіденційність системи захисту інформації в організації;

3) знати експлуатаційну документацію на АРМ-СЕП/АРМ-НБУ-інф і вимоги та рекомендації Національного банку щодо усунення вразливостей операційної системи комп'ютера з АРМ-СЕП/АРМ-НБУ-інф;

4) установлювати АКЗІ та драйвери до нього і забезпечувати постійне її підключення до комп'ютера, на якому функціонує АРМ-СЕП;

5) забезпечувати технологічну дисципліну під час роботи АРМ-СЕП/АРМ-НБУ-інф;

6) здійснювати генерацію ключів АРМ-СЕП/АРМ-НБУ-інф та контроль за строком їх дії;

7) зберігати ТК до АРМ-СЕП/АРМ-НБУ-інф (за необхідності - їх копії), АКЗІ та СК для АРМ-СЕП;

8) уносити необхідні зміни до ТВК АРМ-СЕП/АРМ-НБУ-інф за допомогою АРМ-СЕП/АРМ-НБУ-інф;

9) знищувати в установленому порядку ТК АРМ-СЕП/АРМ-НБУ-інф та їх копії;

10) дотримуватися режиму допуску до приміщення з АРМ-СЕП/АРМ-НБУ-інф;

11) здавати під охорону і знімати з охорони приміщення з АРМ-СЕП/АРМ-НБУ-інф;

12) вести журнал приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф ([додаток 5](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran452#n452));

13) інформувати адміністратора інформаційної безпеки про виявлення недоліків, що можуть призвести до компрометації ЗЗІ або несанкціонованого їх використання;

14) брати участь (за розпорядженням керівника організації) у розгляді фактів порушення правил інформаційної безпеки під час роботи АРМ-СЕП/АРМ-НБУ-інф.

13. Оператори АРМ бухгалтера САБ, операціоністи та оператори інших робочих і технологічних місць САБ та інформаційних задач, які працюють із ЗЗІ, зобов'язані:

1) знати нормативно-правові акти Національного банку з питань інформаційної безпеки, що стосуються їх функцій, і використовувати їх у роботі;

2) забезпечувати конфіденційність відомостей про систему захисту інформації в організації;

3) забезпечувати технологічну дисципліну в роботі з програмним забезпеченням робочого місця;

4) виконувати правила використання і зберігання ЗЗІ;

5) здійснювати генерацію власних ключів;

6) здійснювати контроль за строком дії ключів і своєчасну генерацію (з урахуванням часу на сертифікацію) нових ключів;

7) зберігати власний ТК (за необхідності - його копію), у разі використання незахищеного носія ТК - в особистому сейфі (за його наявності);

8) у разі використання незахищеного носія ТК передавати в установленому порядку на зберігання (якщо немає особистого сейфа) власний ТК (і його копію) адміністратору інформаційної безпеки;

9) забезпечувати схоронність ЗЗІ під час їх використання;

10) знищувати в установленому порядку власні ТК (і їх копії);

11) вести журнал приймання-передавання таємних ключів робочих і технологічних місць ([додаток 6](http://zakon3.rada.gov.ua/laws/show/v0829500-15/paran456#n456)) у разі передавання ТК робочого місця іншій відповідальній особі;

12) інформувати адміністратора інформаційної безпеки про виявлення недоліків, що можуть призвести до компрометації ЗЗІ або несанкціонованого їх використання;

13) брати участь (за письмовим або усним розпорядженням керівника організації) у розгляді фактів порушення правил інформаційної безпеки під час роботи САБ та інформаційних задач.

**Організація зобов'язана дотримуватися такого порядку допуску відповідальних осіб до ЗЗІ:**

1) допуск до ПМГК для роботи з ним мають лише адміністратори інформаційної безпеки;

2) допуск до роботи з АКЗІ, СК, ТК АРМ-СЕП/АРМ-НБУ-інф мають тільки адміністратори АРМ-СЕП/АРМ-НБУ-інф;

3) допуск до ТК робочих і технологічних місць САБ та інформаційних задач має відповідальна особа і тільки до власного ТК;

4) відповідальні особи виконують генерацію власних ТК за допомогою ПМГК лише в присутності адміністратора інформаційної безпеки;

5) адміністратори інформаційної безпеки виконують свої функціональні обов'язки і функції контролю під час роботи з ТВК на АРМ-СЕП/АРМ-НБУ-інф та інших робочих місцях лише в присутності відповідальних осіб.

Порядок роботи з апаратними ЗЗІ

## 4.    "НАЦІОНАЛЬНА ПЛАТІЖНА СИСТЕМА "УКРАЇНСЬКИЙ ПЛАТІЖНИЙ ПРОСТІР".

|  |
| --- |
| В рамках проекту ребрендингу Національної системи масових електронних платежів (НСМЕП), Національний банк України обрав нову назву, логотип та слоган для національної платіжної системи. Відтепер НСМЕП має назву – ПРОСТІР.   Національний банк України як платіжна організація Український платіжний ПРОСТІР докладає максимум зусиль щодо сприяння створенню в Україні привабливого клімату для масового використання платіжних карток та інших електронних платіжних засобів під час здійснення безготівкових роздрібних платежів на території України.  Так Національним банком України була проведена модернізація рішення платіжної системи, що базувалось на національних стандартах і забезпечено перехід на відкриті міжнародні стандарти. Побудовано центральний маршрутизатор, розрахунково-кліринговий центр, здатний забезпечити маршрутизацію та проведення розрахунків з використанням платіжних карток з магнітною смугою та EMV-чипом. |

 На сьогодні банки – учасники системи розпочали роботу в ПРОСТІР за такими напрямами:



**Вступ банку до ПРОСТІР та подальше впровадження карток цієї платіжної системи нададуть нові можливості для розвитку банку та дозволять оптимізувати його витрати за рахунок:**

• відсутності необхідності модернізації термінальної мережі, яка вже приймає платіжні картки міжнародних платіжних систем, для приймання карток ПРОСТІР;

• здійснення емісії карток ПРОСТІР для пенсійних та зарплатних проектів, вартість якої є меншою, ніж вартість аналогічної емісії карток міжнародної платіжної системи;

• зниження емісійних витрат у зв’язку з відсутністю плати за наявну емісію карток ПРОСТІР;

• отримання додаткових доходів від обслуговування клієнтів інших банків у разі встановлення додаткової комісії еквайра (surcharge) для операцій з видачі готівки в банкоматах банку;

• меншого розміру страхового депозиту в розрахунковому банку ПРОСТІР порівняно з міжнародними платіжними системами;

• меншої середньозваженої вартості трансакції внутрішньодержавної платіжної системи ПРОСТІР порівняно з вартістю трансакції в будь-якій міжнародній платіжній системі;

• економії коштів у зв’язку з відсутністю додаткової плати за обслуговування кореспондентського рахунку в розрахунковому банку, оскільки розрахунки за операціями в ПРОСТІР проводяться за наявним кореспондентським рахунком банку в Національному банку України;

• відсутності плати в ПРОСТІР за емісійну або еквайрингову ліцензію (банк одноразово сплачує за приєднання і має можливість вести як емісійну, так і еквайрингову діяльність);

• істотно меншої кількості послуг, що тарифікуються порівняно з міжнародними платіжними системами. Така прозора тарифна політика надає можливість швидко розрахувати вартість будь-якого банківського продукту;

• запровадження в системі ПРОСТІР нової, швидкої та зручної системи вирішення спорів, основні процедури якої розроблено з урахуванням світового досвіду в галузі технологій безготівкових роздрібних платежів. Кожний банк-учасник отримує можливість самостійно керувати претензійною роботою шляхом доступу до відповідного он-лайн інтерфейсу.

### НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

##### РЕКОМЕНДАЦІЇ ДЕРЖАТЕЛЯМ ПЛАТІЖНИХ КАРТОК ЩОДО ЇХ ВИКОРИСТАННЯ

Дотримання цих рекомендацій дасть змогу забезпечити держателям платіжних карток надійне їх зберігання, нерозголошення реквізитів платіжної картки, персонального ідентифікаційного номера (далі – ПІН) та інших даних, а також зменшить можливі ризики під час здійснення операцій з використанням платіжної картки в банкоматах, безготівкової оплати товарів і послуг, у тому числі через мережу Інтернет. Рекомендації діють в частині що не суперечать правилам користування платіжною карткою відповідної платіжної системи (у разі її надання емітентом держателю). Ці рекомендації не поширюються на платіжні картки Національної системи масових електронних платежів.

##### ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ

1. Ніколи не розголошуйте ПІН стороннім особам, у тому числі родичам, знайомим, працівникам банку, касирам та особам, які намагаються допомогти вам під час використання платіжної картки.
2. ПІН необхідно запам’ятати або зберігати його окремо від платіжної картки в недоступному для сторонніх осіб, у тому числі родичів, місці.
3. Ніколи не передавайте платіжну картку для використання іншими особами, у тому числі родичами. Якщо на платіжній картці нанесено прізвище та ім’я фізичної особи, то тільки ця фізична особа має право використовувати платіжну картку.
4. Не розголошуйте та не повідомляйте персональні дані або інформацію про платіжну картку (у тому числі ПІН) на вимогу будь-яких сторонніх осіб, у тому числі й працівників банку. У разі виникнення такої ситуації зателефонуйте до банку-емітента, який видав платіжну картку, і повідомте про цей факт.
5. Під час отримання платіжної картки поставте підпис на її зворотному боці в місці, яке призначено для підпису держателя платіжної картки. Це зменшить ризик використання платіжної картки без вашої згоди в разі її втрати.
6. Будьте уважні до умов зберігання та використання платіжної картки. Не піддавайте платіжну картку механічним, температурним та електромагнітним діям, а також уникайте потрапляння на неї вологи. Платіжну картку не можна зберігати разом з мобільним телефоном, побутовою та офісною технікою, а також поблизу металевих предметів та інших магнітних носіїв/пристроїв.
7. Телефон банку-емітента, який видав платіжну картку, зазначено на зворотному боці платіжної картки. Також потрібно завжди мати при собі контактні телефони банку-емітента, номер платіжної картки на інших носіях інформації: у записнику, мобільному телефоні тощо, але не разом із записом про ПІН.
8. З метою запобігання незаконним операціям з використанням платіжної картки та зняття коштів з вашого карткового рахунку доцільно встановити добовий ліміт на суму та кількість операцій із застосуванням платіжної картки та одночасно підключити електронну послугу оповіщення про проведені операції (наприклад, оповіщення у вигляді коротких текстових повідомлень на мобільний телефон (SMS) або іншим способом).
9. Не рекомендується відповідати на електронні листи, у яких від імені банку пропонується надати персональні дані. Не потрібно відкривати сторінки в мережі Інтернет (сайти/портали), що зазначені в листах (уключаючи офіційну сторінку банку в мережі Інтернет), оскільки це можуть бути сторінки-двійники, через які можуть здійснюватися незаконні дії/сумнівні операції з використанням даних вашої платіжної картки.
10. У цілях інформаційної взаємодії з банком-емітентом рекомендуємо використовувати тільки реквізити засобів зв’язку (мобільних, стаціонарних телефонів, факсів, нтерактивних сторінок у мережі Інтернет (сайтів/порталів), звичайної та електронної пошти тощо), які зазначені в документах, отриманих безпосередньо в банку-емітенті.
11. Пам’ятайте, що в разі розкриття ПІНу, персональних даних, втрати платіжної картки існує ризик здійснення незаконних дій з коштами на вашому рахунку з боку третіх осіб.
12. У разі втрати платіжної картки держатель повинен негайно повідомити про це емітента. У противному разі емітент не несе відповідальності за переказ коштів, ініційований до отримання такого повідомлення за допомогою цієї платіжної картки, якщо інше не передбачено договором.

##### ЗДІЙСНЕННЯ ОПЕРАЦІЙ ЧЕРЕЗ БАНКОМАТ

1. Рекомендуємо здійснювати операції з використанням платіжних карток через банкомати, які встановлені в безпечних місцях (наприклад, в установах, банках, еликих торговельних комплексах, готелях, аеропортах тощо).
2. Не використовуйте пристрої, які потребують уведення ПІН для доступу в приміщення, де розташовано банкомат.
3. Перед використанням банкомата огляньте його щодо наявності додаткових приладів, які не відповідають його конструкції та розташовані в місці набору ПІНу, та в місці (отвір), призначеному для приймання карток (наприклад, наявність нерівно встановленої клавіатури для набору ПІН). У разі виявлення зазначеного е використовуйте такий банкомат.
4. Якщо клавіатура або місце для приймання карток банкомата обладнані додатковими пристроями, що не відповідають його конструкції, не використовуйте його для здійснення операцій з використанням платіжної картки і повідомте про це банк за номером телефону, який зазначено на банкоматі.
5. Не застосовуйте фізичну силу, щоб вставити платіжну картку в отвір призначений для приймання карток. Якщо платіжна картка легко не вставляється, то не використовуйте такий банкомат.
6. Набирайте ПІН таким чином, щоб особи, які перебувають поруч, не змогли його побачити. Під час набору ПІНу прикривайте клавіатуру рукою.
7. Якщо банкомат працює некоректно (наприклад, довгий час перебуває в режимі очікування, мимоволі перезавантажується), відмовтесь від послуг такого банкомата, ідмініть поточну операцію, натиснувши на клавіатурі кнопку ”Відміна” (”Отмена” чи ”CANCEL”) і дочекайтесь повернення платіжної картки.
8. Після отримання готівки в банкоматі необхідно її перерахувати та переконатись у тому, що платіжна картка була повернена банкоматом, дочекатись видачі чека в разі його запиту і тільки після цього відходити від банкомата.
9. Роздруковані банкоматом чеки потрібно зберігати для звірки зазначених у них сум з випискою про рух коштів на картковому рахунку.
10. Не слід проводити ніяких дій за підказками третіх осіб, а також не приймайте від них допомоги під час здійснення операцій через банкомат з використанням платіжної картки.
11. Якщо під час проведення операції через банкомат платіжна картка не повертається, то необхідно зателефонувати до банку за телефоном, який зазначено на банкоматі, та описати ситуацію, що склалася, а також звернутися з цього приводу до банку-емітента, який видав платіжну картку.

##### ЗДІЙСНЕННЯ БЕЗГОТІВКОВИХ РОЗРАХУНКІВ

1. Не використовуйте платіжну картку в торговельній мережі для оплати товарів або послуг, якщо торговець/продавець/касир (у ресторані, магазині, на АЗС тощо) викликав у вас недовіру.
2. Розрахунки з використанням платіжної картки мають виконуватися тільки у вашій присутності. Це забезпечить зниження ризику неправомірного отримання ваших персональних даних, зазначених на платіжній картці.
3. Під час використання платіжної картки для оплати товарів або послуг продавець/касир може вимагати від держателя платіжної картки надати паспорт, підписати квитанцію або ввести ПІН. Перед набором ПІНу слід переконатися, що треті особи, які перебувають у безпосередній близькості від вас, не зможуть його побачити. еред тим, як підписати квитанцію, в обов’язковому порядку перевірте суму, що зазначена на ній.
4. Якщо під час спроби здійснити оплату товарів або послуг з використанням платіжної картки не вдалося здійснити успішно операцію, то необхідно зберігати один примірник виданої терміналом квитанції для перевірки відсутності зазначеної операції у виписці про рух коштів за картковим рахунком.

##### ВИКОНАННЯ ОПЕРАЦІЙ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

1. Не використовуйте ПІН під час замовлення товарів або послуг через мережу Інтернет, а також за телефоном/факсом.
2. Не повідомляйте інформацію про платіжну картку або картковий рахунок через мережу Інтернет, наприклад ПІН, паролі доступу до рахунків, термін дії платіжної картки, кредитні ліміти, персональні дані тощо.
3. З метою запобігання незаконним діям або сумнівним операціям з використанням даних платіжної картки міжнародної платіжної системи рекомендуємо для оплати товарів (послуг) через мережу Інтернет використовувати окрему платіжну картку (так звана ”віртуальна картка”) з граничним лімітом, яка передбачена тільки для цієї цілі та яка не дає змоги здійснювати з її використанням операції в торговельній мережі та зняття готівки.
4. Необхідно використовувати сторінки в мережі Інтернет (сайти/портали) тільки відомих і перевірених Інтернет-магазинів.
5. Обов’язково переконайтесь у правильності зазначення адреси сторінок у мережі Інтернет (сайтів/порталів), до яких підключаєтесь і через які збираєтеся здійснювати оплату товарів (послуг), оскільки схожі адреси можуть використовуватися для здійснення незаконних дій або сумнівних операцій з використанням персональних даних платіжної картки.
6. Рекомендуємо здійснювати оплату товарів (послуг), придбаних через мережу Інтернет, тільки зі свого комп’ютера з метою збереження конфіденційності персональних даних та/або інформації про картковий рахунок. Якщо оплата товару (послуги) здійснюється через чужий коzмп’ютер, рекомендуємо після завершення всіх розрахунків переконатися, що персональні дані та інша інформація не збереглася (знову відкривши сторінку продавця, на якій здійснювалась оплата товару).
7. Слід встановити на свій комп’ютер антивірусне програмне забезпечення і регулярно здійснювати його оновлення та оновлення інших програмних продуктів (операційної системи, прикладних програм). Це захистить вас від проникнення неліцензійного програмного забезпечення (вірусів).

##### ЗАКРИТТЯ КАРТКОВОГО РАХУНКУ

1. Пам’ятайте, що поточні/карткові рахунки закриваються на підставі заяви клієнта, якщо інше не передбачено договором.
2. У разі звільнення з роботи або дострокового розірвання договору з вашої ініціативи, якщо ви не плануєте використовувати в подальшому рахунок та якщо банком передбачено стягнення комісійної винагороди за його обслуговування, доцільно закрити поточний/картковий рахунок, який був відкритий вам для отримання заробітної плати. Для цього ви маєте звернутись із заявою про закриття рахунку до банку, якщо інше не передбачено договором, і повернути платіжну картку (у разі потреби), одержати виписку про рух коштів за картковим рахунком.
3. Під час закриття карткового рахунку (після виконання зобов’язань або в разі розірвання чи закінчення терміну дії договору) банк зобов’язаний видати залишок коштів (у разі його наявності) та на вимогу держателя платіжної картки – довідку про закриття рахунку та повернення платіжної картки, кредиту і процентів за ним. Кошти видаються готівкою або за дорученням клієнта перераховуються на інший рахунок.

**Лекція 2. Ключі для захисту банківської інформації.**

# 1.     Комплексні системи захисту банківських інформаційних технологій та їх застосування.

**2.     Засвідчувальний центр ключів НБУ.**

# 1. Комплексні системи захисту банківських інформаційних технологій та їх застосування.

# 1.1 Мета і призначення комплексної системи захисту банківських інформаційних технологій (КСЗ БІТ).

Мета розробки, створення і використання КСЗ БІТ внутрішньобанківської платіжної системиКСЗ БІТ полягає в зниженні збитку Банку і користувачам (клієнтам) банку в процесі здійснення електронних платежів за рахунок або ліквідації істотного обмеження нефінансових ризиків шляхом комплексного використання організаційних (адміністративних) заходів, правових, морально-етичних норм, фізичних і технічних (апаратних і програмних) способів і засобів захисту інформації.

Комплексна система захисту інформації внутрішньобанківської платіжної системиКСЗ БІТ призначена для забезпечення безпеки критичної інформації й інформаційних ресурсів у процесі функціонування внутрішньобанківської платіжної системиКСЗ БІТ.

Мета функціонування КСЗ внутрішньобанківської платіжної системиполягає у підтримці потрібного рівня значень параметрів стану «інформаційної безпеки ВПС» відповідно до політики безпеки інформації, яка визначається Правлінням АКБ та користувачами (клієнтами) ВПС.

# 1.2 Загальна характеристика ВПС КБ і умови її функціонування.

Топологічна структура внутрішньобанківської платіжної системиКБ являє собою розподілену автоматизовану систему, утворену сукупністю локальних обчислювальних мереж (центральне відділення, регіональні відділення і філії), взаємодіючих між собою і клієнтами на основі еталонної моделі взаємодії відкритих систем (ЕМВВС) за допомогою телекомунікаційних мереж.

Функціональну структуру внутрішньобанківської платіжної системиКБ утворюють компоненти програмних комплексів інформаційних підсистем «Операційний день банку (ОДБ)», «Розрахункова Палата» і «Фінансовий термінал», що взаємодіють між собою, а також із програмним комплексом інформаційної підсистеми «Клієнт - Банк» у процесі формування і передачі електронних платіжних документів.

Інформаційний обмін у локальних і телекомунікаційних мережах реалізується службами передачі повідомлень, електронної пошти на базі протоколів різних рівнів  (Х-400-423, TCP/IP, Frame Relay, Х-25, Х-32, 24 тощо),

Загальна структурна схема і склад ВПС КБ, характеристики каналів зв'язку, характеристики фізичного середовища, загальна технічна характеристика й умови функціонування, призначення і склад оснащення структурних елементів ВПС КБ наведені у вихідних даних, що видаються Замовником, і є невід'ємною частиною даного ТЗ.

Порівняльна оцінка локальних і міжмережевих інформаційних потоків, інформаційних ресурсів складових частин ВПС КБ (ЛОМ центрального відділення, регіональних відділень і філій) за цілеспрямованістю можливих впливів і наслідків (можливого збитку) у термінах потенційних утрат для Банку і користувачів ВПС КБ показує, що у ВПС КБ повинен забезпечуватися захист від таких видів загроз:

     розкриття змісту інформації з обмеженим доступом;

     порушення фізичної і логічної цілісності (модифікація, знищення, нав'язування помилкової) критичної інформації;

     несанкціоноване використання ресурсів як складової частини, так і ВПС КБ у цілому (включаючи порушення функціонування, блокування доступу до ресурсів і інформації, несанкціонований доступ до інформації);

     помилки при використанні ресурсів, як складової частини, так і ВПС КБ у цілому;

     несанкціонований обмін інформацією (обман, підміна);

     відмова від інформації;

     відмова від обслуговування.

Можливі загрози безпеки (конфіденційності, цілісності і доступності) інформації користувачів і безпеки ВПС КБ можуть виявлятися в кожній складовій частині (ЛОМ Центральна дирекція, обласні дирекції, філії, ОДБ, РРП, РП та т.п.) і внутрішньобанківській платіжній системіКБ у цілому на рівні:

1)   окремих апаратно-програмних пристроїв (ПЕОМ, принтер, дисплей, модем, операційна система, файл, каталог, база даних, і т.п.) – 1-й рівень;

2)   окремих локальних мереж (регіональні відділення, філії) – 2 й рівень;

3)   окремої телекомунікаційної мережі КБ у цілому (при роботі наземних магістральних, зонових і внутрішньозонових каналів і трактів передачі) – 3-й рівень;

На першому рівні можливі такі загрози :

     несанкціонований доступ (використання, підключення, зміна) до пристрою і інформаційно - програмного забезпечення (у т.ч. БД);

     перехоплення побічних електромагнітних випромінювань і наведень  від пристрою;

     несанкціоноване одержання інформації з обмеженим доступом (ІзОД), у т.ч. за рахунок перехоплення акустичних випромінювань, що підслухують пристрої і т.п.;

     несанкціоноване порушення фізичної і логічної цілісності ІзОД (перекручування, знищення, модифікація ), у т.ч. за рахунок наявності вірусів, апаратних і програмних закладок у пристроях закордонного виробництва;

     крадіжка носіїв з ІзОД;

     відмова ( збої, помилки ) устаткування;

На другому рівні додатково можливі такі загрози:

     несанкціонована зміна конфігурації ЛОМ (виключення штатних або підключення додаткових апаратно-програмних компонентів);

     злочинний вивід зі строю елементів підсистем (устаткування ЛОМ, каналоутворюючої апаратури і т.п.);

     порушення функціонування компонента (у т.ч. за рахунок наявності апаратних і програмних закладок у закордонному устаткуванні);

На рівні окремих телекомунікаційних мереж внутрішньобанківської платіжної системиКБ у цілому (при роботі наземних і супутникових каналів і трактів передачі в різних мережах зв'язку ) додатково, до другого рівня, можливі такі  загрози:

     перехоплення інформації з обмеженим доступом при передачі ії у каналах зв'язку;

     нав'язування користувачам помилкової інформації (у т.ч. оперативно-службової) при віддаленому доступі;

     аналіз трафіка;

     порушення інформаційного обміну за рахунок порушення каналу (тракту) передачі первинної мережі, атак на протоколи мережі, телекомунікаційні служби, нав'язування помилкової службової інформації і режимів роботи в системі управління як окремих інформаційних мереж, так і системи інформаційного забезпечення у цілому (включаючи зміну маршруту передачі інформації);

     маскування під зареєстрованого користувача або запити системи;

     відмова одержувача (відправника) від факту прийому (передачі) інформації;

     формування одержувачем помилкової інформації, що нібито отримана від відправника;

     формування відправником помилкового підтвердження одержання інформації, що нібито прийнята від одержувача;

     зараження вірусами по інформаційних і службових каналах мереж зв'язку.

**1.3. Вимоги до комплексної системи  захисту інформації ВПС АКБ УСБ**

Об'єктами захисту є:

а) критична інформація, що включає:

     електронні платіжні документи  (категорія – банківська таємниця);

     відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку України (категорія – банківська таємниця);

     операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди (категорія – банківська таємниця);

     фінансово-економічний стан клієнтів (категорія – банківська таємниця);

     системи охорони банку та клієнтів (категорія – банківська таємниця);

     інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності (категорія – банківська таємниця);

     відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація (категорія – банківська таємниця);

     інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню (категорія – банківська таємниця);

     коди, що використовуються банками для захисту інформації (категорія – банківська таємниця).

     інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду (категорія – банківська таємниця);

     оперативно-службова інформація на всіх стадіях обробки (категорія – для службового користування);

     інформація про діючі значення ключів, паролів доступу і параметри настроювання засобів криптографічного і технічного захисту інформації (категорія – державна таємниця);

б) апаратно-програмні й інформаційні ресурси, що включають:

     на рівні окремих пристроїв: клавіатура, дисплеї, системні блоки, сполучні кабелі, принтери, НГМД, локальні ЖМД, пам'ять, апаратура комутації, локальне базове і прикладне функціональне ПЗ (вихідні тексти програм, об'єктні модулі, утиліти, діагностичне ПЗ, СУБД), клієнтські компоненти мережного ПЗ, локальні прикладні і сервісні інформаційні процеси, адресний простір;

     на рівні ЛОМ: робоча станція, сервер друку, файл-сервер, концентратор, комутатор, мережні ЖМД, мережне базове і прикладне функціональне ПЗ, мережні протоколи, центральні, регіональні і філіальні банки даних відомчих інформаційних обліків, мережні інформаційні процеси по обробці інформації з обмеженим доступом (ІзОД), інформаційні процеси з адміністративного управління ЛОМ і т.п.;

     на рівні окремих телекомунікаційних мереж ВПС АКБ УСБ: мережні сервери (сервери доступу), канали зв'язку і канали передачі, міжмережеві маршрутизатори, центри (станції) комутації (пакетів, повідомлень), програмно-інформаційне забезпечення, що реалізує телекомунікаційні служби і протоколи віддаленого доступу, інформаційні процеси міжмережевого обміну даними, інформаційні процеси з міжмережного адміністративного управління.

Опис політики безпеки ВПС КБ наведене в окремому документі «Політика безпеки інформації у внутрішньобанківській платіжній системі Акціонерного комерційного банку.

СЗІ  всіх ЛОМ (доменів) внутрішньобанківської платіжної системи КБ повинні реалізовувати адміністративне керування доступом. Адміністратор СЗІ  кожного домену ВПС КБ має статус «власника» інформації, усього функціонального (прикладного, спеціального і системного) програмного забезпечення і ресурсів (папок, файлів, принтерів і т.д.) на всіх АРМах операторів банку.

На адміністратора СЗІ  кожного домену внутрішньобанківської платіжної системи КБ покладається виконання таких категорій функцій адміністрування: облікових записів користувачів і груп, комплексу засобів захисту, принтерів, моніторингу подій і ресурсів мережі, резервного копіювання і відновлення даних.

Для захисту критичної інформації користувачів ВПС КБ послуги щодо забезпечення конфіденційності, контролю за доступом, захисту цілісності, автентифікації джерела даних і об'єктів комунікації можуть реалізовуватися на декількох рівнях еталонної моделі взаємодії відкритих систем (ЕМВВС), але обов'язково на прикладному і мережному рівнях. При використанні протоколу мережного рівня TCP/IP і подібних протоколів послуги безпеки можуть реалізовуватися на транспортному чи сеансовому рівнях.

Захист інформації телекомунікаційної мережної служби виробляється на мережному і прикладному рівнях, причому, захист основної інформації й інформації мережної служби на мережному рівні виробляється ідентично. При використанні протоколу X-25 захист інформації мережної служби може здійснюватися на транспортному чи сеансовому рівнях.

Інформаційний обмін критичною інформацією, здійснюваний як усередині внутрішньобанківської платіжної системи КБ, так і з клієнтами (споживачами послуг ВПС), повинний здійснюватися з реалізацією механізмів цифрового підпису, автентифікації, контролю цілісності, шифрування, керування доступом і маршрутизації, автоматичного протоколювання й аудиту. При цьому механізми, що застосовуються, повинні реалізувати модель взаємної недовіри і взаємного захисту всіх учасників інформаційного обміну, включаючи арбітра і зловмисника, і, як наслідок, реалізацію функції причетності.

Для вирішення завдань генерації, сертифікації, розподілу, передачі, прийому, збереження, уведення, використання, знищення і відновлення ключових даних для різних користувачів або груп користувачів внутрішньобанківської платіжної системи КБ, створюється 1-4 рівнева система центрів керування і сертифікації ключів ВПС КБ (центральна дирекція, обласні дирекції, філії і системи «клієнт-банк»).

Для керування безпекою рівнів створюється служба безпеки мережного і прикладного (транспортного чи сеансового) рівнів. Керування і сертифікація ключів мережного рівня здійснюється з центра керування ключами 1-го рівня. Керування і сертифікація ключів прикладного (транспортного чи сеансового) рівнів здійснюється з центрів керування ключами 1-4 рівнів відповідно до прийнятої політики безпеки ВПС КБ.

Захист керуючого трафіка (блоків даних мережної служби) виробляється, як правило, на мережному рівні. Окрема керуюча інформація мережної служби може захищатися на прикладному і (або) транспортному рівнях мережної служби.

Інформація користувачів  внутрішньобанківської платіжної системи КБ, як правило, повинна захищатися на прикладному чи транспортному рівні. При необхідності захист може здійснюватися тільки на мережному або мережному і прикладному рівнях. Інформація в локальних мережах доменів може захищатися на прикладному і мережному рівнях. У радіоканалах супутникового зв'язку допускається можливість захисту службової й основної інформації і на фізичному рівні.

 Захист трафіка на мережному рівні здійснюється за допомогою цифрового підпису і шифрування або інкапсуляції пакетів із шифруванням інформаційної частини пакета, заголовка й адреси з використанням високошвидкісних симетричних алгоритмів шифрування. Сеансові ключі шифруються на пакетних (транспортних) ключах, що виробляються, наприклад, у криптосистемі з відкритим поширенням ключів за схемою Диффі-Хеллмана.

Механізми цифрового підпису, симетричного і несиметричного шифрування можуть реалізовуватися  програмно, програмно - апаратно або апаратно.

Захист інформації в окремих комп'ютерах і серверах внутрішньобанківської платіжної системи КБ може вироблятися, при необхідності,  на основі прозорого шифрування, цифрового підпису даних і спрямованого шифрування, керування доступом і розмежування повноважень відповідно до політики безпеки.

Захист інформації в локальних мережах внутрішньобанківської платіжної системи КБ  виробляється з використанням принципів «квитування» доступу, ресурсів і повноважень сервером - адміністратором і «запитів» клієнтів з їх автентифікацією.

Ідентифікація й автентифікація об'єктів і суб'єктів у мережі, а також обмін ключами виробляється з використанням протоколів управління.

Усі користувачі внутрішньобанківської платіжної системи КБ відправляють і приймають відкриті ключі і/або сертифікати в захищеному виді, використовуючи для цього особисті (конфіденційні) транспортні ключі.

Центри керування і сертифікації 1-4 рівнів приймають і сертифікують ключі користувачів з використанням особистих ключів сертифікації. Для захисту сертифікатів, баз сертифікатів і загальносистемних параметрів використовуються ключі сертифікації центра або  транспортні ключі. Відповідно до прийнятої політики безпеки ВПС КБ  центри керування ключами 1-4 рівнів повинні здійснювати імпорт - експорт відкритих ключів, сертифікатів і баз сертифікатів.

Особисті (конфіденційні) ключі цифрового підпису і спрямованого шифрування генеруються кожним користувачем внутрішньобанківської платіжної системи КБ персонально з використанням іменного генератора ключів, яким відповідний центр постачає кожного користувача. Допускається, що всі або деякі ключі генеруються і розподіляються центром керування і сертифікації ключів відповідного рівня (1-4).

Управління доступом виробляється на основі застосування симетричних і несиметричних систем паролювання.

Арбітраж конфліктів за інформацією, переданою службою обміну повідомленнями внутрішньобанківської платіжної системи КБ, здійснюється спеціальною службою КБ. Організаційно-технічні можливості арбітражу створюються за рахунок реалізації в системі автентифікації відправника й одержувача з підтвердженням (функція причетності).

**1.4 Вимоги до комплексної системи захисту інформації у ВПС КБ у частині захисту від витоку інформації технічними каналами**

Вимоги до захисту інформації повинні  бути реалізовані відповідно до Положення - 94, ВПКО-95,  та інших керівних документів ДСТСЗІ  СБУ.

Устаткування ВПС КБ, у яких циркулює інформація з обмеженим доступом, повинне розміщатися вприміщеннях об'єктів з урахуванням вимог мінімізації зон небезпеки інформації.

Повинні бути проведені спецдослідження робочих станцій і мережного устаткування ВПС КБ на предмет визначення рівня побічних електромагнітних випромінювань. ПЕОМ і мережні засоби, що використовуються у ВПС КБ, повинні бути в спеціальному виконанні, що забезпечує рівень захищеності по 3 категорії згідно з СТР-3, для реальної контрольованої зони об'єкта з радіусом (R2) не більш 30 метрів.

Системи електроживлення і заземлення устаткування складових частин ВПС КБ, у якому циркулює інформація з обмеженим доступом, повинні розміщатися усередині контрольованої зони і не мати виходів за її межі.

До складу заходів захисту повинні бути включені організаційні заходи захисту.

# 1.5. Вимоги до підсистеми криптографічного захисту інформації

Система криптографічного захисту призначена для комплексного і безупинного захисту інформації в кожній локальній мережі внутрішньобанківської платіжної  системи КБ при обробці критичної й оперативно-службової інформації центральних, регіональних і територіальних відомчих інформаційних підсистем і при інформаційному обміні повідомленнями по електронній пошті КБ.

Система повинна включати робочі станції користувачів, сервери мережі (сервери доступу), Головний центр управління ключами і регіональні центри.

Робоча станція користувачів локальної мережі складової частини внутрішньобанківської платіжної  системи КБ на прикладному рівні повинна забезпечувати:

     цифровий підпис повідомлення з використанням національного або міжнародного стандарту, включаючи цифровий підпис в групах точок еліптичних кривих;

     архівування і рандомізацію (додаткове шифрування) повідомлень;

     симетричне зашифрування і розшифрування повідомлень;

     підготовку криптограм для ефективної передачі по інформаційних мережах ВПС АКБ УСБ;

     автоматичне протоколювання всіх операцій, виконуваних на робочих станціях, блокування у випадку НСД із сигналізацією на вищий рівень управління;

     генерацію для деяких користувачів особистих і відкритих ключів з використанням іменних генераторів, передачу їх у центр для сертифікації, прийом сертифікованих, запис, збереження і використання.

Сервер мережі (доступу ЛОМ), повинен забезпечувати:

     інкапсуляцію шифрування всіх пакетів на мережному рівні з використанням стандартних протоколів;

     вироблення особистих і відкритих ключів, передачу і  прийом відкритих ключів після їхньої сертифікації;

     взаємодію з «видимими» робочими станціями мережного рівня (криптографічними серверами ЛОМ (серверами доступу);

     взаємодію з усіма центрами управління безпекою (серверами криптографічного захисту ЛОМ).

Локальний центр управління ключами (сервер криптографічного захисту ЛОМ) повинен забезпечувати:

     створення інсталяційного пакета іменного генератора ключів для кожного користувача ЛОМ;

     регенерацію і розподіл симетричних ключів;

     генерацію (розрахунок) відкритих ключових параметрів цифрового підпису;

     формування секретних і відкритих параметрів ключа сертифікації центру;

     формування, розподіл і доставку відкритих загальносистемних параметрів, відкритого ключа сертифікації центру (сервера криптографічного захисту ЛОМ) і транспортних ключів користувачів на відповідні робочі станції;

     генерацію і/або сертифікацію відкритих робочих ключів усіх робочих станцій і передачу сертифікатів на робочі станції.

Головний центр управління ключами (Міжмережевий Центр управління ключами) повинен забезпечувати:

     формування, розподіл і доставку відкритих і загальносистемних параметрів і відкритих ключів сертифікації центру на робочі станції мережного рівня (сервера мережі (доступу) ЛОМ);

     сертифікацію відкритих ключів і створення бази сертифікатів;

     узгодження механізмів захисту між різними відомствами і регіонами;

     генерацію і розподіл усіх видів ключів користувачів;

     управління ключовими структурами з використанням слушних протоколів;

     зміна конфігурації мережі, у тому числі в режимах видалення або додавання робочих станцій;

     розсилання баз сертифікатів користувачам відповідно до вимог конфігурації.

Генератор ключів адміністратора (користувача) повинен забезпечувати:

     генерацію конфіденційних і відкритих ключів;

     запис на носій конфіденційних ключів у захищеному виді;

     прямі і зворотні захисні перетворення робочих ключів при їхній передачі на сертифікацію і прийом сертифікатів;

     запис сертифікатів у базу відкритих ключів;

     безупинний самоконтроль цілісності і дійсності;

     планову або аварійну зміну ключів та ін.

**2. Засвідчувальний центр ключів НБУ.**

Засвідчувальний центр Національного банку України (далі – Засвідчувальний центр) проводить реєстрацію й акредитацію центрів сертифікації ключів відповідно до вимог [Регламенту роботи Засвідчувального центру Національного банку України.](http://zc.bank.gov.ua/content/files/nd34_ua.pdf)

       Засвідчувальний центр надає центрам сертифікації ключів послуги на договірних засадах згідно з [Тарифами на послуги, які надаються Засвідчувальним центром Національного банку України.](http://zc.bank.gov.ua/content/files/nd36_ua.pdf)

       Центр сертифікації ключів зобов’язаний здійснювати свою діяльність відповідно до регламенту роботи центру сертифікації ключів, що визначає організаційно-методологічні та технологічні умови його діяльності в процесі надання послуг електронного цифрового підпису підписувачам. Регламент роботи центру сертифікації ключів має розроблятися відповідно до [Правил оформлення Регламенту роботи центрів сертифікації ключів банків України.](http://zc.bank.gov.ua/content/files/nd20_ua.pdf) Приклад оформлення Регламенту роботи центру сертифікації ключів наведено у [Примірному регламенті роботи центру сертифікації ключів.](http://zc.bank.gov.ua/content/files/nd14_ua.pdf)

       Центр сертифікації ключів зобов’язаний погодити свій регламент роботи центру сертифікації ключів із Засвідчувальним центром до початку проведення реєстрації/акредитації. Центр сертифікації ключів зобов’язаний додатково погодити свій регламент роботи із органом контролю до початку проведення акредитації.

       Банк/окрема юридична особа для проведення реєстрації/акредитації центру сертифікації ключів в Засвідчувальному центрі укладає з Національним банком України договір про надання Засвідчувальним центром послуг центру сертифікації ключів у двох примірниках – по одному для кожної зі сторін. Зразок договору для центру сертифікації ключів, створеного в банку, наведено в додатку 1, а зразок договору для центру сертифікації ключів, створеного окремою юридичною особою, наведено в додатку 2 до [Регламенту роботи Засвідчувального центру Національного банку України.](http://zc.bank.gov.ua/content/files/nd34_ua.pdf)

       Форми заяв, які центр сертифікації ключів подає до Засвідчувального центру, наведено в додатках 4 – 9, 11 [Регламенту роботи Засвідчувального центру Національного банку України.](http://zc.bank.gov.ua/content/files/nd34_ua.pdf)

**Регламент роботи засвідчувального центру НБУ.**

Суб’єктами правових відносин у сфері електронного цифрового підпису, що обумовлюються цим Регламентом, є центри сертифікації ключів, які зареєстровані/акредитовані в Засвідчувальному центрі, Засвідчувальний центр та центральний засвідчувальний орган.

У цьому Регламенті терміни вживаються в такому значенні:

адміністратор безпеки Засвідчувального центру – відповідальна особа Засвідчувального центру, яка виконує функції служби захисту інформації;

адміністратор реєстрації Засвідчувального центру – відповідальна особа Засвідчувального центру, яка виконує функції служби реєстрації;

адміністратор сертифікації Засвідчувального центру – відповідальна особа Засвідчувального центру, яка виконує функції служби сертифікації;

база даних – база даних Засвідчувального центру, у якій зберігається реєстр Засвідчувального центру, інформаційно-довідкова, технологічна та інша службова інформація, потрібна для функціонування програмно-технічного комплексу Засвідчувального центру;

блокування посиленого сертифіката відкритого ключа (далі – сертифікат ключа) – процедура управління статусом сертифіката ключа, яка тимчасово зупиняє чинність сертифіката ключа;

ключі Засвідчувального центру - власні криптографічні ключі Засвідчувального центру (особистий і відкритий) та криптографічні ключі (особистий і відкритий) послуги інтерактивного визначення статусу сертифіката ключа;

комплексна система захисту інформації Засвідчувального центру - сукупність інженерно-технічних, організаційних заходів та програмно-апаратних засобів, які забезпечують технічний та криптографічний захист інформації в програмно-технічному комплексі Засвідчувального центру;

поновлення сертифіката ключа - процедура управління статусом сертифіката ключа, що забезпечує поновлення чинності сертифіката ключа (якій передувала відповідна процедура блокування сертифіката ключа);

регламентна процедура - реєстрація Центру або акредитація Центру, або формування сертифікатів ключа Центру, або зміна статусу сертифікатів ключа Центру, або зміна даних Центру, або процедура передавання документованої інформації в разі припинення діяльності Центру;

список відкликаних сертифікатів ключів Засвідчувального центру - перелік блокованих і скасованих сертифікатів ключів, що формується Засвідчувальним центром, захист якого забезпечується накладенням електронного цифрового підпису за допомогою власних особистих ключів Засвідчувального центру;

скасування сертифіката ключа - процедура управління статусом сертифіката ключа, яка зупиняє чинність сертифіката ключа;

строк чинності сертифіката ключа - проміжок часу між датою і часом початку та датою і часом закінчення чинності сертифіката ключа, що встановлюються під час формування сертифіката ключа;

строк чинності особистого ключа - строк, протягом якого використання особистого ключа є чинним.

Цей Регламент є нормативно-правовим актом, що визначає організаційно-методологічні та технологічні умови діяльності Засвідчувального центру під час проведення процедур реєстрації, засвідчення чинності відкритих ключів, акредитації Центрів у Засвідчувальному центрі, зміни ідентифікаційних даних Центрів та надання послуг електронного цифрового підпису для Центрів від Засвідчувального центру.

Банки, їх працівники та клієнти мають право отримувати послуги електронного цифрового підпису від:

Центру, створеного в банку згідно з внутрішніми документами банку (далі - Центр банку);

Центру, що є окремою юридичною особою.

Банк/окрема юридична особа для проведення реєстрації/акредитації Центру в Засвідчувальному центрі укладає з Національним банком України договір про надання Засвідчувальним центром послуг Центру (далі - договір про надання послуг) у двох примірниках - по одному для кожної зі сторін. Зразок договору для Центру банку наведено в [додатку 1](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran734#n734) до цього Регламенту, зразок договору для Центру, що є окремою юридичною особою, наведено в [додатку 2](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran741#n741) до цього Регламенту.

Центр зобов’язаний здійснювати свою діяльність відповідно до регламенту роботи, що визначає організаційно-методологічні та технологічні умови його діяльності в процесі надання послуг електронного цифрового підпису підписувачам. Регламент роботи Центру має розроблятися відповідно до [Правил оформлення Регламенту роботи центрів сертифікації ключів банків України](http://zakon4.rada.gov.ua/laws/show/z1036-10).

Центр зобов’язаний погодити свій регламент роботи із Засвідчувальним центром до початку проведення реєстрації/акредитації. Центр зобов’язаний додатково погодити свій регламент роботи із органом контролю до початку проведення акредитації.

Центр зобов’язаний кожні шість місяців надсилати електронною поштою до служби реєстрації Засвідчувального центру інформацію про діяльність Центру згідно з формою, визначеною в [додатку 3](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran614#n614) до цього Регламенту, протягом одного місяця, наступного за останнім місяцем відповідного півріччя.

Засвідчувальний центр має право скасувати реєстрацію/акредитацію Центру в разі ненадходження такої інформації у встановлений термін з вини Центру.

Адміністратор реєстрації Засвідчувального центру зобов’язаний контролювати термін вчасного подання зареєстрованим/акредитованим Центром до Засвідчувального центру інформації про діяльність Центру шляхом надсилання офіційного листа з попередженням про необхідність негайно подати звіт, якщо звіт не надійшов вчасно.

Адміністратор реєстрації Засвідчувального центру зобов’язаний проводити аналіз інформації про діяльність Центру, яка надається Центром відповідно до пункту 7 розділу I цього Регламенту, визначати потребу в перевірці виконання Центром вимог, визначених цим Регламентом та нормативно-правовими актами з питань застосування електронного цифрового підпису. Перевірка Центру проводиться, якщо кількість скарг користувачів на неправомірну діяльність (або бездіяльність) Центру протягом відповідного періоду перевищує десять. Перевірка Центру здійснюється Національним банком України в межах повноважень та згідно із законодавством України.

Основними функціями Центру є:

створення і забезпечення функціонування програмно-технічного комплексу Центру;

реєстрація підписувачів;

генерування і зберігання ключів Центру та відповідальних осіб Центру;

забезпечення підписувачів засобами криптографічного захисту інформації (генерування ключів) і в разі потреби надання допомоги під час генерування ключів, а також ужиття заходів щодо забезпечення безпеки інформації під час їх генерування;

засвідчення чинності відкритих ключів Центру в Засвідчувальному центрі відповідно до вимог цього Регламенту та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;

формування сертифікатів відкритих ключів відповідно до вимог регламенту роботи Центру та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;

ведення реєстру Центру;

розповсюдження сертифікатів відкритих ключів Центру та підписувачів відповідно до вимог регламенту роботи Центру та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;

блокування, скасування та поновлення сертифікатів відкритих ключів, сформованих Центром, у випадках, передбачених регламентом роботи Центру і законодавством України у сфері електронного цифрового підпису;

надання підписувачам послуги фіксування часу;

забезпечення можливості перевірки статусу сертифікатів відкритих ключів, сформованих Центром;

публікація на інформаційному ресурсі Центру відкритої інформації;

інші функції, визначені [Законом України](http://zakon4.rada.gov.ua/laws/show/852-15) “Про електронний цифровий підпис”, та дії, пов’язані з технічною і технологічною підтримкою діяльності Центру.

Ідентифікаційні дані Засвідчувального центру:

Повне найменування: Засвідчувальний центр Національного банку України.

Місцезнаходження: 01601, м. Київ, вул. Інститутська, 9.

Адреси розміщення Засвідчувального центру:

03028, м. Київ, просп. Науки, 7;

01601, м. Київ, вул. Інститутська, 9.

Телефон: (044) 525-37-36.

Факс: (044) 524-39-63.

Код за ЄДРПОУ: 00032106.

Електронна адреса інформаційного ресурсу (веб-сайта): [http://zc.bank.gov.ua.](http://zc.bank.gov.ua./)

Організаційна структура Засвідчувального центру містить дві основні складові, що виконують адміністративні, технічні й технологічні функції.

**Адміністративні функції Засвідчувального центру:**

реєстрація Центрів;

акредитація Центрів;

видача, переоформлення та анулювання свідоцтв/дублікатів свідоцтв про реєстрацію/акредитацію Центрів;

забезпечення діяльності Комісії з питань реєстрації, акредитації, повторної акредитації, скасування реєстрації та акредитації, погодження регламентів роботи Центрів;

ведення списку Центрів, що припинили діяльність;

надання Центрам консультацій з питань, пов’язаних із використанням електронного цифрового підпису;

погодження регламентів роботи Центрів;

аналіз інформації про діяльність Центрів, розгляд заяв і скарг щодо неналежного функціонування Центрів та вживання відповідних заходів;

приймання на зберігання від Центрів документованої інформації, яка підлягає передаванню в разі скасування реєстрації, акредитації чи припинення їх діяльності.

**Технічні й технологічні функції Засвідчувального центру:**

створення і забезпечення функціонування програмно-технічного комплексу Засвідчувального центру;

забезпечення захисту інформації впродовж експлуатації програмно-технічного комплексу Засвідчувального центру;

генерування і зберігання ключів Засвідчувального центру та відповідальних осіб Засвідчувального центру;

вивантаження з програмно-технічного комплексу Засвідчувального центру власних відкритих ключів Засвідчувального центру для засвідчення їх чинності в центральному засвідчувальному органі;

установлення належності Центру особистого ключа та його відповідності відкритому ключу під час формування сертифіката ключа Центру;

формування сертифікатів ключів відповідно до вимог цього Регламенту та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису;

ведення реєстру Засвідчувального центру;

поширення сертифікатів ключів Засвідчувального центру та Центрів у встановленому цим Регламентом порядку;

блокування, скасування та поновлення сертифікатів ключів, сформованих Засвідчувальним центром, у випадках, передбачених цим Регламентом і законодавством України у сфері електронного цифрового підпису;

забезпечення можливості визначення статусу сертифікатів ключів, сформованих Засвідчувальним центром;

оприлюднення на інформаційному ресурсі Засвідчувального центру відкритої інформації;

інші дії, пов’язані з технічною й технологічною підтримкою діяльності Засвідчувального центру.

**У Засвідчувальному центрі для виконання адміністративних, технічних і технологічних функцій створено такі служби:**

служба захисту інформації;

служба сертифікації;

служба реєстрації;

служба системного адміністратора.

**Основними функціями служби захисту інформації є:**

проектування, розроблення, експлуатація, обслуговування та модернізація комплексної системи захисту інформації Засвідчувального центру;

адміністрування відповідальних осіб Засвідчувального центру.

**Основними функціями служби сертифікації є:**

генерування ключів Засвідчувального центру;

збереження та використання особистих ключів Засвідчувального центру;

вивантаження з апаратури криптографічних засобів захисту інформації (далі - АКЗЗІ) власних відкритих ключів Засвідчувального центру для засвідчення їх чинності в центральному засвідчувальному органі;

завантаження сертифікатів власних ключів Засвідчувального центру в програмно-технічний комплекс Засвідчувального центру;

перехід на використання нових ключів Засвідчувального центру;

знищення особистих ключів Засвідчувального центру, строк чинності яких закінчився;

засвідчення чинності відкритих ключів Центрів та послуги інтерактивного визначення статусу сертифіката ключа;

звернення до центрального засвідчувального органу щодо зміни статусу сертифікатів власних ключів Засвідчувального центру у випадках, передбачених цим Регламентом і законодавством України у сфері електронного цифрового підпису;

управління статусом сертифікатів ключів, сформованих Засвідчувальним центром;

унесення змін до реєстру Засвідчувального центру щодо статусу Центру (Центр може мати один із таких статусів: збережений, зареєстрований, акредитований, анульований);

забезпечення можливості визначення статусу сертифікатів ключів, сформованих Засвідчувальним центром;

вивантаження/завантаження резервної інформації із/в програмно-технічний комплекс Засвідчувального центру.

**Основними функціями служби реєстрації є:**

установлення осіб заявників Центрів;

перевірка Центрів у процесі їх реєстрації, акредитації та подальшої роботи на відповідність вимогам, установленим цим Регламентом та іншими нормативно-правовими актами у сфері електронного цифрового підпису;

опрацювання документів і запитів, які подаються заявником Центру до Засвідчувального центру під час проведення регламентних процедур;

уведення в програмно-технічний комплекс Засвідчувального центру запитів на формування сертифікатів ключів Центрів для засвідчення їх чинності;

формування в програмно-технічному комплексі Засвідчувального центру запитів на блокування, поновлення та скасування сертифікатів ключів Центрів у разі подання відповідних заяв ([додаток 4](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran616#n616));

контроль за строками подання акредитованими Центрами до Засвідчувального центру інформації про діяльність Центрів за формою, установленою в [додатку 3](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran614#n614) до цього Регламенту, та її опрацювання.

**Основними функціями служби системного адміністратора є:**

установлення та налаштування операційної системи на робочих місцях відповідальних осіб Засвідчувального центру та на серверах Засвідчувального центру;

установлення та налаштування серверних і клієнтських застосувань на робочих місцях відповідальних осіб Засвідчувального центру та на серверах Засвідчувального центру;

виконання оновлень серверного та клієнтського програмного забезпечення програмно-технічного комплексу Засвідчувального центру;

під’єднання робочих місць відповідальних осіб Засвідчувального центру та серверів Засвідчувального центру до інформаційної мережі Національного банку України;

підтримка належного функціонування програмно-технічного комплексу Засвідчувального центру.

У Засвідчувальному центрі для виконання завдань, покладених на зазначені в пункті 4 цього розділу служби, створено такі автоматизовані робочі місця:

автоматизовані робочі місця адміністраторів безпеки Засвідчувального центру;

автоматизовані робочі місця адміністраторів сертифікації Засвідчувального центру;

автоматизовані робочі місця адміністраторів реєстрації Засвідчувального центру;

неспеціалізовані автоматизовані робочі місця.

Відповідальні особи Засвідчувального центру мають право виконувати роботу з нормативно-довідковою інформацією Засвідчувального центру на своїх спеціалізованих автоматизованих робочих місцях або на неспеціалізованому автоматизованому робочому місці з дотриманням вимог, визначених політикою безпеки інформації в програмно-технічному комплексі Засвідчувального центру, у межах повноважень, наданих їм адміністратором безпеки Засвідчувального центру.

Відповідальна особа Засвідчувального центру не має права суміщувати функції служби захисту інформації Засвідчувального центру з функціями інших служб у Засвідчувальному центрі.

Усі відповідальні особи Засвідчувального центру перед початком виконання своїх функціональних обов’язків зобов’язані ознайомитися зі змістом цього Регламенту, інструкцій щодо роботи на автоматизованих робочих місцях, інструкції щодо забезпечення безпеки експлуатації засобів криптографічного захисту інформації та порядку генерування ключових даних і поводження з ключовими документами (далі - інструкції щодо роботи з ключовими даними). Відповідальні особи Засвідчувального центру підтверджують факт ознайомлення з цими документами під підпис.

**Архітектура програмно-технічного комплексу Засвідчувального центр**

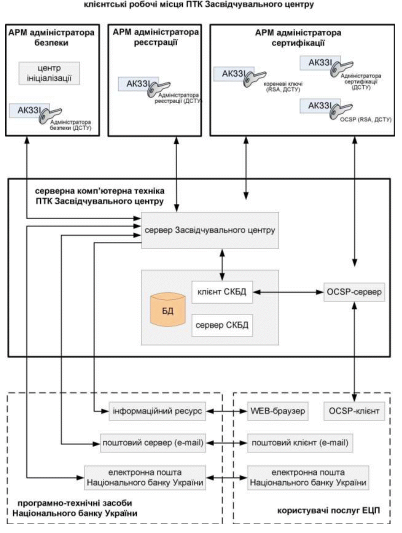
1. Графічна архітектура та загальна технологічна схема оброблення інформації в програмно-технічному [комплексі Засвідчувального центру зображені](http://zakon4.rada.gov.ua/laws/file/text/26/f430886n649.doc) на рис. 1.
2. 

Рис. 1. Архітектура програмно-технічного комплексу Засвідчувального центру.

Програмно-технічний комплекс Засвідчувального центру є автоматизованою системою класу 3. Технічні засоби комплексу об’єднані в розподілену обчислювальну мережу з використанням інформаційної мережі Національного банку України, частина з яких підключена до зовнішніх телекомунікаційних мереж.

Апаратне комп’ютерне забезпечення програмно-технічного комплексу Засвідчувального центру складається з двох типів комп’ютерної техніки, а саме:

серверної комп’ютерної техніки;

клієнтської комп’ютерної техніки.

Програмне забезпечення програмно-технічного комплексу Засвідчувального центру є централізованим трирівневим комплексом, що складається з таких компонентів:

база даних;

серверні застосування;

клієнтські застосування.

База даних, клієнтське застосування системи керування базою даних та серверні застосування функціонують у серверній комп’ютерній техніці.

Усі інші клієнтські застосування, що використовуються в програмно-технічному комплексі Засвідчувального центру, функціонують у клієнтській комп’ютерній техніці, яка входить до складу автоматизованих робочих місць відповідальних осіб Засвідчувального центру.

У програмно-технічному комплексі Засвідчувального центру організовано основні та резервні автоматизовані робочі місця адміністратора сертифікації Засвідчувального центру та адміністратора безпеки Засвідчувального центру. Забороняється одночасно експлуатувати основне та резервне автоматизовані робочі місця.

Сервер Засвідчувального центру виконує такі технічні й технологічні функції програмно-технічного комплексу Засвідчувального центру:

ініціювання завантаження/вивантаження інформації до/із бази даних шляхом використання клієнтського застосування системи керування базою даних (за запитами клієнтських застосувань, установлених на автоматизованих робочих місцях відповідальних Засвідчувального центру, та під час поширення сертифікатів ключів і списку відкликаних сертифікатів ключів Засвідчувального центру);

формування сертифікатів ключів;

створення запитів на блокування, скасування та поновлення сертифікатів ключів;

блокування, скасування та поновлення сертифікатів ключів;

формування списку відкликаних сертифікатів ключів Засвідчувального центру;

поширення сертифікатів ключів;

поширення списку відкликаних сертифікатів ключів Засвідчувального центру;

зберігання нормативно-довідкової інформації Засвідчувального центру;

ідентифікація, автентифікація та авторизація відповідальних осіб Засвідчувального центру;

ведення журналів аудиту функціонування сервера Засвідчувального центру.

Сервер надання послуги інтерактивного визначення статусу сертифіката ключа (сервер OCSP) надає послугу інтерактивного визначення статусу сертифіката ключа, сформованого Засвідчувальним центром.

Сервер системи керування базою даних виконує такі технічні й технологічні функції програмно-технічного комплексу Засвідчувального центру:

управління даними бази даних (завантаження/вивантаження інформації до/із бази даних, створення нових записів тощо);

ведення журналів аудиту функціонування бази даних;

резервне копіювання бази даних;

відновлення бази даних після збоїв.

За допомогою клієнтських застосувань ініціюється:

виконання технічних і технологічних функцій програмно-технічного комплексу Засвідчувального центру з використанням серверних застосувань;

генерування і зберігання криптографічних ключів Засвідчувального центру та відповідальних осіб Засвідчувального центру засобами АКЗЗІ;

вивантаження з АКЗЗІ відкритих ключів Засвідчувального центру для засвідчення їх чинності відповідно до вимог цього Регламенту та інших нормативно-правових актів, що регулюють відносини у сфері електронного цифрового підпису.

Лише за допомогою серверних застосувань може проводитися завантаження/вивантаження інформації до/із бази даних шляхом використання клієнтського застосування системи керування бази даних. Клієнтські застосування, що функціонують у складі автоматизованих робочих місць, отримують доступ до інформації в базі даних за допомогою серверних застосувань.

Серверні застосування програмно-технічного комплексу Засвідчувального центру функціонують на базі відмовостійкого кластера.

Моніторинг роботи кластера здійснює Єдина система моніторингу та управління інформаційними ресурсами Національного банку України.

**Режими доступу до інформації у Засвідчувальному центрі**

У Засвідчувальному центрі приймається, обробляється, пересилається і зберігається інформація, яка за режимом доступу поділяється на відкриту інформацію та інформацію з обмеженим доступом, що має гриф “банківська таємниця” та “конфіденційно”.

Відкрита інформація може оприлюднюватися шляхом її розміщення на інформаційному ресурсі Засвідчувального центру і розсилання засобами електронної пошти (e-mail) та електронної пошти Національного банку України.

Доступ до інформації з обмеженим доступом Засвідчувального центру мають керівник/заступник керівника та відповідальні особи Засвідчувального центру з дотриманням вимог, визначених політикою безпеки інформації в Засвідчувальному центрі.

До відкритої інформації Засвідчувального центру належать:

положення цього Регламенту;

нормативні документи та довідкові матеріали;

зразок договору про надання послуг;

примірний регламент роботи Центру;

сертифікати ключів Засвідчувального центру та Центрів;

інформація про статус сертифікатів ключів Засвідчувального центру та Центрів;

частина бази даних, у якій міститься інформація про Центри, що вноситься в сертифікати ключів Центрів та оприлюднюється шляхом розміщення на інформаційному ресурсі Засвідчувального центру.

Відкрита інформація може зберігатися на паперових носіях та в електронній формі.

До відкритої інформації, яка потребує захисту (забезпечення цілісності та доступності), належить інформація, що оприлюднюється шляхом розміщення на інформаційному ресурсі Засвідчувального центру.

До інформації з обмеженим доступом Засвідчувального центру в електронній формі належать:

особисті ключі Засвідчувального центру та відповідальних осіб Засвідчувального центру;

частина бази даних, у якій міститься інформація про Центри, що не підлягає безпосередньому оприлюдненню (персональні дані про заявника, керівника та заступників керівників Центрів, списки відповідальних осіб Центрів, плани-схеми приміщень Центрів, порядок доступу до спеціальних приміщень та інша інформація, яка не оприлюднюється на електронному інформаційному ресурсі Засвідчувального центру);

налаштування програмних засобів програмно-технічного комплексу Засвідчувального центру (налаштування комплексу засобів захисту, перелік мережевих адрес, протоколів і портів, що використовуються для забезпечення взаємодії між клієнтськими та серверними застосуваннями тощо);

списки відповідальних осіб Засвідчувального центру, їх ідентифікаторів, повноважень, права доступу, зміст протоколів роботи програмно-технічного комплексу Засвідчувального центру тощо;

журнали аудиту, які ведуться в електронній формі.

До інформації з обмеженим доступом Засвідчувального центру на паперових носіях належать:

документи, що подаються Центрами до Засвідчувального центру під час проведення регламентних процедур і не підлягають безпосередньому оприлюдненню;

журнали аудиту, які ведуться на паперових носіях;

інструкції відповідальних осіб Засвідчувального центру;

інструкції щодо роботи з ключовими даними.

**Захист інформації в Засвідчувальному центрі**

Захист інформації в Засвідчувальному центрі забезпечується в результаті впровадження комплексної системи захисту інформації. Комплексна система захисту інформації повинна мати атестат відповідності вимогам захисту інформації.

Усі складові частини програмно-технічного комплексу Засвідчувального центру перебувають у межах контрольованих зон об'єктів Національного банку України, на яких вони розташовані.

Серверна комп’ютерна техніка програмно-технічного комплексу Засвідчувального центру розміщується в спеціальних серверних приміщеннях (у будівлях Національного банку України за адресами: м. Київ, вул. Інститутська, 9; м. Київ, просп. Науки, 7), що відповідають вимогам [Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи](http://zakon4.rada.gov.ua/laws/show/z0955-07), затверджених постановою Правління Національного банку України від 04 липня 2007 року № 243, та [додатка](http://zakon4.rada.gov.ua/laws/show/za104-05) до Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (у редакції наказу від 10 травня 2006 року № 50).

Основне та резервне автоматизовані робочі місця адміністратора сертифікації Засвідчувального центру розміщуються в будівлях Національного банку України за адресами: м. Київ, просп. Науки, 7; м. Київ, вул. Інститутська, 9. Обидва автоматизовані робочі місця розміщені в екранованих шафах, які розташовані в спеціальних приміщеннях з обмеженим доступом. Ключі від екранованих шаф мають тільки адміністратори сертифікації Засвідчувального центру. Адміністратор безпеки Засвідчувального центру отримує доступ до автоматизованого робочого місця адміністратора сертифікації Засвідчувального центру тільки на час проведення процедури генерування криптографічних ключів Засвідчувального центру.

Сторонні особи не мають доступу до приміщень, у яких розташовано обладнання програмно-технічного комплексу Засвідчувального центру. Ці приміщення перебувають під цілодобовою охороною, оснащені охоронною сигналізацією, датчиками руху та датчиками пожежної сигналізації. Ключі від приміщень видаються охороною тільки авторизованому персоналу. Такі умови розміщення обладнання програмно-технічного комплексу Засвідчувального центру забезпечують захищеність середовища його розміщення та унеможливлюють несанкціоноване проникнення до програмно-технічного комплексу Засвідчувального центру.

Усі засоби криптографічного захисту інформації програмно-технічного комплексу Засвідчувального центру повинні мати позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Усі особисті ключі, що використовуються в Засвідчувальному центрі, зберігаються виключно всередині пристроїв АКЗЗІ. Відкриті ключі відповідальних осіб Засвідчувального центру зберігаються виключно всередині АКЗЗІ та в базі даних програмно-технічного комплексу Засвідчувального центру.

Відповідальні особи Засвідчувального центру зобов’язані здійснювати генерування і використання криптографічних ключів відповідно до своїх функціональних обов’язків виключно засобами АКЗЗІ на своїх спеціалізованих автоматизованих робочих місцях.

Відповідальні особи Засвідчувального центру зобов’язані зберігати інформацію з обмеженим доступом на паперових носіях чи в електронному вигляді на зйомних носіях (у тому числі в АКЗЗІ), у сейфах/ящиках/шафах, що надійно замикаються і до яких не мають доступу сторонні особи.

Відповідальні особи Засвідчувального центру несуть особисту відповідальність за надійне зберігання АКЗЗІ та нерозголошення значення паролів доступу і розблокування.

Адміністратор безпеки Засвідчувального центру та адміністратор сертифікації Засвідчувального центру зобов’язані зберігати свої основні пристрої АКЗЗІ на своїх основних робочих місцях, а резервні пристрої АКЗЗІ - на резервних робочих місцях.

Адміністратор сертифікації Засвідчувального центру зобов’язаний зберігати основні та частину резервних АКЗЗІ з ключами Засвідчувального центру в екранованій шафі на основному робочому місці, а іншу частину резервних АКЗЗІ – в екранованій шафі на резервному робочому місці. Адміністратор сертифікації Засвідчувального центру несе особисту відповідальність за надійне зберігання цих АКЗЗІ та нерозголошення паролів доступу і розблокування.

Адміністратор сертифікації Засвідчувального центру зобов’язаний забезпечити зберігання резервних копій бази даних Засвідчувального центру на зйомних носіях в екранованих шафах на своїх основному та резервному робочих місцях.

Серверні застосування та всі автоматизовані робочі місця забезпечують можливість:

криптографічного захисту інформації, що передається каналами зв’язку (автентифікація та шифрування);

захищеного від модифікації протоколювання подій, визначених цим Регламентом;

використання засобів антивірусного захисту на комп’ютерах програмно-технічного комплексу Засвідчувального центру.

Захист інформації, що надається заявником Центру для проведення регламентних процедур (у тому числі персональних даних керівника Центру, заступників керівників Центру та заявника Центру), забезпечується шляхом ужиття:

організаційних заходів щодо обліку та зберігання справ Центрів (формування справ Центрів та їх облік; призначення осіб, відповідальних за зберігання справ Центрів; обмеження доступу до приміщень (шаф), у яких зберігаються справи Центрів);

організаційно-технічних і технічних заходів, реалізованих у результаті впровадження комплексної системи захисту інформації, у тому числі використання надійних засобів електронного цифрового підпису, ведення журналів роботи програмно-технічного комплексу Засвідчувального центру в захищеному вигляді, розмежування та здійснення контролю за інформаційними потоками між внутрішньою локальною мережею Засвідчувального центру і підсистемою відкритого доступу, використання антивірусних засобів, міжмережевих екранів тощо.

**Журнали аудиту в програмно-технічному комплексі Засвідчувального центру**

У програмно-технічному комплексі Засвідчувального центру ведуться такі журнали аудиту:

функціонування програмного забезпечення та АКЗЗІ в програмно-технічному комплексі Засвідчувального центру;

обліку АКЗЗІ;

обліку носіїв інформації з резервними копіями бази даних Засвідчувального центру;

проведення регламентних процедур;

технічного обслуговування програмно-технічного комплексу Засвідчувального центру.

Журнали функціонування програмного забезпечення та АКЗЗІ в програмно-технічному комплексі Засвідчувального центру ведуться в електронній формі на всіх серверних та клієнтських застосуваннях. Інші журнали ведуться в електронній формі або на паперових носіях. Журнали аудиту, які ведуться в електронній формі, повинні мати захист від модифікації.

Програмне забезпечення програмно-технічного комплексу Засвідчувального центру забезпечує захищене від модифікації протоколювання подій, пов’язаних з функціонуванням програмного забезпечення та АКЗЗІ. Цей журнал подій містить дату та час події, опис події, а також ідентифікатор суб’єкта, що ініціював цю подію. У журналі реєструються події, пов’язані з:

генеруванням, резервуванням, використанням і знищенням особистих ключів Засвідчувального центру та відповідальних осіб Засвідчувального центру;

формуванням, переформуванням, блокуванням, поновленням та скасуванням сертифікатів ключів;

унесенням, модифікацією та вилученням даних про Засвідчувальний центр, відповідальних осіб Засвідчувального центру (у тому числі інформації про їх права доступу до програмно-технічного комплексу Засвідчувального центру) та Центри;

наданням доступу до програмно-технічного комплексу Засвідчувального центру відповідальним особам Засвідчувального центру, у тому числі зі спробами несанкціонованого доступу до програмно-технічного комплексу Засвідчувального центру;

збоями в роботі програмно-технічного комплексу Засвідчувального центру;

установленням, зміною, знищенням паролів та системних привілеїв відповідальних осіб Засвідчувального центру.

Адміністратор безпеки Засвідчувального центру зобов’язаний вести журнал подій, пов’язаних з обліком АКЗЗІ, яка використовується в Засвідчувальному центрі. Цей журнал подій містить дату та час події, опис події, серійний номер АКЗЗІ, підпис адміністратора безпеки Засвідчувального центру. У журналі реєструються події, пов’язані з видачею/поверненням АКЗЗІ відповідальними особами Засвідчувального центру.

Адміністратор сертифікації Засвідчувального центру зобов’язаний вести журнал подій, пов’язаних з обліком носіїв інформації, на яких зберігається резервна копія бази даних Засвідчувального центру. Цей журнал подій містить дату і час події, опис події, назву та серійний номер носія, підпис адміністратора сертифікації Засвідчувального центру.

Адміністратор реєстрації Засвідчувального центру зобов’язаний вести журнал подій, пов’язаних з проведенням регламентних процедур. Цей журнал подій містить дату події, опис події, реєстраційний номер поданої заяви, реєстраційний номер рішення про виконання чи відмову від здійснення відповідної регламентної процедури, підпис адміністратора реєстрації Засвідчувального центру. У журналі реєструються події, пов’язані з:

прийманням заяв про реєстрацію Центру в Засвідчувальному центрі ([додаток 5](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran618#n618)), про акредитацію Центру в Засвідчувальному центрі ([додаток 6](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran620#n620)), про формування посиленого сертифіката відкритого ключа Центру в Засвідчувальному центрі ([додаток 7](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran622#n622)), про зміну статусу сертифіката ключа Центру, про внесення змін до даних Центру в Засвідчувальному центрі ([додаток 8](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran624#n624)), про видачу дубліката свідоцтва про реєстрацію/акредитацію Центру в Засвідчувальному центрі ([додаток 9](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran626#n626));

прийняттям рішення про виконання чи відмову в проведенні реєстрації/ акредитації/формуванні сертифікатів ключів; унесенням даних Центру до реєстру Засвідчувального центру;

видачею/скасуванням свідоцтв про реєстрацію/акредитацію Центру в Засвідчувальному центрі ([додаток 10](http://zakon4.rada.gov.ua/laws/show/v0553500-14/paran633#n633)) та дублікатів цих свідоцтв;

прийманням від Центру документованої інформації.

Системний адміністратор зобов’язаний вести журнал регламентних робіт із технічного обслуговування програмно-технічного комплексу Засвідчувального центру. Цей журнал подій містить дату та час події, опис події. У журналі реєструються події, пов’язані з:

плановою заміною комп’ютерної техніки програмно-технічного комплексу Засвідчувального центру;

виходом з ладу складових частин комп’ютерної техніки програмно-технічного комплексу Засвідчувального центру та їх ремонтом/заміною;

оновленням програмного забезпечення Засвідчувального центру.

Відповідальні особи Засвідчувального центру, які ведуть журнали аудиту на паперових носіях або в електронній формі на зйомних носіях, зобов’язані зберігати їх у сейфах/ящиках/шафах, що надійно замикаються і до яких не мають доступу сторонні особи.

Відповідальні особи Засвідчувального центру зобов’язані здійснювати резервне копіювання журналів аудиту. Відповідальні особи Засвідчувального центру здійснюють резервне копіювання журналів аудиту в електронній формі шляхом їх запису на зйомні носії. Відповідальні особи Засвідчувального центру здійснюють резервне копіювання журналів аудиту на паперових носіях шляхом сканування та запису на зйомні носії.

Відповідальні особи Засвідчувального центру зобов’язані забезпечити зберігання резервних копій журналів аудиту в приміщеннях, що територіально відокремлені від приміщень Засвідчувального центру, із забезпеченням їх захисту від несанкціонованого доступу.

Відповідальні особи Засвідчувального центру мають право переглядати журнали аудиту в програмно-технічному комплексі Засвідчувального центру в разі потреби.

Відповідальні особи Засвідчувального центру (крім адміністратора безпеки Засвідчувального центру) зобов’язані отримати дозвіл від керівника/заступника керівника Засвідчувального центру на перегляд журналів аудиту, що ведуться:

з використанням серверних застосувань (крім системних адміністраторів, які відповідають за функціонування операційної системи чи прикладного програмного забезпечення на серверній комп’ютерній техніці);

з використанням клієнтських застосувань на інших автоматизованих робочих місцях;

іншими відповідальними особами Засвідчувального центру.

Строк зберігання резервних копій журналів аудиту в програмно-технічному комплексі Засвідчувального центру становить п’ять років з дати здійснення резервного копіювання.

**Особисті та відкриті ключі**

1. У Засвідчувальному центрі генеруються та використовуються такі криптографічні ключі:

власні (особистий та відкритий) ключі Засвідчувального центру для криптографічного алгоритму за ДСТУ 4145 - 2002 (довжина не менше 257 біт);

власні (особистий та відкритий) ключі Засвідчувального центру для криптографічного алгоритму RSA (довжина не менше 2048 біт);

особистий та відкритий ключі послуги інтерактивного визначення статусу сертифіката ключа для криптографічного алгоритму за ДСТУ 4145 - 2002 (довжина не менше 257 біт);

особистий та відкритий ключі послуги інтерактивного визначення статусу сертифіката ключа для криптографічного алгоритму RSA (довжина не менше 2048 біт);

особисті та відкриті ключі відповідальних осіб Засвідчувального центру для криптографічного алгоритму за ДСТУ 4145 - 2002 (довжина не менше 191 біта)

Власні особисті ключі Засвідчувального центру використовуються для формування сертифікатів ключів Центрів, Засвідчувального центру (крім сертифікатів власних ключів Засвідчувального центру для криптографічного алгоритму за ДСТУ 4145 - 2002) та списків відкликаних сертифікатів ключів Засвідчувального центру.

Особисті ключі послуги інтерактивного визначення статусу сертифіката ключа використовуються під час формування відповіді на запит про визначення статусу сертифіката ключа.

Особисті ключі відповідальних осіб Засвідчувального центру використовуються виключно для їх автентифікації, авторизації, забезпечення цілісності інформації та спостережності в програмно-технічному комплексі Засвідчувального центру.

Центр самостійно генерує особисті та відкриті ключі Центру. Засвідчувальний центр не надає послуг з генерації ключів для Центру.

Довжина особистих ключів для зареєстрованого Центру або Центру, що проходить реєстрацію, має бути:

для алгоритму ДСТУ 4145-2002 - не менше 162 біт;

для алгоритму RSA - не менше 1 536 біт.

Довжина особистих ключів для акредитованого Центру або Центру, що проходить акредитацію, має бути:

для алгоритму ДСТУ 4145-2002 - не менше 257 біт;

для алгоритму RSA - не менше 2 048 біт.

Центр зобов’язаний:

використовувати особисті ключі Центру для формування списку відкликаних сертифікатів ключів Центру та сертифікатів ключів підписувачів, які є клієнтами цього Центру;

використовувати та зберігати особистий ключ та фразу-пароль для голосової автентифікації у спосіб, що унеможливлює ознайомлення з ними сторонніх осіб;

звернутися до служби реєстрації Засвідчувального центру щодо блокування/скасування сертифіката ключа внаслідок виявлення даних про: утрату або компрометацію особистого ключа Центру; утрату контролю за особистим ключем Центру через компрометацію пароля (коду, персонального ідентифікаційного номера), доступу до нього; зміну відомостей, зазначених у сертифікаті ключа Центру;

негайно припинити використання особистого ключа Центру після подання заяви про блокування/скасування відповідного йому сертифіката ключа Центру;

не використовувати особистий ключ Центру в разі його компрометації чи втрати чинності відповідного йому сертифіката ключа Центру.

Центр має право використовувати особисті ключі Центру для формування сертифікатів ключів відповідальних осіб Центру та послуги інтерактивного визначення статусу сертифіката ключа.

Відкритий ключ відповідальної особи Засвідчувального центру використовується виключно для її ідентифікації, автентифікації та авторизації під час завантаження автоматизованого робочого місця та перевірки електронного цифрового підпису, що накладається нею на документи під час виконання своїх функціональних обов’язків.

Строк чинності особистого та відкритого ключів дорівнює строку чинності відповідного сертифіката ключа. Особистий ключ тимчасово не є чинним, якщо сертифікат відповідного йому відкритого ключа заблоковано.

Строк чинності особистого та відкритого ключів відповідальної особи Засвідчувального центру становить не більше двох років з дати і часу їх генерування.

Адміністратор сертифікації Засвідчувального центру зобов’язаний здійснювати процедури генерування та резервування ключів Засвідчувального центру на своєму автоматизованому робочому місці. Процедури здійснюються під контролем адміністратора безпеки Засвідчувального центру. Резервування здійснюється на кількох пристроях АКЗЗІ. Резервування можна провести тільки під час генерування ключів Засвідчувального центру.

Адміністратор сертифікації Засвідчувального центру зобов’язаний використовувати резервні копії особистих ключів Засвідчувального центру в разі:

виходу з ладу основних пристроїв АКЗЗІ з ключами Засвідчувального центру;

експлуатації резервного автоматизованого робочого місця адміністратора сертифікації Засвідчувального центру.

Відповідальні особи Засвідчувального центру зобов’язані виконувати генерування ключів, які використовуватимуться для виконання їх функціональних обов’язків, на своїх спеціалізованих автоматизованих робочих місцях.

Адміністратор сертифікації Засвідчувального центру зобов’язаний приймати рішення про факт або загрозу компрометації особистих ключів Засвідчувального центру чи паролів доступу до пристроїв АКЗЗІ, на яких вони записані.

Адміністратор сертифікації Засвідчувального центру в разі компрометації або підозри на компрометацію будь-якого з особистих ключів Засвідчувального центру зобов’язаний забезпечити скасування або блокування відповідного сертифіката ключа Засвідчувального центру в спосіб, визначений цим Регламентом.

Відповідальна особа Засвідчувального центру зобов’язана приймати рішення про факт або загрозу компрометації свого особистого ключа чи пароля доступу до АКЗЗІ.

Відповідальна особа Засвідчувального центру зобов’язана припинити роботу в програмно-технічному комплексі Засвідчувального центру та змінити пароль доступу до АКЗЗІ в разі компрометації чи підозри на компрометацію пароля доступу.

Відповідальні особи Засвідчувального центру зобов’язані знищити свої особисті ключі після закінчення строку їх чинності з використанням методу, що унеможливлює їх відновлення.

**Сертифікати ключів у Засвідчувальному центрі**

Засвідчувальний центр формує сертифікати ключів відповідно до [Вимог до формату посиленого сертифіката відкритого ключа](http://zakon4.rada.gov.ua/laws/show/z1398-12/paran25#n25), затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (зі змінами).

**Лекція 3. МІЖНАРОДНА МІЖБАНКІВСЬКА ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА (SWIFT).**

### **1. ПРИЗНАЧЕННЯ ТА ОРГАНІЗАЦІЙНА СТРУКТУРА.**

### **2. АРХІТЕКТУРА SWIFT.**

### **3. КОНЦЕПЦІЯ ФОРМУВАННЯ ТА ПЕРЕДАЧІ ПОВІДОМЛЕНЬ.**

### **4. БЕЗПЕКА ПЕРЕДАЧІ ТА ОПРАЦЮВАННЯ ПОВІДОМЛЕНЬ.**

### **5. ФІНАНСОВІ ВИТРАТИ ЩОДО ПІДКЛЮЧЕННЯ ТА РОБОТИ В СИСТЕМІ.**

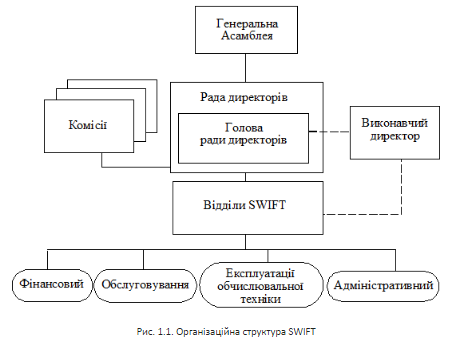
### 1. ПРИЗНАЧЕННЯ ТА ОРГАНІЗАЦІЙНА СТРУКТУРА

Товариство міжнародних міжбанківських фінансових телекомунікацій (Society for Worldwide Interbank Financial Telekom­municatoin — SWIFT) було засноване в 1973 р. Метою створення системи була розробка швидкодіючої й надійної мережі для передачі банківської інформації при суворому контролі і захисту від несанкціонованого доступу. SWIFT спочатку створювалась лише як міжбанківська система. З часом розвиток стандартизації в галузі міжнародної торгівлі цінними паперами зробив доцільним доступ до мережі небанківських закладів. З 1987 р. постановою загальних зборів членів товариства доступ до мережі дозволено брокерським і ділерським конторам, клірінговим і страховим компаніям, а також фірмам, що працюють з цінними паперами.

SWIFT належить до транспортних систем, бо забезпечує тільки передачу і доставку повідомлень учасникам системи, не виконуючи при цьому розрахункових операцій, пов’язаних з їх бухгал­терськими проведеннями. Тобто SWIFT не виконує клірінгових функцій, а є лише глобальною міжбанківською телекомунікаційною мережею.

Система SWIFT працює 24 години на добу і 365 днів на рік. Якщо відправник і одержувач повідомлення працюють в мережі одночасно, то його доставка займає не більше 20 сек. Кількість учасників системи постійно збільшується. Кількість країн-учасників становить 174, повних членів — 2959, неповних членів (sub-member) — 2590, учасників — 604, всього користувачів — 6153.

Організаційну структуру SWIFT наведено на рис. 1.1.



Законодавча влада SWIFT належить Генеральній асамблеї — загальним зборам представників всіх банків, що мають акції. Засідання асамблеї проводиться раз на рік.

Виконавчим органом SWIFT є Рада директорів, яка щорічно переобирається. Оперативне керівництво Радою директорів виконує Голова Ради директорів. До складу Ради директорів входять представники країн (чи групи країн).

До складу SWIFT входять відділи: адміністративний, фінансовий, експлуатації обчислювальної техніки, обслуговування та ін. Стосунки з банками-клієнтами підтримуються головним чином через відділ обслуговування, директор якого очолює групу менеджерів, що несуть відповідальність за стан справ в регіоні. Зокрема, на них покладаються такі функції:

 перевірка готовності країни до підключення її банків до SWIFT;

 координація діяльності SWIFT в регіоні, включаючи і оперативні вирішення питань у випадку аварійних ситуацій;

 маркетинг програмно-технічних засобів і засобів зв’язку, що експлуатуються в системі.

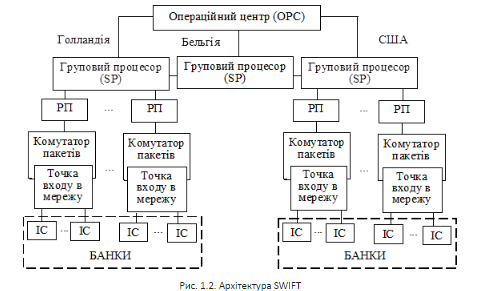
Акції розподіляються лише між банками—членами SWIFT пропорційно обсягу операцій, які проводять за допомогою телекомунікаційної мережі. Якщо член товариства представляє собою країну, банки якої ще не користуються послугами мережі, то йому надається одна акція, а решта тоді, коли банки почнуть користуватись системою. При виході з товариства вартість акцій повертається.

### **2. АРХІТЕКТУРА SWIFT**

Система SWIFT має багаторівневу архітектуру. На нижньому рівні знаходяться банківські установи, де встановлені інтерфейсні системи (ІС), за допомогою яких вони підключаються до мережі. SWIFT пропонує своїм користувачам цілий спектр ІС. Користувачі можуть запропонувати свій варіант ІС, але вона обов’яз­ково погоджується із SWIFT.

Наступний рівень — це регіональні процесори (РП), що розміщені в більшості країн, банки яких вступили в SWIFT. До одного регіонального процесора може бути підключена довільна кількість інтерфейсних систем. Регіональні процесори виконують прийом та перевірку повідомлень користувачів системи і передають їх для подальшої обробки на груповий процесор (SP). Груповий процесор здійснює розподіл повідомлень за адресами по регіональних процесорах, виконує зберігання, архівування та пошук повідомлень, а також генерацію системних звітів.

На верхньому рівні знаходиться операційний центр, який складається з процесора повідомлень, процесора контролю та центра управління, що виконують моніторинг всіх повідомлень системи.



### 3. КОНЦЕПЦІЯ ФОРМУВАННЯ ТА ПЕРЕДАЧІ ПОВІДОМЛЕНЬ

Дані в SWIFT передаються по мережі у вигляді структурованих повідомлень, кожне з яких призначене для виконання певної фінансової операції. Для кожного підключеного вузла і банку сис­тема індивідуально підтверджує прийом повідомлення та його обробку.

Особливістю SWIFT є використання єдиних для всіх користувачів правил і понять. Розроблені типи повідомлень охоплюють такі сфери: платежі клієнтів; міжбанківські платежі; торгівлю грошима та валютою; виписки з поточних рахунків банків тощо.

Всі повідомлення вводяться у систему в стандартному форматі, що спрощує їх автоматизовану обробку та виключає можливість різної інтерпретації відправником і одержувачем. Повідомлення в системі розділені на 10 (0,1, ...9) категорій.

До 0-ї категорії належать системні повідомлення, що дають змогу організувати взаємодію системи з користувачем. З їхньою допомогою SWIFT може також інформувати користувача про стан системи, нові послуги та ін.

Повідомлення категорій 1, 2 ... 9 призначені для операцій, пов’язаних з банківською діяльністю, і нараховують більш як 70 їхніх типів.

Категорії (6) і (8) є резервними, а інші визначають: (1) — операції щодо обслуговування клієнтів, (2) — міжбанківські операції, (3) — валютні операції, (4) —інкасо і документи по грошах, (5) — цінні папери, (7) — документальні акредитиви і гарантії і (9) — спеціальні повідомлення (запит, підтвердження тощо). Всі категорії фінансових повідомлень та їх коди наведено в таблиці 1.1.

Повідомлення в системі SWIFT структуровані і мають такий вигляд (див. табл. 1.2).

Заголовок і «хвостовик» утворюють так званий конверт (епve­lope), в якому немовби пересилаються повідомлення. У заголовку в жорстко стандартизованому вигляді розміщується інформація про відправника і одержувача повідомлення, послідовний номер повідомлення, його тип і пріоритет. Код типу повідомлення в системі має три знаки. Перший знак коду визначає номер категорії, а останні два — номер типу в категорії. Наприклад, код 100 означає повідомлення про операцію «переказ за дорученням клієнта», 200 — переказ за рахунок коштів банку і т. ін.

#### ТАБЛИЦЯ 1.1

| Категорія (А) | Код повідомлення (В) | Тип повідомлення (С) |
| --- | --- | --- |
| 0 |  | Системні повідомлення |
| 1 | 0  1 | КЛІЄНТСЬКІ ПЕРЕКАЗИ І ЧЕКИ Клієнтський переказ  Чекові повідомлення |
| 2 | 0  1 | ПЕРЕКАЗИ ФІНАНСОВИХ УСТАНОВ Банківський переказ  Повідомлення про отримання |
| 3 | 0  2  3  4  5  6 | ВАЛЮТНІ ОПЕРАЦІЇ Валютний обмін і валютні опціони  Фіксовані позичкові й депозитні угоди  Позичково-депозитна угода, яка передбачає повідомлення або вимогу  Угода з форвардним обмінним курсом  Процентні платежі за позичково-депозитною угодою  Обмін процентними платежами |
| 4 | 0  1  2  3  5 | ІНКАСО І ДОКУМЕНТИ ПО ГОТОВИХ ГРОШАХ  Повідомлення про оплату  Підтвердження  Запитання  Зміна інструкцій  Документи по готових грошах |
| 5 | 0  1  2  3  5  6  7  8 | ЦІННІ ПАПЕРИ Доручення на купівлю  Повідомлення/Підтвердження купівлі-продажу  Інструкції з «руху» кредитів і цінних паперів  Підтвердження «руху»  Корпоративні дії, доручення, претензії  Корпоративні події  Бюлетень і управління інвестиціями  Спеціальні повідомлення |
| 6 | 0  4 | ДОРОГОЦІННІ МЕТАЛИ І СИНДИКАТИ Дорогоцінні метали  Синдикати |
| 7 | 0  1  2  3  4  5  6 | ДОКУМЕНТАРНІ АКРЕДИТИВИ І ГАРАНТІЇ Емісія/позика, передоручення і доповнення (зміни документар­ного акредитиву)  Авізовані документарні акредитиви третього банку  Перекази документарного акредитиву  Підтвердження і доручення  Гамбурзьке повноваження  Доручення і повноваження  Гарантії |
| 8 | 0  1  2 | ПОДОРОЖНІ ЧЕКИ Продаж і розрахунок  Відшкодування витрат  Управління запасом |
| 9 | 0  1  2  3  4  5  7  8 | ЗМІШАНІ ПОВІДОМЛЕННЯ Підтвердження дебетування  Підтвердження кредитування  Запити балансового звіту  Повідомлення про зміну відсоткової ставки. Виписка з рахунків і балансів клієнтів  Виписки по рахунках «ностро»  Виписки по системі «нетто»  Запит про фінансовий стан |
| N | 9 | ЗАГАЛЬНА ГРУПА Оплата, відсоток, затрати  Запити анулювання  Запити і відповіді  Приватні, а також повідомлення вільного формату |

*Таблиця 1.2.*

###### **СТРУКТУРА ПОВІДОМЛЕННЯ SWIFT**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Початок повідомлення | Заголовок | Початок  тексту | Текст повідомлення | Кінець тексту | Хвостовик | Кінець повідомлення |
| Start of Message | Неаdег | Start End of | Техt оf  Message | End of  text | Тгаіlег | End of  End of |

У текст повідомлення інформація заноситься також у суворій послідовності й реалізується при заповненні відповідного поля повідомлення, яке має чітку нумерацію. Повідомлення складається з послідовності полів, що заздалегідь закодовані двозначними цифровими кодами. Наприклад, 32 — сума, 50 — переказник, 70 — призначення платежу і т. ін.

При цьому поля в повідомленнях поділяються на обов’язкові та необов’язкові. Обов’язкові містять ключову інформацію для повідомлень даного типу. Необов’язкові поля необхідні для здійснення складних багатоступеневих операцій або для передачі додаткових інструкцій. У «хвостовику» повідомлення розміщується код аутентифікації, а також інші кодові повідомлення, призначення яких — попередити банк-отримувач про можливість подвійного платежу, затримки в передачі повідомлення, інша допоміжна інформація. В особливу групу виділено системні повідом­лення, які здійснюють діалог користувача із системою. Ці повідомлення використовуються для виконання певних системних функцій: вимоги повідомлень; навчальні цілі; відповіді на запити користувачів та інформування останніх про розвиток мережі; її нові можливості.

Існують три основних системних повідомлення:

— LJG-IN/OUT— системне повідомлення для входу/виходу в систему;

— RETRIEVAL — за цим запитом система надсилає копію повідомлення, яке зберігається;

— REPORTS — дає змогу одержати різні види рахунків (періо­дичних або разових).

Системним повідомленням надається першочерговий пріо­ритет, оскільки вони містять основну інформацію щодо функціо­нування системи. Банківські повідомлення поділяються на тер­мінові та звичайні. За пересилання термінових повідомлень стягується спеціальний тариф.

### 4. БЕЗПЕКА ПЕРЕДАЧІ ТА ОПРАЦЮВАННЯ ПОВІДОМЛЕНЬ

Безпека обміну повідомленнями має дуже важливе значення для нормальної банківської діяльності, тому їй приділяється велика увага і в системі SWIFT.

Організаційно питаннями безпеки та надійності роботи системи займається Генеральна інспекція, що підпорядкована безпосередньо тільки Раді директорів SWIFT.

Для всіх приміщень існує режим обмеженого і контрольованого доступу. Співробітники центрів працюють і переміщуються в обмежених їхніми обов’язками робочих зонах. Існують також спеціальні інструкції на випадок пожежі, терористичних актів, витоків газу, збоїв в живленні і т.ін.

На програмному рівні спеціальна система автоматично виявляє випадки несанкціонованого доступу або необгрунтоване проникнення в роботу регіонального процесора. Автоматично фіксуються також аномалії параметрів системи.

Крім того, кожному повідомленню при його вступі в систему автоматично присвоюється послідовний вхідний номер, а при виводі — вихідний. Повідомлення, що вводяться у систему з відхиленнями від прийнятого стандарту, протоколу або формату, відкидаються. Всі пересилання повідомлень на міжнародних лініях зв’язку кодуються з використанням шрифтів, що міняються через випадкові проміжки часу.

Високий рівень безпеки гарантується також системою контролю доступу до роботи в мережі, що включає в себе місцеві паролі для вузлів, log-файли, в яких зберігається інформація про кожне підключення до мережі і т.ін.

Усі питання, зв'язані з безпекою в системі SWIFT, умовно можна віднести до таких напрямів:

•  фізична безпека;

•  безпека логічного доступу до системи SWIFT;

•  забезпечення безпеки повідомлень, що передані і зберігаються в системі;

•  безпека обміну повідомленнями «користувач-користувач».

Засоби безпеки, які забезпечуються системою SWIFT, складаються із:

•  процедури входу в систему;

•  процедури вибору програмного забезпечення;

•  нумерації повідомлень;

•  перевірки помилок:

•  криптозахисту;

•  контролю доступу до повідомлень у регіональних процесорах, комутаційних процесорах, центрах керування системою.

Відділ головного інспектора системи SWIFT керує всіма питаннями безпеки роботи мережі SWIFT. Користувачам рекомендується забезпечувати належну безпеку процедур, здійснюваних у їх власних організаціях, наприклад контроль доступу до терміналів SWIFT, керування їх підключенням і використанням.

**Фізична безпека**

Здійснюється на основі розмежування і контролю доступу до всіх операційних і адміністративних вузлів SWIFT шляхом використання електронних засобів і засобів виявлення несанкціонованого доступу. Застосовується також дистанційне керування для вузлів SWIFT, що керуються автоматично. Якщо користувач запитує центр про доступ до SWIFT, то в обов'язковому порядку повинний бути зроблений запит до головного інспектора і без його санкції нікому не буде даний дозвіл на доступ.

**Безпека логічного доступу до системи SWIFT**

Як уже говорилося вище, користувачі можуть одержати фізичний доступ до системи SWIFT II тільки через відділ головного інспектора, що працює з одним чи більш логічним терміналом (LT). Кожному LT призначаються унікальні таблиці безпеки для процедур LOGIN і SELECT, що являють собою послідовності ключів у табличному виді. Кожен ключ у таблиці може застосовуватися тільки один раз і зв'язаний з послідовними номерами процедур, що використовують ці ключі. Ці таблиці формуються і відсилаються користувачу до їх підключення до системи SWIFT на основі запиту на їх застосування, причому нові таблиці безпеки створюються відразу після висилки чергових таблиць і пересилаються користувачу тільки в міру необхідності. Користувачі, що активно застосовують таблиці безпеки, можуть запросити у відділі головного інспектора таблиці з 2400 ключами замість звичайних таблиць (1200 ключів).

Доступ LT до системи SWIFT здійснюється за допомогою команди LOGIN. До того як буде надісланий запит LOGIN, користувачу необхідно ввести ключ запиту і ключ відповіді з таблиці безпеки LOGIN. Ціль запиту LOGIN:

•  визначити логічний шлях для зв'язку LT із системою;

•  обмежити доступ у систему несанкціонованих користувачів;

•  дозволити користувачам перевірити, що вони підключилися до справжньої системи SWIFT.

При запиті процедури LOGIN система SWIFT робить такі дії:

1.  Перевіряє заголовок і текст повідомлення, що відправляється процедурою LOGIN.

2.  Перевіряє дійсність кінцевика повідомлення, сформованого з використанням ключа з таблиці безпеки.

3.  Якщо підтвердження дійсності користувача пройшло успішно, порядковий номер запиту LOGIN (LSN) порівнюється з очікуваним системою LSN. Якщо LSN знаходиться в припустимому діапазоні, система перевіряє, що запит LOGIN виданий після дня, зазначеного в останній команді LOGOUT (указує часові рамки для LT, протягом яких від даного LT не будуть прийматися запити).

4. Підтверджує запит LOGIN, повертаючи або позитивне підтвердження LOGIN (LAK), або негативне підтвердження LOGIN (LNK). Підтвердження буде містити кінцевик, заснований на ключі відповіді, і дозволяє користувачу перевірити дійсність системи.

5. Записує спробу LOGIN разом з відповіддю системи в історію LT.

*Спроба зробити запит LOGIN на лінії зв'язку, по якій LT вже увійшов у систему, розглядається як серйозна помилка й ігнорується системою.*

Доступ до додатка FIN (з якого відправляються повідомлення «користувач-користувач» і ряд системних повідомлень) здійснюється за допомогою команди SELECT, що проходить процедуру підтвердження для гарантії того, що:

•  тільки перевірені користувачі можуть одержати доступ до системи SWIFT;

•  користувач зв'язався зі справжньою системою SWIFT.

У SWIFT розроблена і рекомендована Радою директорів для повсюдного використання поліпшена архітектура системи забезпечення безпеки, що відповідає в широкому змісті сучасному рівню розвитку телекомунікаційних технологій і криптографічних методів. Основою нового підходу стало застосування інтелектуальних карт (ICC), зміна алгоритму перевірки вірогідності і збільшення довжини двосторонніх ключів, якими обмінюються користувачі.

Для забезпечення безпеки логічного доступу до системи SWIFT у рамках нового підходу була розроблена служба безпечного входу в систему і вибору режиму (SLS), що дозволяє користувачам одержати доступ до послуг системи SWIFT за допомогою ICC замість використання паперових таблиць Login і Select. При застосуванні ICC вимагаються *зчитувачі карт.*На даному етапі пропонується два різних типи зчитувачів карт. Перший - спрощений *зчитувач* карт (BCR), що підтримує тільки службу SLS. Другий - *зчитувач* карт із модулем захисту (SCR), у якому крім функцій *зчитувача*реалізована також функція модуля апаратного захисту, що виконує генерування ключів і шифрування секретної інформації (застосовується як для підтримки SLS, так і інших служб, створених у рамках нового підходу). Тому що в SCR повинні зберігатися секретні дані, це пристрій виконаний захищеним від розкриття - будь-яка спроба добратися до його внутрішніх частин викликає автоматичне знищення секретної інформації, що зберігається в SCR.

**Служба SLS і операції в рамках цієї служби**

Як уже говорилося, основне призначення SLS - заміна паперових таблиць Login/Select механізмом, здатним генерувати сеансові ключі доступу до системи, що при використанні паперових таблиць приходилося зчитувати операторам СВТ вручну. Необхідно відзначити, що ICC не містить самих ключів доступу, але зберігає алгоритм, що може згенерувати необхідний сеансовий ключ для будь-якого запиту Login/Select.

Для забезпечення логічного доступу до послуг системи SWIFT необхідно вставити відповідним чином зконфігуровану ICC у зчитувач карт і ввести PIN-код на клавіатурі зчитувача. При виборі функції Login (Select) на СВТ необхідні коди автоматично генеруються ICC і передаються у СВТ, до якого підключений зчитувач. Потім СВТ продовжує обробляти запит Login (Select) звичайним чином. Для більшості користувачів зчитувач карт буде залишатися підключеним до СВТ з метою одержання максимальної зручності від служби SLS. Але є можливість використання і непідключеного зчитувача карт (наприклад, для вилучених терміналів чи у випадку аварії), коли необхідні коди доступу хоча і генеруються в ICC, але відображаються на дисплеї зчитувача карт, а потім вручну вводяться у СВТ.

**Забезпечення безпеки повідомлень, що передані і зберігаються в системі**

Безпека обміну повідомленнями в системі SWIFT полягає в наступному:

•  забезпеченні безпеки передачі;

•  перевірці повідомлень;

•  забезпеченні безпеки доставки.

З огляду на те, що мережа захищена від несанкціонованого доступу, потік повідомлень при передачі і збереження повинен мати захист від:

•  утрати, ушкодження, помилкової доставки чи затримки повідомлень;

•  помилок при передачі і збереженні;

•  утрати конфіденційності;

•  внесення в повідомлення помилкових змін.

**Забезпечення безпеки передачі**

В усі повідомлення додатків GPA і FIN системи SWIFT додається обов'язкове закінчення *-*так званий кінцевик СНК, що містить контрольну суму даного повідомлення, яка перелічується у вузлах введення/виведення мережі. Якщо відбулося перекручування повідомлення під час передачі (це встановлюється шляхом перевірки контрольної суми прийнятого повідомлення, що є унікальної для кожного повідомлення) і це не було зафіксовано в протоколі перевірок низького рівня, то на інформацію, що надійшла, буде передана негативна відповідь і буде необхідне повторне введення.

**Перевірка повідомлень**

Усі вхідні повідомлення перевіряються відповідним RP до того, як передати їх SP. Тільки повідомлення, що відповідають стандартам SWIFT і синтаксису, приймаються до доставки. Результати безупинних перевірок постійно зберігаються, і через дуже строгі стандарти, встановлених у SWIFT, будь-яка серйозна помилка протоколу приводить до закриття сеансів FIN чи GPA.

**Безпека доставки**

Після строгих перевірок, проведених для усіх вхідних потоків повідомлень і високоякісних методів забезпечення безпеки, використаних для передачі повідомлень, усі повідомлення, позитивно підтверджені системою SWIFT, розглядаються правильними і, отже, доставленими у системі.

Обов'язковий кінцевик СНК використовується одержуючим LT для перевірки того, що ні однієї помилки не з'явилося при передачі між вхідним RP і реципієнтом. Обов'язкове використання підтверджень прийому користувачем повідомлення (UAK/UNK) дає можливість системі SWIFT відповісти, чи прийняв LT послане йому повідомлення чи ні. Система SWIFT не буде вважати повідомлення доставленим доти, поки позитивне підтвердження прийому користувачем повідомлення (UAK) не буде отримано від LT-реципієнта. Система SWIFT буде намагатися доставити повідомлення 11 разів, після чого доставка повідомлення припиняється і відправник сповіщається, що повідомлення не може бути доставлено. Кожна наступна спроба доставки після першої буде містити відповідну кількість кінцевиків PDM.

**Безпека обміну повідомленнями «користувач-користувач»**

При обміні повідомленнями між користувачами для забезпечення конфіденційності і дійсності, а також для контролю над цілісністю повідомлень система SWIFT рекомендує застосовувати алгоритм перевірки вірогідності. Перевірка вірогідності - важлива частина системи забезпечення безпеки SWIFT, вона полягає в обміні між користувачами ключами і перевірці того, що достовірний результат представлений у визначених типах повідомлень.

Приймаючий термінал перевіряє текст отриманого повідомлення за допомогою стандартного алгоритму SA/2 і погоджені ключі вірогідності. І якщо в ході перевірки отриманий негативний результат, то це може, швидше за все, відбутися через помилки передачі чи невірного ключа вірогідності.

Ключ вірогідності складається з 32 шістнадцятирічних символів, розділених на дві частини по 16 знаків, і може бути використаний як для передачі, так і для прийому чи в обох напрямках. Для формування ключа необхідно дотримувати наступних правил:

•  перша і друга половина повинні бути різні;

•  у кожній половині будь-який дозволений символ може з'явитися тільки один раз.

Тут необхідно відзначити, що ключі вірогідності передаються між кореспондентами поштою, і для забезпечення безпеки ключової інформації всім користувачам системи SWIFT рекомендується підтримувати кореспондентські відносини тільки з відомими користувачами й в організації - ініціаторі обміну вибирати тип ключа вірогідності відповідно до проведеної політики безпеки цієї організації.

Як уже говорилося, у зв'язку з переходом на нові технології забезпечення безпеки в системі SWIFT, що використовують ICC, був удосконалений і процес обміну ключами вірогідності між користувачами, результатом чого стала поява служби обміну двосторонніми ключами (ВКЕ). Призначення ВКЕ - замінити стомлюючу систему ручного обміну двосторонніми ключами підтвердження дійсності між кореспондентами по відкритій пошті на систему, що використовує нові повідомлення SWIFT II і зчитувач карт із модулем захисту, спеціально розроблені для цієї мети. Система дозволить цілком автоматизувати процес обміну ключами. За новою технологією кожен двосторонній ключ підтвердження дійсності створюється усередині SCR і зашифровується перед передачею у СВТ, до якого SCR підключений. Ключі підтвердження дійсності бувають або двоспрямованими (той самий ключ служить для перевірки переданих і прийнятих повідомлень), або односпрямованими (для прийому і передачі повідомлень використовуються окремі ключі). Служба ВКЕ заснована на стандарті ISO по обміні ключами (ISO 11166 - Banking - Key Management by Means of Asymmetric Algorithms). У цьому стандарті визначене використання асиметричних алгоритмів для шифрування і цифрового підпису двосторонніх ключів, якими обмінюються кореспонденти. Спеціально для забезпечення розподілу відкритих ключів у системі SWIFT був створений Центр керування безпекою (SMC), у складі якого працює Центр сертифікації ключів, що видає сертифікати відкритих ключів користувачів системи SWIFT.

Наступний за процедурами переходу і початкової установки реальний обмін двосторонніми ключами підтвердження дійсності по мережі SWIFT складається з передачі чотирьох спеціальних повідомлень SWIFT між кореспондентами, один із яких виступає як ініціатор обміну, а інший - як одержувач. Перші два повідомлення використовуються винятково для цілей установлення сеансу обміну двосторонніми ключами. У третьому повідомленні ініціатор обміну посилає ключ, створений і зашифрований усередині SCR, використовуючи відкритий ключ одержувача. У такий же спосіб SCR створює цифровий підпис ініціатора обміну ключами. Після одержання третього повідомлення учасник обміну перевіряє цифровий підпис, і якщо він дійсно належить відправнику, то йому висилається підтвердження, ключ визнається вірним і заноситься у файл двосторонніх ключів.

Безпосередньо після обміну новий ключ стає «майбутнім» ключем для цих кореспондентів і буде використовуватися для перевірки фінансових повідомлень, починаючи з взаємно погоджених дати і часу. При використанні ключів прийому/передачі кожен кореспондент є ініціатором обміну для свого ключа передачі.

### 5. ФІНАНСОВІ ВИТРАТИ ЩОДО ПІДКЛЮЧЕННЯ ТА РОБОТИ В СИСТЕМІ

Підключитися до SWIFT може будь-який банк, що має валютну ліцензію та готовий понести відповідні одноразові, щорічні та поточні фінансові витрати.

До одноразових витрат можна віднести: вступний внесок в 400 тис. бельгійських франків або близько 12500 доларів США, оплату однієї акції вартістю в 1500 дол., а також оплату програмного та технічного забезпечення і т. ін. в сумі близько 170 тис. дол. В умовах України до цих витрат потрібно віднести і витрати в розмірі близько 1000 дол. за підключення до мережі УкрПАК як телекомунікації SWIFT. Таким чином, для початку роботи в системі потрібно заплатити близько 185000 дол. США.

Щорічні витрати пов’язані з оплатою за супровід програмного та технічного забезпечення, за аренду модемів, каналів і т.ін. і залежать від конкретних умов.

Поточні витрати залежать від кількості пересланих повідомлень (за вихідні повідомлення платня не береться) і становлять від 0,2 до 0,5 дол. залежно від пріоритету повідомлення.

**Лекція 4. Сучасний стан дистанційного банківського обслуговування**

1. Сутність дистанційного банківського обслуговування.

2. Технології дистанційного банківського обслуговування.

3. Ризики, пов’язані з дистанційним банківським обслуговуванням.

4. Захист інформації у системах ДБО.

**1. Сутність дистанційного банківського обслуговування**

З розвитком ринку банківських послуг склалася така практика обслуговування клієнтів, за якої вони зобов’язані кожного разу відвідувати банк для проведення будь-якої операції. Це означає, що банк для того, щоб обслужити клієнтів повинен створити потужну базу (інфраструктуру), і витрачати значні суми, окупність яких складає декілька років. В Україні, далеко не всі банки можуть собі дозволити  значні капіталовкладення у створення філій та відділень для обслуговування клієнтів, тому така схема забезпечення якісного банківського обслуговування не завжди прийнятна. Отже, постає питання щодо створення зручних і ефективних каналів надання банківських послуг  споживачам. На сьогоднішній день актуальним є поступовий перехід від філійної моделі до моделі дистанційного банківського обслуговування (ДБО).

Дистанційне банківське обслуговування – це загальний термін для технології, яка використовується з метою надання банківських послуг клієнтам на основі розпоряджень, переданих ними на відстані (без обов’язкового візиту до банку), за допомогою різноманітних засобів самообслуговування, найчастіше з використанням комп'ютерних і телефонних мереж. Усі операції, що не виконуються безпосередньо в офісі банку, має здійснювати система дистанційного банківського обслуговування.

Головна мета впровадження та використання дистанційного банківського обслуговування в банківській діяльності полягає в наданні рівних можливостей оперування фінансовими інструментами в будь-яких регіонах та за межами країни.

Функціонування дистанційного банківського обслуговування населення побудоване на таких принципах:

    екстериторіальність і неперервність роботи системи – клієнт може здійснювати управління коштами незалежно від того, де він знаходиться і у який час;

    загальнодоступність – засоби доступу  клієнта до системи мають бути досить поширені і прийнятні за ціною;

    множинність каналів доступу – наявність можливості використання різних каналів і в будь - якому їх поєднанні;

    інтерактивність обслуговування, яка повинна забезпечувати можливість проведення операцій у режимі самообслуговування. Водночас клієнту має бути надана можливість вільного вибору проведення операцій в інтерактивному режимі або через оператора;

    здатність проведення операцій у режимі реального часу (лише у тому разі, коли це можливо);

    мінімізація ручної обробки операцій передбачає, що дана технологія (ДБО) повинна максимально виключати або скорочувати стадії, які вимагають ручної обробки.

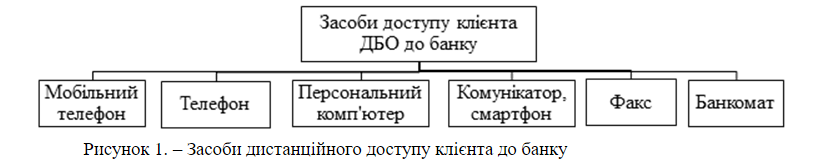
Основні суб’єкти дистанційного банківського обслуговування такі:

    клієнт – юридична або фізична особа, що відкрила рахунок у                  банку-учаснику;

    аутсорсер – спеціалізована компанія, що здійснює реєстрацію та обробку дистанційних розпоряджень клієнтів-учасників;

    банк – установа, що веде рахунки учасників і виконує розрахункові функції.

Дистанційне банківське обслуговування передбачає роботу не тільки з клієнтами банку, а також з банками-кореспондентами, підрозділами банку, до яких можна віднести: філії, відділення, віддалені каси, обмінні пункти та інше. Через систему ДБО реалізується досить широкий спектр послуг – від найпростіших інформаційних сервісів (отримання інформації щодо залишку коштів на рахунку) до більш складних, таких як отримання кредиту в режимі віддаленого доступу, розміщення заявок брокерові під час операцій на фондовому або валютних ринках тощо. За допомогою технологій ДБО банк може проводити платежі або здійснювати інші операції з коштами клієнтів на основі дистанційних розпоряджень, які вони передають до банківської установи, використовуючи різні канали та засоби доступу (телефонні, Internetтощо). (рис.1.1)



Завдяки існуванню таких засобів доступу, банк який надає можливість своїм клієнтам отриматиповний набір сервісів ДБО, стає      телекомунікаційно-фінансовим центром, до якого з різних каналів надходять розпорядження клієнтів. Клієнт такого «телекомунікаційного банку» може мати у своєму розпорядженні для здійснення операцій будь-які доступні канали або мати можливість користуватись різними комбінаціями каналів, залежно від ситуації.

Система ДБО побудована на використанні автоматизованої комп’ютерної системи, яка складається з таких компонентів:

    сервер каналу зв’язку, що забезпечує інтерфейс між системою і клієнтами у формі реєстрації дистанційних розпоряджень клієнтів і створення відповідних електронних документів у базі даних системи ДБО. Крім цього, даний сервер каналу здійснює введення інформації, яка надходить від клієнта і передає клієнтові відповіді системи. Функції і архітектура серверу каналу залежать від особливостей каналу: сервери телефонних каналів складаються з плати комп’ютерної телефонії і відповідного програмного забезпечення; сервер для каналу Інтернет – це програма на Інтернет- сервері.

    сервер обробки дистанційних розпоряджень – призначений для обробки зареєстрованих дистанційних розпоряджень клієнтів і формування на їхній основі документів (квитанцій, повідомлень, платіжних доручень тощо) і реальних проведень на внутрішніх рахунках системи ДБО.

    операційний день системи ДБО (окремий програмний комплекс або складова частина системи автоматизації банківських операцій), що призначений для збереження інформації про клієнтів, рахунки проведення операцій та інше.

Безумовно, впровадження технології ДБО є вигідним як для банків, так і для клієнтів, але використання даної системи має не тільки переваги, а й деякі недоліки. До переваг системи ДБО на рівні банку можна віднести:

    конкурентні переваги відносно інших банків, які не надають послуги ДБО;

    розширення масштабів бізнесу (оскільки збільшення клієнтської бази не обмежується кількістю філій і відділень чи персоналом банку);

    екстериторіальність банківського обслуговування (банк може обслуговувати іногородніх та іноземних клієнтів без відкриття додаткових відділень);

    можливість забезпечення цілодобового сервісу, що актуально для залучення віддалених клієнтів;

    спрощення процесу розширення бізнесу і впровадження нових продуктів (оскільки всі операції здійснюються за допомогою централізованого комп'ютеру, то вводити додаткові послуги можна швидко, без суттєвих витрат та зайвих організаційних процедур);

    спрощення процесу реалізацій комплексних фінансових продуктів (наприклад, банківських і страхових);

    суттєве скорочення організаційних витрат за рахунок вивільнення персоналу і зниження додаткових (накладних) витрат на функціонування відділень.

До основних недоліків використання системи ДБО можна віднести:

    високий рівень витрат на придбання або створення системи ДБО, її впровадження та навчання співробітників банку;

    тривалий процес перепідготовки співробітників для роботи з електронними документами;

    необхідність здійснення постійних витрат на обслуговування (у тому числі й каналів зв’язку з високою пропускною спроможністю при обслуговуванні великої кількості клієнтів).

Основними перевагами використання ДБО клієнтами банку є:

    можливість проведення операції в будь-який час і в будь-якому місці без відвідування банку;

    доступність актуальної інформації про стан рахунків, надходження коштів тощо;

    прискорення обігу коштів на внутрішньому ринку;

    здешевлення банківських операцій.

Недоліки системи дистанційного банківського обслуговування для клієнтів наступні:

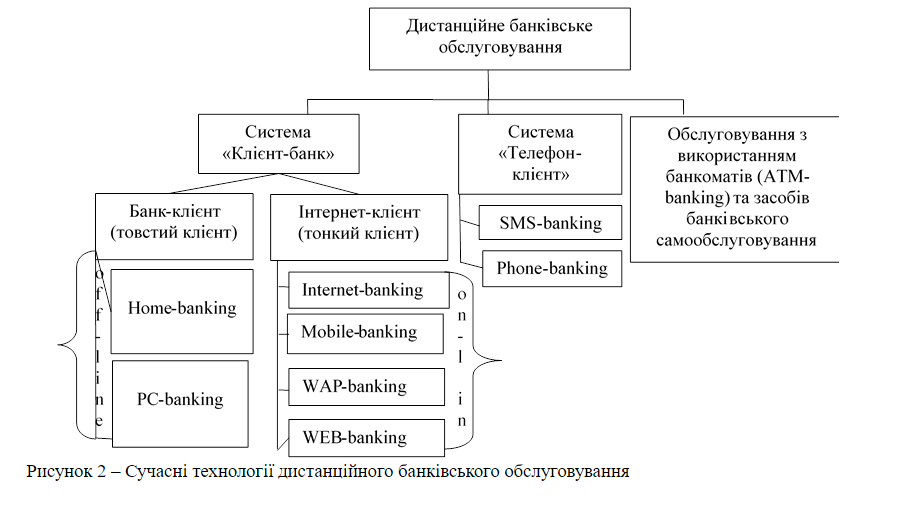
    потреба в додатковому обладнанні та більш високої кваліфікації користувачів основних каналів доступу ДБО;

    як правило, банки стягують плату за користування такою системою.

Отже, підводячи підсумок, варто відзначити, що сутність ДБО полягає у самообслуговуванні клієнтів, що у свою чергу є технологічним видом взаємодії банку з клієнтами у межах якого клієнти мають змогу користуватися послугами незалежно від працівника банківської сфери.

**2. Технології дистанційного банківського обслуговування**

З метою підвищення ефективності обслуговування своїх клієнтів, сучасні банки досить активно впроваджують системи дистанційного банківського обслуговування, які представлені на рисунку 2.



Завдяки можливостям, які надають канали дистанційного доступу клієнта добанку сьогодні стали звичними такі поняття:

    direct-banking - прямі банківські операції;

    phone-banking, telebanking – дистанційні операції телефоном;

    handy ipocket-banking - операції за допомогою мобільного телефону;

    fax-banking - операції факсом.

Однією з найперших типових технологій дистанційного банківського обслуговування сталатехнологія під назвою «Home-banking» (банківське обслуговування вдома). Дана технологія дозволяє клієнту, не відвідуючи банк, отримувати банківські послуги з надання фінансової інформації, а також здійснювати банківські операції із передачею інформації телефонними каналами, двосторонньою системою кабельного телевізійного зв’язку.

На сьогоднішній день «Home-banking» – це узагальнене поняття моделі банківської діяльності, яка базується на використанні різних каналів віддаленого доступу з метою підвищення ефективності діяльності банківської установи та охоплення нових сегментів ринку фінансових послуг.

PC-banking – забезпечує управління банківськими рахунками за допомогою комп’ютерів через спеціалізоване програмне забезпечення.           PC-banking має два напрямки: «Клієнт-Банк», якщо клієнтом є юридична особа та домашній банкінг, якщо клієнт – фізична особа.

ПОСЛУГА СЕП «КЛІЄНТ-БАНК»

*Загальна інформація про послугу*

Послуга дозволяє Клієнту віддалено управляти своїми поточними рахунками, відкритими в Банку, і формувати електронні платіжні документи (далі Електронні Документи). Для забезпечення автентичності та цілісності електронних документів в СЕП «Клієнт-Банк» використовується механізм електронно-цифрових підписів (далі – ЕЦП) під електронними документами.

Електронний Документ з ЕЦП є доказовим матеріалом при вирішенні конфліктних ситуацій.

Для підпису Електронних Документів використовуються електронно-цифрові підписи (далі – ЕЦП). Робота з ЕЦП побудована на базі криптографічного системи "ЩИТ", яка призначена для захисту оброблюваної, що зберігається та передається між комп'ютерами інформації.

У системі реалізований криптографічний алгоритм, відповідний ГОСТ 28147–89. Система строгої аутентифікації та сертифікації ключів побудована за ГОСТ 34.310-95, довжина ключа – 512 бітів.

Кожен користувач Послуги має свій ключ (ЕЦП), а також секретний код (пароль) для доступу до ключа. Таблиця відкритих ключів Клієнтів зберігається в Банку. У Клієнта зберігається відкритий ключ Банку («Майстер-Ключ»). Клієнтські ключі зберігаються на стандартних флоппі-дисках.

У разі втрати, псування носіїв ключової інформації, зміни осіб, які мають право підпису, необхідно негайно поставити до відома про це Банк для блокування старих ключів та формуванні нових.

Увага!

Кожен користувач зобов'язаний зберігати свій секретний ключ і код в таємниці. Секретність ключа користувача забезпечує таємність зашифрованої інформації і неможливість підробки його цифрового підпису.

Клієнтська частина Послуги встановлюється на комп'ютери користувачів з встановленою СУБД Pervasive.SQL та працює на платформі MS Windows. Для роботи в мережі Інтернет потрібна виділена IP-адреса комп’ютера Клієнта.

Підключення до Послуги

Для підключення до Послуги Клієнт оформлює відповідну Заяву на підключення до Послуги. Для оформлення Послуги представник Клієнта повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви, Послуга активується.

Після оформлення Послуги Банк здійснює установку, настройку програмного забезпечення СЕП «Клієнт-Банк» та навчання клієнтів роботі з Послугою.

Банк надає Клієнту «Майстер-Ключ» (пакет ініціалізації системи криптозахисту), який дозволяє Клієнту сформувати для своїх співробітників ЕЦП для роботи з Послугою.

Клієнт, за допомогою «Майстер-Ключа», створює ЕЦП «Ключ супервізора» і «Ключ-підпис».

Увага!

ЕЦП «Ключ-підпис» користувача необхідно реєструвати тільки на персональну особу – у полі «Ім’я власника підпису» необхідно вказувати строго ПІБ безпосереднього користувача системи Клієнт-Банк –співробітника Клієнта. В іншому випадку підпис буде заблокований. Підписувати за допомогою ЕЦП електронні документи в системі Клієнт-Банк для відправки їх до Банку можуть тільки співробітники Клієнта, зазначені в картці зразків підписів і відбитка печатки. Кількість ЕЦП під електронними документами Клієнта повинна відповідати кількості підписів у картці зразків підписів. В іншому випадку, електронні документи, направлених Клієнтом у банк будуть відхилені.

У разі зміни складу картки зразків підписів і відбитка печатки, необхідно заблокувати ЕЦП співробітників, які виключені з картки зразків підписів та зареєструвати ЕЦП доданих співробітників.

З моменту передачі Клієнту «Майстер-Ключа» та створення ЕЦП «супервізора» і «Підписи», відповідальним за їх використання і зберігання стає Клієнт.

Клієнт і представник Банку оформляють Акт виконаних робіт, який є підставою для виникнення зобов'язань між Клієнтом і Банком за Послуги у рамках Договору ДБО. Підключення додаткових і віддалених робочих місць для роботи з Послугою з декількох комп'ютерів всередині локальної мережі Клієнта встановлюються «Додаткові робочі місця» системи Клієнт-Банк. Якщо Клієнту необхідно працювати зі своїми банківськими рахунками з різних офісів, не пов'язаних локальною мережею, використовується «Віддалене робоче місце» СЕП «Клієнт Банк». Для установки Додаткових або Віддалених робочих місць СЕП «Клієнт Банк» необхідно оформити відповідну Заяву. Представник Клієнта повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви, здійснюються роботи з організації робочих місць. Встановлення даних робочих місць тарифікується окремо, у відповідності з діючими Тарифами Банку. Встановлення робочих місць проводиться представниками Банку та оформлюється Актом виконаних робіт. Вартість робіт включається у рахунок, який виставляється Банком наприкінці розрахункового періоду.

*Установка Аудит та Корпоративної версій СЕП «Клієнт Банк»*

Для віддаленого контролю і управління дочірніми фірмами або філіями Клієнта використовуються Аудит та Корпоративна версії СЕП «Клієнт Банк». Аудит-версія Послуги дозволяє Клієнту віддалено контролювати (переглядати) платежі, формувати виписки і переглядати залишки по рахунках підпорядкованих підрозділів.

Корпоративна версія Послуги, на додачу до функцій Аудит-версії, дозволяє Клієнту підтверджувати або скасовувати Електронні Документи, сформовані підлеглими підрозділами. Для установки Аудит та Корпоративної версій Послуги необхідно оформити відповідну Заяву. Представник Клієнта повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви, здійснюються роботи з встановлення Аудит та Корпоративної версії Послуги. Встановлення даних версій Послуги тарифікується окремо, у відповідності з діючими тарифами Банку. Установка здійснюються представниками Банку та оформлюється Актом виконаних робіт. Вартість робіт включається у рахунок, який виставляється Банком наприкінці розрахункового періоду.

*Робота з Послугою*

Робота з Послугою починається з реєстрації користувача в СЕП «Клієнт Банк». Необхідно вказати користувача, вставити дискету з власним ключем і ввести пароль. Користувачі готують Електронні Документи (платіжні доручення в національній та інвалюті, заявки на придбання і продаж валюти).

Перед відправкою в Банк Електронні Документи повинні бути підписані погодженим з Банком кількістю ЕЦП. Підписи ставлять уповноважені особи Клієнта (наприклад, Головний бухгалтер та Директор). У кожному документі відображається кількість поставлених підписів. Такі документи мають режим «На підпис». Підписані Електронні Документи переводяться користувачем Послуги в режим «Вивантажені». Документи, що знаходяться в цьому режимі, по команді Поштовий обмін будуть відправлені в Банк.

Під час з'єднання з Банком відбувається обмін інформацією, накопиченої у Банку для Клієнта (квітовка документів, виписки по рахунках та ін.), та інформацією, підготовленої Клієнтом для Банку. Після закінчення сеансу зв'язку документи потрапляють в режим «що очікують прийому Банком». Через 5-10 хвилин після відправлення документів необхідно повторно зв'язатися з Банком для прийняття квитанції про доставки документа. Документ вважається прийнятим Банком, якщо він знаходиться в режимі «Доставлений». Документ вважається проведеним Банком, якщо він знаходиться в режимі «Проведено». Документ вважається виконаним Банком, якщо він знаходиться в режимі «Виконано». У разі, якщо документи не можуть бути проведені Банком, їх переводять у стан «Відхилений» із зазначенням підстав.

Увага!

Банк несе відповідальність за виконання документів, що знаходяться в режимі «Доставлений». За виконання документів, що знаходяться на попередніх стадіях, Банк відповідальності не несе.

Електронні Документи, сформовані Клієнтом та доставлені до Банку в операційний час і в післяопераційний час, тарифікуються окремо. Вартість обробки платіжних документів визначається діючими Тарифами Банку.

На початку робочого дня Клієнт повинен зв'язатися з Банком та отримати виписки і додатки до них за попередній банківський операційний день. Підтвердженням прийому виписки служить встановлення в програмі поточного операційного дня.

Клієнт протягом дня здійснює сеанси зв'язку з Банком. При цьому він контролює зміну статусу відправлених ним документів, а також стан своїх рахунків у Банку. У випадку якщо Клієнт не згоден з діями Банку (наприклад, Клієнт не згоден з підставою, по якій документ був відхилений), слід негайно зв'язатися зі своїм Операціоністом.

У кінці робочого дня, після відправлення останнього документа до Банку та отримання підтвердження від Банку його обробки, необхідно сформувати реєстр проведених документів за день і звірити його з отриманою випискою на ранок наступного дня. У разі виявлення будь-яких розбіжностей, проінформувати свого Операціоніста. Будь-які претензії по виписці приймаються Банком протягом 10 -ти днів від дати здійснення операції. Період звірки документів визначається Банком.

*Повторна реєстрація ЕЦП*

У процесі роботи з Послугою (наприклад, у разі псування носіїв) може знадобитися повторна реєстрація ЕЦП Клієнта. Перереєстрація ЕЦП оформляється відповідною Заявою. Для оформлення реєстрації ЕЦП, представник Клієнта повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви проводяться необхідні заходи з реєстрації ЕЦП. Реєстрація ЕЦП проводиться представниками Банку на місці у Клієнта і оформляється Актом виконаних робіт. Повторна реєстрація ЕЦП тарифікується відповідно до чинних Тарифів Банку.

*Супроводження Послуги*

Консультації по роботі з Послугою – безкоштовні. У разі виникнення збоїв у роботі програмного забезпечення СЕП «Клієнт-Банк», необхідності переінсталяції робочого місця та інших ситуацій, які тягнуть за собою виїзд до Клієнта представників Банку і подальшої роботи з відновлення працездатності Послуги, Клієнт оплачує такі роботи згідно з чинними Тарифами Банку. Вартість робіт включається у рахунок, який виставляється Банком наприкінці розрахункового періоду.

*Відключення від Послуги*

Відключення від Послуги в виконується відповідно до умов цього Договору. Відключення може бути ініційовано Клієнтом, для чого оформляється відповідна Заява.

ПОСЛУГА СЕП «ІНТЕРНЕТ-БАНКІНГ»

*Загальна інформація про послугу*

Послуга дозволяє користувачам віддалено управляти своїми поточними рахунками, відкритими в Банку та формувати електронні платіжні документи (далі Електронні Документи). Для забезпечення автентичності та цілісності електронних документів в СЕП «Інтернет-Банкінг» використовується механізм електронно-цифрових підписів (далі – ЕЦП) під електронними документами. Електронний Документ з ЕЦП є доказовим матеріалом при вирішенні конфліктних ситуацій.

Криптографічний захист інформації в СЕП «Інтернет-Банкінг» заснований на сертифікованій ДСТСЗІ СБУ платформонезалежної java-кріптобібліотеці «Стандарт-Ява» компанії НВЦ «БІТІС». Сертифікат відповідності рег. No UA 1.112.0135242-06. Використовуються криптоалгоритми, реалізовані відповідно до ГОСТ 28147-89, ГОСТ 34.310-95 та ГОСТ 34.311-95.

Кожен користувач Послуги має свій ключ (ЕЦП), а також секретний код (пароль) для доступу до ключа. Клієнтські ключі повинні зберігатися у недоступних для інших осіб місцях (особисті флеш-накопичувачі, захищені розділи дисків і т. ін.). Додатково Банк пропонує Клієнтам скористатися USB-токенами – пристроями безпечного зберігання ЕЦП.

У разі втрати, псування носіїв ключової інформації, зміни осіб, які мають право підпису, необхідно негайно поставити до відома про це Банк для деактивації старих ключів та формуванні нових.

Увага!

Кожен користувач зобов'язаний зберігати свій секретний ключ і код в таємниці. Секретність ключа користувача забезпечує таємність зашифрованої інформації і неможливість підробки його цифрового підпису.

Доступ до Послуги надається на Інтернет-Сайті Банку за адресою

https://ibank.marfinbank.ua

Робота із зазначеним сайтом відбувається по захищеному протоколу HTTPS, справжність сайту підтверджується відповідним сертифікатом, який належить Банку.

Робота з Послугою здійснюється за допомогою java-аплетів, для роботи яких на комп'ютері користувача повинна бути встановлена віртуальна машина Java (http://java.com). Всі Java-аплети СЕП «Інтернет-Банкінг» підписані електронним цифровим підписом, що виданий розробнику Системи ТОВ «BIFIT». У разі якщо програми підписані іншою компанією, або не мають підпису взагалі, Клієнт повинен припинити користуватися цими java-аплетами та повинен повідомити про це Банк.

Із послугою також можна працювати безпосередньо в ПЗ «1С-Підприємство» за допомогою відповідного модуля, який розроблений постачальником системи Інтернет-Банкінг iBank2ua, компанією «BIFIT».

Додатково, у разі використання опції «Центру Фінансового Контролю», користувач може управляти одночасно декількома компаніями з одного вікна Java-аплета СЕП «Інтернет-Банкінг».

*Підключення до Послуги*

Для отримання доступу до Послуги, Клієнт самостійно проходить реєстрацію в СЕП «Інтернет-Банкінг». Реєстрація в СЕП «Інтернет-Банкінг» здійснюється за допомогою java–аплету АРМ-Реєстратор, що завантажується з Інтернет-Сайту

https://ibank.marfinbank.ua

У ході реєстрації Клієнт вказує реквізити свого підприємства та реквізити рахунків, відкритих в Банку; формує один або декілька ЕЦП і відповідні їм документи Сертифікат відкритого ключа ЕЦП. ЕЦП використовується для входу в СЕП «Інтернет-Банкінг» і підписання Електронних Документів Клієнта. Сертифікат відкритого ключа ЕЦП є підставою для оформлення Клієнту Послуги. У процесі реєстрації вказується кількість ЕЦП, які будуть необхідні для підписання Електронних Документів Клієнта (наприклад, два ЕЦП: для Директора та Головного бухгалтера).

Клієнт має можливість зареєструвати декілька співробітників свого підприємства та їх ЕЦП для роботи з СЕП "Інтернет-Банкінг", але в обов'язковому порядку це повинні бути працівники, зазначені в картці зразків підписів та печатки, тому до обробки в банку приймаються електронні документи, які підписані ЕЦП працівників, зазначених у картці зразків підписів та печатки.

Після проходження реєстрації у СЕП «Інтернет-Банкінг», Клієнт заповнює і підписує Сертифікат відкритого електронного ключа ЕЦП (або декілька, якщо є декілька ЕЦП). У полі «Телефон» Клієнт вказує номер свого мобільного телефону для СМС-авторизаціі (СМС-Авторизація – це режим підтвердження входу до системи СЕП «Інтернет-Банкінг» за допомогою одноразових паролів отриманих по СМС).

Клієнт звертається в Банк для оформлення Послуги та заповнює відповідні Заяву, Договір та інші документи для підключення до Послуги. У разі, якщо Послугу оформлює представник Клієнта, він повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви Послуга активується.

У разі потреби, допомога в реєстрація в СЕП «Інтернет-Банкінг» може бути виконана представниками Банку на місці у Клієнта (вказується Клієнтом у Заяві на підключення). У цьому випадку виїзд представників Банку до Клієнта і проведення ними відповідних робіт оформляються Актом виконаних робіт, які тарифікуються згідно з чинними Тарифами Банку.

Для підвищення рівня безпеки зберігання ЕЦП, Клієнт може скористатися USB-токенами, які є апаратними пристроями безпечного зберігання інформації. У цьому випадку Клієнт оформлює відповідний Акт прийому-передачі USB-токенів.

Після цього, Клієнт проводить реєстрацію в СЕП «Інтернет-Банкінг» вже з використанням USB-токенів. Вартість USB-токенів визначається діючими Тарифами Банку.

Також Клієнт може активувати режим IP-фільтрації, який дозволяє обмежити доступ до системи Інтернет-Банкінг Клієнта тільки з комп'ютерів клієнта, які мають реальний фіксовані IP-адреси. Для цього в Заяві Клієнт вказує необхідні дані: IP-адреси своїх комп’ютерів або мережі.

У момент оформлення Послуги, Клієнт повинен вибрати спосіб отримання одноразових паролів для входу в СЕП «Інтернет-Банкінг»: отримання одноразових пролий по СМС на свій мобільний телефон або використання OTP-токенів для генерації одноразових паролів. У другому випадку, Клієнт оформляє відповідний Акт прийому-передачі токенів. Вартість OTP-токенів визначається діючими Тарифами Банку.

Для посилення рівня безпеки Клієнт може встановити граничну суму електронних документів, понад яку електронні документи необхідно додатково підтверджувати одноразовими паролями (отриманими по СМС або за допомогою OTP-токенів).

Для роботи з Послугою через ПЗ «1С-Підприємство», необхідно скачати модуль «iBnak2UA для 1С-Підпріємства» з сайту [https://ibank2.ua](https://ibank2.ua/) та встановити його згідно з відповідною інструкцією <https://ibank2.ua/1c.html.> Для роботи з модулем «iBank2UA для 1С-Підпріємства» ключі ЕЦП повинні зберігатися тільки на USB-токенах. Ключі ЕЦП у вигляді файлів не підтримуються.

Через ПЗ «1С-Підприємство» можливо працювати тільки з платіжними документами в національної валюті.

У разі використання опції «Центр Фінансового Контролю», клієнту необхідно вказати дані т.з. Керуючих ЦФК, які від імені клієнта будуть керувати його рахунками у СЕП «Інтернет-Банкінг».

Термін дії ключів ЕЦП – 1 рік, у разі активації використання одноразових паролів – 10 років.

*Робота з Послугою*

Робота з Послугою відбувається в java-аплеті АРМ-Клієнт, що завантажується з Інтернет-Сайту Банку за адресою

https://ibank.marfinbank.ua

Для входу в СЕП «Інтернет-Банкінг» використовується ЕЦП клієнта. Система дозволяє переглядати залишки по рахунках клієнта, формувати виписки за ними за довільний період і формувати Електронні Документи (платежі, заявки на придбання і покупку валюти), які є підставою для проведення Банком платежів. Також працювати с Послугою можливо в ПЗ «1С-Підприємство» за допомогою модулю «iBnak2UA для 1С-Підпріємства», де користувачу доступно формування гривневих платіжних доручень та отримування виписок по банківських рахунках Клієнта.

Створені Клієнтом Електронні Документи мають статус «Новий». Для проведення Банком Електронних Документів Клієнта їх необхідно підписати за допомогою одного або декількох ЕЦП Клієнта, після чого документи отримують статус «Доставлений». Після доставки документів в Банк, вони отримують статус «На обробці». Після обробки документи набувають статусу «Виконано». Документи зі статусом «Виконано» вважаються проведеними. У разі якщо документи не можуть бути проведені Банком, їх переводять у стан «Відхилений» із зазначенням підстав.

Увага! Банк несе відповідальність за виконання документів, що знаходяться в режимі «Доставлений». За виконання документів, що знаходяться на попередніх стадіях, Банк відповідальності не несе.

Електронні Документи, сформовані Клієнтом та доставлені до Банку в операційний час і в післяопераційний час, тарифікуються окремо. Вартість обробки платіжних документів визначається чинними Тарифами Банку.

Клієнт протягом дня підключається до Послуги. При цьому він контролює зміну статусу відправлених ним документів, а також стан своїх рахунків у Банку. У випадку якщо Клієнт не згоден з діями Банку (наприклад, Клієнт не згоден з підставою, по якій документ був відхилений), або виявлені розбіжності у виписках по рахунках, слід негайно зв'язатися зі своїм Операціоністом. Будь-які претензії за виписками по рахунках приймаються Банком протягом 10-ти днів від дати здійснення операції.

*Блокування та реєстрація нових / додаткових ЕЦП, блокування OTP-токенів*

У процесі роботи з Послугою може знадобитися блокування поточного ЕЦП Клієнта (наприклад, у разі його компрометації) і реєстрація нового ЕЦП, або блокування OTP-токенів у разі їх втрати.

Блокування поточного ЕЦП Клієнта чи OTP-токена може бути зроблено в телефонному режимі, після звернення Клієнта в Банк до свого Операціоніста. Після цього, Клієнту необхідно звернутися до Банку для письмового оформлення Заяви на блокування ЕЦП чи токена (якщо це не зроблено, заблокований ЕЦП чи токен можуть бути знову активовані Банком).

Реєстрація нових ЕЦП проводиться Клієнтом самостійно, в АРМ Реєстратор, що завантажується з Сайту Банка. Процес аналогічний процесові реєстрації в СЕП «Інтернет-Банкінг», але є скороченим: немає необхідності у вказуванні реквізитів підприємства та рахунків Клієнта. Після створення нового ЕЦП необхідно сформувати Сертифікат відкритого ключа ЕЦП. Із заповненим і підписаним Сертифікатом Клієнт звертається до Банку, де оформлює Заяву на реєстрацію нового ЕЦП. Для оформлення нового ЕЦП або блокування поточного, представник Клієнта повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви, блокується поточний, або реєструється новий ЕЦП.

*Супроводження Послуги*

Консультації по роботі з Послугою безкоштовні. У разі виникнення збоїв у роботі програмного забезпечення Послуги, необхідності налаштування робочого місця Клієнта, реєстрації ЕЦП та інших ситуацій, які тягнуть за собою виїзд представників Банку до Клієнта і подальші роботи з відновлення працездатності Послуги, Клієнт оплачує такі роботи згідно з чинними Тарифами Банку. Вартість робіт включається у рахунок, який виставляється Банком наприкінці розрахункового періоду.

*Відключення від Послуги*

Відключення від Послуги виконується відповідно до умов Договору. Може бути ініційовано Клієнтом, для чого оформляється відповідна Заява.

ПОСЛУГА МОБІЛЬНИЙ БАНКІНГ

Послуга Мобільний Банкінг призначена для надання користувачам можливості управління своїми рахунками та платіжними документами СЕП «Інтернет-Банкінг» за допомогою мобільних пристроїв на базі платформ Android та iOS. Послуга надається клієнтам банку, які вже є користувачами послуги СЕП «Інтернет-Банкінг». Послуга оформляється на один мобільний пристрой Клієнта (чи його співробітника).Для оформлення Послуги на інший мобільний пристрій Клієнта, необхідно ще одне оформлення Послуги.

*Підключення до Послуги*

1. Встановити на свій мобільний пристрій програмне забезпечення iBank2UA з Google Play абоApple Store (для Android:

https://play.google.com/store/apps/details?id=com.bifit

для Apple:

https://itunes.apple.com/us/app/ibank2ua/id548267780

2. Згенерувати ЕЦП на мобільному пристрої при першому запуску програми та отримати в програмі ідентифікатор Мобільного Банкінгу.

3. Звернутися в банк для оформлення Послуги та пред'явити співробітнику банку мобільний пристрій та ідентифікатор Мобільного Банкінгу на ньому. У процесі оформлення послуги, необхідно заповнити та підписати Заяву на підключення Послуги та Сертифікат відкритого ключа, який відповідає ЕЦП, що згенерований на мобільному пристрої. Заява та Сертифікат повинні мати підпис керівника тапечатку Клієнта.

Увага!

До послуги Мобільний Банкінг на одному мобільному пристрої (один ідентифікатор Мобільного Банкінгу) можна підключити декілька підприємств, при умові що цим пристроєм буде користуватися тільки одна особа. Для підключення декількох підприємств до одного мобільного пристрою, необхідно скласти стільки ж заяв на підключення до послуги.

*Відключення від Послуги чи блокування мобільного пристрою*

Для відключення від Послуги або блокування одного з використовуваних мобільних пристроїв, необхідно звернутися в банк і заповнити відповідну Заяву. У Заяві необхідно вказати ідентифікатор мобільного пристрою, який відповідає мобільному пристрою, що блокується.  Заява повинна мати підпис керівника та печатку Клієнта.

*Розблокування мобільного пристрою*

Для розблокування мобільного пристрою, наприклад у випадку багаторазового невірного введення пароля, необхідно направити в банк по електронній пошті, через систему Інтернет-Банкінг лист у довільній формі, з проханням розблокувати мобільний пристрій. У листі обов'язково вказати ідентифікатор Мобільного Банкінгу BIFITID. Після розблокування пристрою, користувач отримає підтверджує СМС повідомлення.

ПОСЛУГА «СМС-БАНКІНГ»

Для підключення до Послуги Клієнт звертається до Банку та заповнює відповідну Заяву. Для оформлення Послуги представник Клієнта повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви, Послуга активується. Послуга оформляється на один номер мобільного телефону Клієнта. Для оформлення Послуги на інший номер мобільного телефону Клієнта, необхідно ще одне оформлення Послуги. Клієнт отримує СМС-повідомлення про будь-якіфінансові операції, які викликають зміни балансу контрольованих рахунків.

Вартість підключення до Послуги та її обслуговування визначаються чинними Тарифами Банку. Підставою для виникнення зобов'язань між Клієнтом і Банком за Послуги у рамках цього Договору є Заява Клієнта на підключення до Послуги.

Для відключення від Послуги Клієнт повинен звернутися до Банку та оформити відповідну Заяву.

ПОСЛУГА «EMAIL-БАНКІНГ»

Для підключення до Послуги Клієнт звертається до Банку та заповнює відповідну Заяву. Для оформлення Послуги Клієнт повинен мати при собі Заяву з підписом керівника і печаткою Клієнта. Після ідентифікації Клієнта та оформлення Заяви, Послуга активується.

При оформленні Послуги Клієнт зазначає у Заяві електронну адресу, на яку будуть приходити виписки. Виписки приходять щодня, крім вихідних та святкових днів.

Вартість підключення до Послуги і її обслуговування визначаються чинними Тарифами Банку. Підставою для виникнення зобов'язань між Клієнтом і Банком за Послуги у рамках цього Договору є Заява Клієнта на підключення до Послуги.

Для відключення від Послуги Клієнт повинен звернутися до Банку та оформити відповідну Заяву.

Однією з сучасних технологій організації дистанційного банківського обслуговування стала й система «Telebanking», яка згодом отримала назву «Телефон-клієнт».

Система «Telebanking» – це різновид системи ДБО, що, перш за все, забезпечує з’єднання клієнта збанківським комп’ютером за допомогою телефону.

Дистанційна послуга «Telebanking» була і залишається на сьогоднішній день однією з найпривабливіших банківських послуг, оскільки і сьогодні є найдешевшою і найпростішою у використанні, завдяки чому вона й отримала прихильність широкого кола споживачів банківських послуг: підприємців, менеджерів різних рівнів, людей, які часто бувають у відрядженні і т.д.

Сьогодні система «Телефон-клієнт» – це банківський сервіс, заснований на використанні певних можливостей телефонів із тоновим набором номера. Дана система дозволяє клієнтові за допомогою кнопок даного телефонного апарата віддавати розпорядження стосовно здійснення фінансових операцій, а також замовляти та отримувати відповідну інформацію про рух коштів на рахунку. Наприклад, процедура оплати рахунку телефоном здійснюється наступним чином: клієнт підключається до банківського комп’ютера і за допомогою клавіш уводить відповідні реквізити. Якщо поточний рахунок одержувача відкрито в тому ж банку, він негайно кредитується, якщо ні-одержувачеві надсилається чек.

За допомогою даної послуги клієнт банку може здійснювати будь-які повсякденні фінансові операції без відвідування банківської установи. Практика користуванням такою послугою демонструє, що через систему «Телефон-клієнт» частіше за все здійснюється такі операції: платежі за комунальні послуги,електроенергію, телефон. Окрім цього, у клієнта є можливість дізнатися про надходження коштів на рахунок, поповнити кредитну картку та одержати готівку в будь-якому банкоматі, перевести тимчасово вільні кошти на депозит, проконтролювати операції за рахунком а також довідатися про поточний залишок на рахунку.

Дані послуги, клієнт може отримати з будь-якого телефонного аппарата –стаціонарного, мобільного, міського телефону-автомату.

Дистанційна послуга «Телефон-клієнт» включає в себе технології             «SMS-banking» та «Phone-banking».

«SMS-banking» – це послуга ДБО, яка надається у будь-якій час з використанням номеру мобільного телефона клієнта, попередньо зареєстрованого в банку. За допомогою SMS-повідомлень відбувається обмін інформацією та передача команд для виконання банківських операцій. При використанні «SMS-banking»відсутня необхідність встановлення клієнтської частини програмного забезпечення на мобільний телефон.

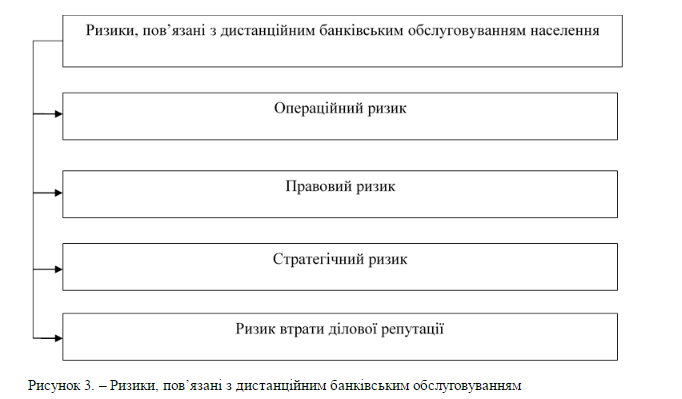
Дана система базується на використанні технології передавання коротких повідомлень (Shot Message Service), як спеціального каналу передачі даних. Технологія надає клієнтові можливість мати достовірну інформацію про стан свого рахунку. Ця технологія особливо важлива у разі збільшення кількості операцій з оплати безготівковим шляхом, коли власнику картки необхідно мати повний контроль за банківським рахунком. Підключення до даної послуги може відбуватися через банкомат, а також безпосередньо увідділенні банку. Основним недоліком даної послуги є те, що інформація про картковий рахунок стає відомою операторам мобільного зв’язку і банки не можуть гарантувати конфіденційність інформації.

Обслуговування з використанням банкоматів (АТМ-banking) та засобів банківського самообслуговування є одними з найбільш популярних у світі і в Україні.

Банкомати і термінали, входять до системи  ДБО, через те, що надають майже повний спектр банківських послуг дистанційно та забезпечують можливість дублювання основних функцій стандартного Банк-клієнт, який використовується приватними (фізичними) особами для здійснення платежів.

**3. Ризики, пов’язані з дистанційним банківським обслуговуванням.**

Виокремлююють ряд ризиків, які виникають при використанні дистанційного банківського обслуговування (рис. 3)



Причинами виникнення операційного ризику при застосуванні системи ДБО можуть бути:

    неналежна організація інформаційних потоків, внутрішньобанківських процесів і процедур, а також забезпечення інформаційної безпеки як у самій кредитної організації, так і у провайдерів;

    порушення режимів функціонування використовуваних для     Інтернет-банкінгу інформаційних систем банку, пов'язані з аваріями, відмовами, збоями устаткування і програмного забезпечення банку або його провайдерів;

    помилки або збої в роботі апаратно-програмного забезпечення ДБО, що можуть призвести до порушень цілісності даних в інформаційному контурі ДБО;

    дії відносно банку у вигляді неправомірного доступу із застосуванням системи ДБО до його інформаційних ресурсів;

    недостатня продуктивність і захищеність інформаційних систем та інформаційно-телекомунікаційних мереж як банку, так і провайдерів, задіяних у інформаційному контурі ДБО (з урахуванням можливого неправомірного доступу із застосуванням Інтернет-технологій);

    помилки службовців банку, його клієнтів або провайдерів (у тому числі розробників програмного забезпечення систем ДБО), а також недостатній рівень контролю (у тому числі програмного) за можливістю їх вчинення;

    невиконання постачальниками послуг (виконавцями робіт) договірних зобов’язань перед кредитною організацією;

    невиконання кредитною організацією зобов’язань перед клієнтами через неналежної якості апаратно-програмне забезпечення систем ДБО.

До основних причин виникнення правового ризику пов’язаних із застосуванням системи ДБО можна віднести:

    порушення банком вимог законодавства України, в тому числі нормативних актів НБУ, через недоліки (помилки) у апаратно-програмному забезпеченні системи ДБО;

    недосконалість правової системи (неврегульованість окремих наданих питань дистанційного банківського обслуговування та відповідальності сторін, в тому числі при транскордонному наданні банківських послуг);

    неправомірний доступ до конфіденційної інформації під час її обробки, передачі або зберігання як у банку, так і у провайдерів, з якими кредитна організація уклала договори на обслуговування;

    недостатність опрацювання банком правових питань при укладанні договорів з провайдерами на надання послуг з виконання функцій обробки, передачі, зберігання банківської та іншої інформації, в тому числі визначення відповідальності провайдерів при невиконанні зобов'язань з обслуговування в рамках системи ДБО.

Причинами виникнення стратегічного ризику при застосуванні системи ДБО можуть бути можливі збитки внаслідок помилкових рішень органів управління кредитної організації по відношенню до впровадження, супроводу та розвитку системи ДБО, що може бути обумовлено:

    відсутністю або недоліками стратегічного плану розвитку, що передбачає застосування системи ДБО;

    неможливістю досягнення стратегічних цілей, поставлених банком, у зв’язку з відсутністю або незабезпеченням в повному обсязі необхідними ресурсами (фінансовими, матеріально-технічними, людськими) і невиконанням організаційних заходів (управлінських рішень) у сфері надання послуг через систему ДБО;

    надмірними витратами на впровадження та обслуговування системи ДБО або їх нерентабельністю, а також вимушеним відмовитись від  використання вже впроваджених в експлуатацію технологій банківського обслуговування і відповідних інформаційних систем.

Причинами виникнення ризику втрати ділової репутації (репутаційний ризик) при застосуванні системи ДБО можуть бути:

    витік з банку конфіденційної інформації, в тому числі порушення банківської таємниці (через мережеві атаки в умовах дистанційного банківського обслуговування неправомірного доступу до інформаційних ресурсів);

    залучення банку у протиправну діяльність із застосуванням системи ДБО через неналежне виконання обов’язків з ідентифікації клієнтів, встановлення та ідентифікації вигодонабувачів і встановлення осіб, уповноважених розпоряджатися грошовими коштами, що знаходяться на рахунку, використовуючи аналог власноручного підпису, коди, паролі та інші засоби, що підтверджують наявність зазначених повноважень, а також помилок у повідомленнях про авторизацію і аутентифікації при здійсненні банківських операцій;

    негативна оцінка клієнтами якості наданого дистанційного банківського обслуговування із застосуванням системи ДБО.

**4. Захист інформації у системах ДБО.**

|  |  |
| --- | --- |
| НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ | |
| ЛИСТ | |
| 24.12.2013  № 25-111/29563 | |
| Генеральний департамент інформаційних технологій та платіжних систем  Департамент платіжних систем | Банкам України та їх філіям  Асоціації "Український кредитно-банківській союз"  Незалежній асоціації банків України |

Про посилення захисту інформації при здійсненні переказу коштів

З огляду на стрімкий розвиток високотехнологічних банківських продуктів нового покоління, банкам необхідно звертати особливу увагу на забезпечення інформаційно-технологічної безпеки при наданні послуг клієнтам, зокрема, з переказу коштів за допомогою систем дистанційного обслуговування (далі - СДО).

Враховуючи те, що в більшості випадків несанкціоновані перекази коштів з рахунків пов'язані з неналежним виконанням клієнтами правил користування СДО, Національний банк України вже звертав увагу банків щодо необхідності проведення роз'яснювальної роботи з клієнтами стосовно дотримання ними вимог із захисту інформації при здійсненні переказу коштів з використанням СДО.

Разом з тим, з метою недопущення випадків несанкціонованого доступу до рахунків клієнтів, рекомендуємо банкам переглянути укладені з клієнтами договори банківського рахунку з надання послуг з переказу коштів за допомогою СДО (далі - договір) та доповнити їх умовами, зокрема, щодо:

здійснення обов'язкової автентифікації клієнта під час надання доступу до системи дистанційного обслуговування, у тому числі пропонується визначити випадки, коли обов'язковим є застосування автентифікації, відмінної від простої автентифікації за паролем;

максимального розміру однієї трансакції, яка може здійснюватися без додаткового підтвердження платежу клієнтом;

обов'язкового дотримання правил використання та належного зберігання носіїв ключової інформації (з включенням цих правил як додатка до договору);

права банку на виконання періодичних перевірок щодо дотримання клієнтом вимог захисту інформації на робочих місцях системи дистанційного обслуговування та зберігання носіїв ключової інформації тощо.

Також уважаємо, що у договорі може обумовлюватися право банку на списання коштів з рахунку клієнта у разі надходження від банку ініціатора платежу повідомлення про несанкціонований переказ коштів з рахунку платника.

На нашу думку, співпраця банків з клієнтами з питань захисту інформації щодо переказу коштів на усіх етапах її формування, обробки, передачі і зберігання, своєчасне інформування клієнтів про нові засоби захисту інформації, проведення відповідних організаційних заходів тощо дозволять мінімізувати ризики несанкціонованого доступу до рахунків клієнтів та забезпечать належний рівень безпеки при здійсненні переказу коштів за допомогою СДО.

В рамках концепції безпеки систем дистанційного обслуговування рекомендується реалізувати, як мінімум, такі процедури:

- розмежувати права користувачів;

- провести контроль парольної політики, використання криптографії та поводження з криптографічними ключами;

- антивірусний захист;

- забезпечення безпеки корпоративної мережі;

- міжмережеве екранування,

- аналіз захищеності і внутрішнього аудиту;

- резервне копіювання та аварійне відновлення;

- забезпечення фізичного захисту;

- забезпечення безпеки прикладного та системного програмного забезпечення;

- моніторинг подій та реагування на інциденти інформаційної безпеки;

- підвищення обізнаності клієнтів та співробітників в питаннях інформаційної безпеки;

- оновлення програмних засобів.

При розгляді архітектури систем дистанційного обслуговування, можна виокремити декілька основних рівнів: програмне забезпечення клієнта, прикладне ПЗ, системне ПЗ (web-сервер, СУБД, операційна система) і мережева інфраструктура, фізичне розміщення і користувачі.

Безпека «клієнтської сторони» – головний біль фахівців з інформаційної безпеки. Основним заходом захисту в даному випадку виступає двофакторна аутентифікація (одноразові паролі, sms-код, значення криптокалькулятора, криптотокен). Все частіше банки розробляють для клієнтів навчальні програми, які висвітлюють основні питання інформаційної безпеки та протидії шахрайству. Однак, незважаючи на всі вжиті заходи, атаки на клієнтів активно здійснюються шахраями і є одним з найпоширеніших способів компрометації.

Все частіше користувачі систем дистанційного банківського обслуговування виявляють факти несанкціонованих списань коштів з рахунків та несправність комп'ютера на якому встановлена система по типу ,,Клієнт-Банк”. Зловмисники отримують доступ до комп'ютера жертви шляхом інсталювання шкідливого програмного забезпечення. Для інфікування комп'ютерів шахраї вдаються до різних методів, зокрема і надсилання електронних листів на електронні поштові скриньки в яких міститься шкідлива програма. При відкриванні такого листа, жертва навіть не підозрює про те, що її комп'ютером дистанційно може керувати стороння особа.

Для мінімізації ризику шахрайських дій під час роботи з системою дистинційного банківського обслуговування «Клієнт-Банк» необхідно:

 1. Використовувати ліцензійне програмне забезпечення на комп’ютері, з якого здійснюється платежі засобами систем дистанційного обслуговування.

 2. Користуватися ліцензійним антивірусним програмним забезпеченням та міжмережевим екраном (Brandmauer, Firewall), які блокують втручання в роботу з платежами шкідливого програмного забезпечення, та слідкувати за своєчасним оновленням антивірусних баз.

 3. Обмежити доступ до комп'ютера, де встановлена система «Клієнт-Банк».

 4. Зберігати ключі системи «Клієнт-Банк» на змінному носії інформації. Не передавати носій з ключем системи «Клієнт-Банк» третім особам.

 5. Не зберігати на змінному носії, який використовується для ключів електронно-цифрового підпису системи «Клієнт-Банк», іншу інформацію та захистити змінний носій від запису.

 6. Використовувати паролі, які складаються з букв, цифр та символів. Не використовувати тривіальні й прості паролі. Довжина пароля має бути не менше 7 знаків.

 7. Періодично змінювати пароль. Рекомендований термін зміни пароля – не більше 90 днів.

 8. Не записувати пароль на папері, моніторі, у файлі тощо та не повідомляти його третім особам. Якщо у Вас виникла підозра, що пароль став відомий стороннім особам, негайно змініть його або зверніться до адміністраторів з технічної підтримки системи «Клієнт-Банк» для отримання додаткових консультацій.

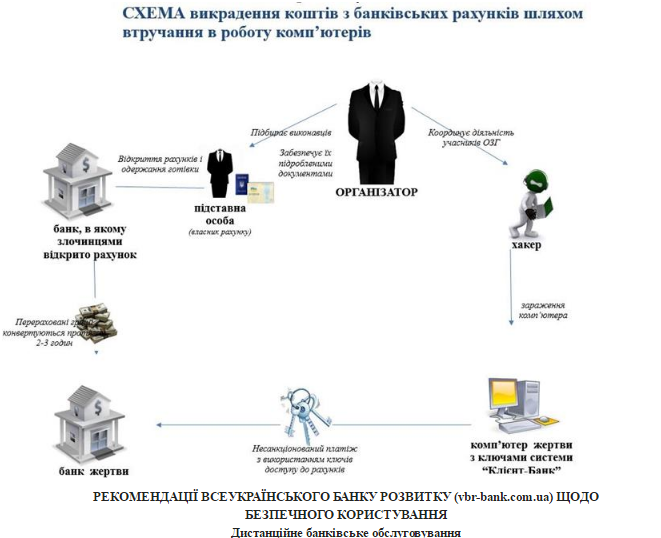
 9. Обов’язково використовувати пункт меню «Вихід» при закінченні роботи в системах дистанційного обслуговування.

 10. У разі виявлення несправності системи дистанційного банківського обслуговування необхідно відразу звернутися до відповідної банківської установи з метою отримання інформації по рахунку, викликати банківського спеціаліста для її переналаштування.

 11. Ні в якому випадку не надавати персональний комп’ютер з встановленою на ньому системою “Клієнт-Банк” незнайомим особам, або ІТ-спеціалістам телефон яких виявили з об’яв розміщених в мережі Інтернет, або отримали у своїх знайомих.

 12. Не дозволяти будь кому, та самим не встановлювати програмні продукти за допомогою яких можливий віддалений доступу до ПК з встановленою системою дистанційного банківського обслуговування “Клієнт-Банк”.

 13. Пам’ятайте про те, що халатне ставлення до визначених банками умов використання системи “Клієнт-Банк” може залишити Вас без готівки, тому що зловмиснику вистачить лише одного натискання на кнопку клавіатури щоб створити псевдо платіжне доручення та переказати кошти на підконтрольні йому рахунки.   
© Сайт Департаменту Кіберполіції України - [https://www.cybercrime.gov.ua](https://www.cybercrime.gov.ua/)



**РЕКОМЕНДАЦІЇ ВСЕУКРАЇНСЬКОГО БАНКУ РОЗВИТКУ (vbr-bank.com.ua) ЩОДО БЕЗПЕЧНОГО КОРИСТУВАННЯ послугами дистанційного банківського обслуговування**

Для забезпечення належної якості послуг та безпеки систем дистанційного банківського обслуговування банки рекомендують:

Використовувати лише ліцензійне програмне забезпечення на робочих місцях.

Використовувати ліцензійне антивірусне програмне забезпечення та своєчасно виконувати оновлення антивірусних баз.

За жодних обставин не зберігати таємні ключі на жорсткому диску комп'ютера. Використовувати для їх збереження лише зовнішні носії (токени і т.п.).

Після закінчення роботи із системою дистанційного обслуговування та під час перерв необхідно від'єднувати носій із секретним ключем від комп'ютера.

Після закінчення роботи із системою дистанційного обслуговування обов'язково здійснювати вихід із системи для недопущення використання системи сторонніми особами.

Не використовувати будь-який віддалений доступ до робочого комп'ютера, на якому встановлено систему дистанційного обслуговування.

У разі будь-якої підозри на компрометацію ключів системи дистанційного банківського обслуговування необхідно негайно сповіщати про це Банк.

Контролювати стан Вашого поточного рахунку.

Не використовувати комп'ютер із встановленою системою дистанційного обслуговування для перегляду сумнівних інтернет-ресурсів та не пов'язаних з роботою, які найчастіше є джерелом поширення шкідливих програм (непомітного втручання кібер-шахраїв).

Не завантажувати та не зберігати на комп'ютері із встановленою системою дистанційного обслуговування підозрілі файли, отримані з невідомих/підозрілих джерел, надіслані електронною поштою від невідомих адресантів і т.п. Такі файли необхідно видаляти або - у разі необхідності завантаження - перевіряти антивірусною програмою.

Зберігати зовнішні носії ключової інформації (токени і т.п.) у сейфі.

Не передавати стороннім особам носії ключової інформації та не повідомляти їм паролі доступу до системи дистанційного обслуговування.

При виявленні/підозрі про факти доступу сторонніх осіб до ключової інформації негайно ініціювати блокування та зміну ключової інформації.

Не зберігати та не записувати паролі таємних ключів разом із носіями ключів (токени, usb flash і т.п.).

Уникати використання для роботи із системою дистанційного обслуговування комп'ютерів, встановлених у публічних місцях, чужих ноутбуків та комп'ютерів, смартфонів та інш.

Не відповідати на підозрілі листи з проханням надіслати секретний ключ електронного цифрового підпису, пароль та інші конфіденційні дані!

**ДОДАТКОВІ ЗАСОБИ ЗАХИСТУ**

Для підвищення безпеки використання систем дистанційного обслуговування замовляйте у своєму Банку додаткові засоби захисту.

|  |  |
| --- | --- |
| Додатковий засіб захисту | Результат від використання |
| Використання засобів для забезпечення безпечного зберігання таємних ключів - USB-токенів, SMART-карток тощо. | Унеможливлює компрометацію таємного ключа. |
| Використання SMS-оповіщення. | Унеможливлює проведення операції без уведення одноразового паролю, який надходить у SMS-повідомленні. |
| Використання електронних пристроїв ідентифікації користувача. | Унеможливлює вхід до системі без уведення одноразового паролю, який генерується спеціальним пристроєм. |

Індикатори несанкціонованого втручання в роботу комп'ютера, на якому встановлено систему дистанційного обслуговування.

1.    Перебій у роботі комп'ютера, раптове перезавантаження системи.

2.    Неможливість або ускладнення запуску програм та додатків.

3.    Наявність невідомих записів в історії входів до системи та проведення операцій.

4.    Поява незрозумілих вікон, незрозуміле уповільнення дії, самостійна активність (наприклад, самостійний рух курсора комп'ютерної миші з відкриттям вікон, запуском програм та інш.).

5.    Сповіщення антивірусного програмного забезпечення про виявлений вірус.

6.    Підвищений трафік мережевого обміну (для адміністраторів ctrl+shift+Esc, закладка «Networking»).

Порядок дій у разі виявлення випадку несанкціонованого доступу до рахунку або підозри на компрометацію логіну, паролю чи ключа.

У разі виявлення несанкціонованого переказу коштів у системі ДБО Клієнту (потерпілому) - юридичній особі, приватному підприємцю чи іншому суб'єкту господарювання необхідно:

1.    Негайно звернутися до підрозділу свого Банку, відповідального за обслуговування рахунку (до свого обслуговуючого менеджера, у Контакт-Центр, до співробітника служби банківської безпеки (за необхідності) тощо), по телефону або іншим доступним засобом зв'язку та сповістити банківського працівника про факт несанкціонованого переказу коштів;

2.    Вимкнути комп'ютер із системою ДБО, знеструмивши його (примусово відключити електроживлення в обхід штатної процедури завершення роботи, витягти всі акумуляторні батареї з ноутбука, від'єднати шнур живлення). Якщо робота з ДБО виконується через віддалений доступ, необхідно завершити сесію. За відсутності можливості знеструмлення комп'ютера здійснити відключення відповідно до штатної процедури і записати зазначений факт. Негайно сповістити IT-підрозділ та внутрішню службу безпеки своєї компанії або директора про інцидент.

**Лекція 5. Аналіз захищеності протоколу SET.**

(Secure Electronic Transaction)

1. Загальні відомості про SET.

2. Головні можливості SET.

3. Учасники транзакцій SET.

4. Дуальний підпис.

5. Опрацювання платежів.

6. Перспективи захисту платежів в Інтернет.

**1. Загальні відомості про SET.**

Протокол SET (Secure Electronic Transaction — протокол захищених електронних транзакцій) являє собою відкриті специфікації, розроблені з метою захисту транзакцій, в Internet за допомогою пластикових платіжних карток. Протокол SETvl, з'явився у 1996 р. через необхідность створення стандарту захисту для кредитних карток MasterCard і Visa. У розробці специфікацій брали участь багато відомих компаній, включаючи IBM, Microsoft, Netscape, RSA, Terisa і VeriSign. Починаючи з 1996 року покладена в основу протоколу концепція пройшла ретельну перевірку практикою, і до 1998 року на ринку з'явилися перші продукти реалізації протоколу SET.

SET є набором протоколів захисту і форматів даних, що дозволяють захищеним чином використовувати наявну інфраструктуру платіжних систем пластикових карток у відкритих мережах типу Internet. По суті, SET забезпечує наступні три види сервісу:

•                  Створення захищеного комунікаційного каналу, який зв'язує всі сторони, що беруть участь у транзакції.

•                  Забезпечення довіри за допомогою цифрових сертифікатів X509v3.

•                  Забезпечення таємності через те, що інформація виявляється доступною тільки учасникам транзакції і тільки тоді і там, де вона необхідна.

Повна специфікація SET описується в трьох книгах, опублікованих у 1997 р.

•                  Книга 1. Опис можливостей застосування (Business Description), 80 стор.

•                  Книга 2. Керівництво програміста (Рrоgrаmmеr's Guide), 629 стор.

•                  Книга 3. Формальне визначення протоколу (Formal Protocol Definition), 262 стор.

Усе разом це складає 971 сторінку специфікацій. Для порівняння відзначимо, що специфікації SSL (Secure Sockets Layer — рівень захищених сокетів) займають 63 сторінки, а специфікації TLS (Transport Layer Security — захист на транспортному рівні) — 71 сторінку.

У книзі 1 специфікацій SET визначені вимоги, що повинні виконуватися при обробці платежів по кредитних картах вInternet.

•                  Конфіденційність платежу й інформації про замовлення. Необхідно гарантувати власникам пластикових карт, що дана інформація надійно захищена і виявиться доступною тільки тому, кому вона призначена. Конфіденційність до того ж зменшує ризик обману кожного з учасників при здійсненні транзакції. Для забезпечення конфіденційності застосовується шифрування.

•                  Гарантія цілісності всіх переданих даних означає, що в ході передачі інформація, яка міститься в повідомленні SET, незазнає ніяких змін.

•                  Автентифікація пред'явника кредитної картки як законного власника відповідного рахунка. Механізм, що зв'язує пред'явника кредитної картки з відповідним номером рахунка, повинен зменшувати імовірність шахрайства і знижувати загальну вартість обробки платежів. Для перевірки того, що пред'явник кредитної картки є законним власником відповідного дійсного рахунка, застосовуються такі засоби, як цифровий підпис і сертифікати.

•                  Автентифікація продавця як особи, що має право приймати транзакції по кредитних картках, за допомогою з'ясування його зв'язку з відповідною фінансовою організацією. Власники платіжних карт повинні мати можливість ідентифікувати продавців, яким вони можуть направляти захищені транзакції. У цьому випадку також використовуються цифрові підписи і сертифікати.

•                  Гарантоване використання кращих конструктивних рішень і методів захисту для забезпечення найвищого ступеня захисту всіх легальних учасників електронних комерційних транзакцій. Специфікації SET будуються на застосуванні криптографічних алгоритмів і протоколів, що мають високий рівень захищеності і добре перевірені.

•                  Незалежність протоколу від механізмів захисту транспортування даних при відсутності обмежень на використання таких механізмів. SET може забезпечувати захист, спираючись безпосередньо і винятково на стек протоколів TCP/IP. Але при цьому SET ніяк не впливає на роботу інших механізмів захисту, таких як IPSec чи SSL/TLS, і не залежить від них.

•Сприяння і підтримка сумісності між прикладними програмними і мережними продуктами різних постачальників. Протоколи і формати SET не залежать від апаратних платформ, операційних систем і програмного забезпечення, призначеного для роботи в Web.

**2. Головні можливості SET.**

Щоб відповідати описаним вище вимогам, у протоколі SET peaлізовані такі можливості.

•                 Конфіденційність інформації. Інформація про рахунок власника карти і платежі захищається під час пересилання по мережі.  Цікава і важлива особливість SET полягає в тому, що продавець при цьому не може з'ясувати номер кредитної картки її власника – ця інформація виявляється доступною тільки банку, який видав кредитну картку. Для забезпечення конфіденційності використовується шифрування за традиційною схемою за допомогоюсиметричного алгоритму DES (Data Encryption Standard) а також за допомогою несиметричного алгоритму RSA(абревіатура від прізвищ Rivest, Shamir та Adleman).

•                 Цілісність даних. Інформація про платіж, що посилається власником карти продавцю, містить інформацію про замовлення, особисті дані й інструкції для здійснення платежу. SET гарантує, що зміст відповідних повідомлень не буде змінено під час їх передачі. Цілісність даних досягається за допомогою цифрових підписів RSA, що використовують хеш-коди SHA-1 (Secure Hash Algorithm 1).

•                  Автентифікація рахунка власника карти. SET дає продавцю можливість перевірити, чи є пред'явник кредитної картки законним користувачем відповідного дійсного рахунка. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509v3 з підписами RSA.

•                 Автентифікація продавця. SET дозволяє власнику карти перевірити, чи має продавець відношення до відповідної фінансової організації і право приймати платежі по кредитних картках. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509v3 з підписами RSA.

Зверніть увагу на те, що на відміну від IPSec і SSL/TLS протокол SET для вирішення кожної конкретної задачі пропонує тільки по одному алгоритму. Це пояснюється тим, що SET є протоколом, що відповідає цілком конкретному набору вимог, тоді як IPSec і SSL/TLS відносяться до універсальних протоколів, призначених для вирішення широкого спектра задач.

**3. Учасники транзакцій SET.**

Учасниками транзакцій, здійснюваних за допомогою SET, є такі сторони (рис. 1).

•                  Власник платіжної карти. У середовищі електронних платежів індивідуальні і корпоративні споживачі взаємодіють із продавцями зі своїх персональних комп'ютерів через Internet. Власником карти в даному випадку є будь-якийзареєстрований власник пластикової платіжної карти (MasterCard, Visa і т.п.), виданої йому уповноваженим емітентом.

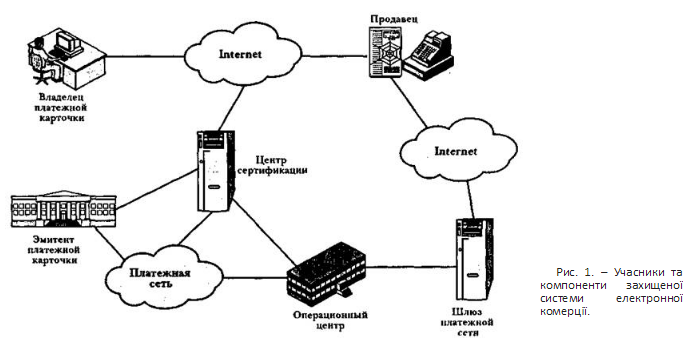
•                  Продавець. Продавець є особою, у якої власник карти може придбати товари чи послуги. Звичайно такі товари чи послуги пропонуються на продаж на Web-вузлі чи по електронній пошті. Продавець, що має право приймати платежі по платіжних картах, повинен мати відповідні відносини з операційним центром.

•                  Емітент платіжної картки. Емітент – це фінансова організація (наприклад банк), що видала платіжну карту відповідній особі (власнику карти). Як правило, відкрити рахунок можна дистанційно чи в офісі емітента особисто. Усю відповідальність по оплаті заборгованості власника карти по даній карті несе емітент.

•                  Операційний центр. Фінансова організація, що веде розрахунки з продавцем та виконує авторизацію платіжних карт і здійснює відповідні платежі. Операційний центр проводить для продавця перевірку того, що рахунок кредитної карти є дійсним, і пропонована покупка по вартості не виходить за рамки припустимого кредитного ліміту. Операційний центр також виконує електронний переказ грошових сум на рахунок продавця. Згодом операційний центр одержує за це визначену компенсацію від емітента карти через банківську платіжну мережу.

•                  Шлюз платіжної мережі (payment gateway). Сукупність засобів, контрольованих операційним центром чи уповноваженою ним третьою стороною, що використовуються для обробки платіжних повідомлень продавця. Шлюз платіжної мережі зв'язує SET і банківські платіжні мережі, виконуючи функції авторизації та передачі платежів. Продавець обмінюється повідомленнями SET зі шлюзом платіжної мережі через Internet, а шлюз платіжної мережі зв'язаний безпосередньо чи по внутрішній мережі із системою обробки фінансових документів відповідного операційного центра.

•                  Центр сертифікації (Certification Authority — СА). Об'єкт, якому довіряється видавати сертифікати X.509v3 відкритихключів власників карт, продавців і шлюзів платіжної мережі. Успішна робота SET багато в чому залежить від наявності добре організованої інфраструктури сертифікації.



Тепер опишемо коротко послідовність подій, що відбуваються під час транзакції, а потім зупинимося докладніше на деяких криптографічних деталях даного процесу.

1. Покупець відкриває рахунок. Покупець відкриває рахунок кредитної картки (наприклад, MasterCard чи Visa) у банку, що здійснює електронні платежі і підтримує SET.

2.               Покупець одержує сертифікат. Після встановленої процедури перевірки особистості покупець одержує цифровісертифікати X.509v3,  підписані центром сертифікації. Один з сертифікатів засвідчує відкритий ключ цифрового підпису, другий – відкритий ключ направленого шифрування. Ці сертифікати засвідчують відкриті RSA ключі покупця і їх термін дії.Вони також установлюють відповідність між парою ключів покупця і його кредитною карткою.

3.               Продавець одержує свої сертифікати. Продавець, який хоче приймати оплату по платіжній картці визначеного типу, повинен одержати два сертифікати двох своїх відкритих ключів: один з них буде використовуватися для цифрового підпису, а другий – для направленого шифрування. Продавцю також буде потрібна копія сертифіката відкритого ключа шлюзу платіжної мережі.

4.               Покупець розміщує замовлення. Цей процес може припускати, що покупець спочатку повинен відвідати Web-вузол продавця, щоб вибрати потрібний товар і визначити ціну. Після цього покупець відправляє продавцю список потрібних йому товарів, а продавець у відповідь висилає бланк замовлення з зазначеними в ньому списком обраних товарів, цінами, загальною вартістю замовлення і номером замовлення.

5.               Перевірка продавця. Разом із бланком замовлення продавець висилає копію свого сертифіката, щоб покупець мав можливість переконатися в тому, що він дійсно має справу зі справжним продавцем.

6.               Замовлення і платіж відправляються продавцю. Покупець відправляє замовлення і платіжну інформацію продавцю, додаючи до них свій сертифікат. Замовлення підтверджує покупку товарів, зазначених у бланку замовлення. Платіжна інформація містить необхідні дані кредитної картки. Платіжна інформація шифрується таким чином, щоб продавець не зміг її прочитати. Сертифікат покупця дозволяє продавцю виконати верифікацію покупця.

7.               Продавець запитує авторизацію платежу. Продавець відправляє платіжну інформацію шлюзу платіжної мережі з запитом підтвердження того, що доступний покупцю кредит достатній для здійснення даного платежу.

8.               Продавець підтверджує замовлення. Продавець відправляє покупцю підтвердження замовлення.

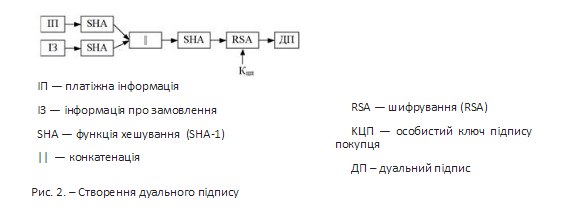
9.               Продавець доставляє товари чи надає послуги.

10.            Продавець запитує одержання платежу. Цей запит відправляється шлюзу платіжної мережі, що опрацьовує всі платіжні доручення.

**4. Дуальний підпис.**

Перш ніж перейти до розгляду деталей протоколу SET, ми обговоримо одне важливе нововведення SET — дуальний підпис (dual signature). Дуальний підпис дозволяє зв'язати два повідомлення, призначені двом різним одержувачам. У даному випадку покупцю потрібно переслати інформацію про замовлення (ІЗ) продавцю і платіжну інформацію (ІП) банку. Продавцю не потрібно знати номер кредитної картки покупця, а банку не потрібні подробиці замовлення. Покупець же, розділяючи ці повідомлення, забезпечує тим самим додатковий захист своїх прав з погляду невтручання в його особисте життя. При цьому потрібно зв'язати ці повідомлення так, щоб їх можна було використовувати при виникненні конфлікту. Зв'язок цих частин потрібен для того, щоб покупець міг довести, що даний платіж призначений для оплати саме цього, а не якогось іншого замовлення.

Щоб зрозуміти необхідність такого зв'язку, припустимо, що покупець відправляє продавцю два підписаних повідомлення IЗ (замовлення) і IП (платіж), а продавець пересилає повідомлення IП у банк. Якщо продавець одержить від покупця якесь інше замовлення, то продавець зможе заявити, що дане повідомлення IП оплачує нове, а не старе повідомлення ІЗ. Зв'язування виключає таку можливість.



|  |  |
| --- | --- |
|  |  |

На рис. 2 показана схема використання дуального підпису: спочатку покупець, використовуючи алгоритм SHA-1, обчислює хеш-коди для повідомлень IП і ІЗ. Два отриманих хеш-коди зв'язуються операцією конкатенації, і для результату зв'язування теж обчислюється хеш-код. Нарешті, покупець шифрує підсумковий хеш-код з використанням свого особистого ключа цифрового підпису, у результаті одержуючи дуальний підпис.

Дуальний підпис перевіряють продавець і банк. Розглянемо послідовність перевірки дуального підпису у банку (див. рис. 3).

|  |
| --- |
|  |
|  |  |



Кожна з перевіряючих сторін повинна мати одне з повідомлень, хеш-код другого повідомлення, відкритий ключ перевірки підпису та сам дуальний підпис. Далі перевіряюча сторона обчислює загальну хеш-функцію (ліва частина рис. 3) та з допомогою відкритого ключа перевірки підпису розшифровує ДП (права частина рис. 3). Якщо ці два отримані значення збігаються, то перевіряючий робить висновок про справжність дуального підпису.

Підводячи підсумок, можна сказати наступне.

1.               Продавець одержує повідомлення IЗ і виконує перевірку підпису покупця.

2.               Банк одержує повідомлення IП і виконує перевірку підпису покупця.

3.               Повідомлення ІЗ і IП виявляються зв'язаними, і покупець може довести їх зв'язок.

Припустимо, що продавець вирішить замінити повідомлення IЗ даної транзакції іншим. Для цього йому доведеться знайти інше повідомлення ІЗ з точно таким же хеш-кодом. На сьогоднішній день при використанні алгоритму SHA-1 це є практично нерозв'язною задачею. Таким чином, у продавця немає можливості зв'язати з даним повідомленням IП інше повідомлення IЗ.

**5. Опрацювання платежів.**

У даному розділі ми розглянемо докладно такі типи транзакцій:

•                  Запит на купівлю (Purchase Request).

•                  Запит авторизації (Payment Authorization).

•                  Відповідь на запит авторизації (Authorization Response).

•                  Запит на платіж (Payment Capture).

*Повідомлення “Запит на купівлю”*

До того як почати формування повідомлення “запит на купівлю”(Purchase Request), власник платіжної картки повинен завершити перегляд списку доступних товарів, вибрати потрібні й оформити замовлення. Даний попередній етап закінчується відправленням продавцем бланка замовлення покупцю. Усі ці попередні операції не зв'язані з SET.

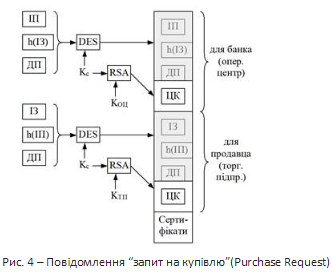
Обмін даними вимоги на закупівлю складаються з чотирьох повідомлень: Initiate Request (ініціюючий запит), Initiate Response (відповідь на ініціюючий запит), Purchase Request (запит на купівлю) і Purchase Response (відповідь на запит накупівлю).

Щоб власник платіжної картки мав можливість відправляти повідомлення SET продавцю, необхідно одержати копії сертифіката продавця і сертифіката шлюзу платіжної мережі. Запити на одержання цих сертифікатів містяться в повідомленні Initiate Request (ініціюючий запит), що покупець відправляє продавцю. Це повідомлення містить інформацію про тип кредитної картки, яка використовується покупцем, ідентифікатор, призначений покупцем даній парі повідомлень "запит-відповідь", і порядковий номер даного сеансу зв’язку. SET гарантує оригінальність повідомлення.

Продавець генерує відповідь і підписує її своїм особистим цифровим підписом. Відповідь повинна включати порядковий номер даного сеансу зв’язку, порядковий номер повідомлення у цьому сеансу зв’язку, а також ідентифікатор даної транзакції. Крім підписаної відповіді, повідомлення Initiate Response (відповідь на ініціюючий запит) містить сертифікат підпису продавця і сертифікат шлюзу платіжної мережі для обміну ключами.

Власник платіжної картки перевіряє дійсність сертифікатів продавця і шлюзу платіжної мережі шляхом перевірки підписів відповідних центрів сертифікації, а потім створює повідомлення ІЗ і ІП. Обидва ці повідомлення містять ідентифікатор транзакції, згенерований продавцем. Повідомлення ІЗ може не включати таких даних замовлення як кількість чи ціна товарів, а містити лише посилання на замовлення, яке створене у процесі обміну повідомленнями між продавцем і покупцем на етапі узгодження ще до першого повідомлення SET. В цьому випадку повідомлення ІЗ може передаватися у відкритому виді. Але частіше повідомлення ІЗ як і ІП перед передачею має бути зашифроване.

Потім власник платіжної картки готує повідомлення Purchase Request (запит на купівлю); див. схему на рис. 4.



|  |
| --- |
|  |

Для цього власник платіжної картки генерує одноразовий ключ Kс для схеми симетричного шифрування з використанням алгоритму DES.

Повідомлення складається з таких блоків інформації.

*1. Інформація про платіж.* Пересилається продавцем шлюзу платіжної мережі і містить наступні дані.

•                  Дані ІП

•                  Профіль повідомлення ІЗ (h(ІЗ)).

•                  Дуальний підпис, обчислений для сукупності ІЗ і IП і підписаний з використанням особистого ключа підпису покупця.

Значення h(ІЗ) необхідно для того, щоб шлюз платіжної мережі міг перевірити дуальний підпис, як це було наведено вище. Усі зазначені елементи шифруються за допомогою алгоритма DES та ключа Kс.

Останнім для даного блоку інформації є цифровий конверт. Цифровий конверт формується шляхом шифрування Kс за допомогою відкритого ключа шлюзу платіжної мережі (або операційного центру), призначеного для обміну ключами. Цей елемент називається *цифровим конвертам,*оскільки для того, щоб прочитати елементи, названі вище, цей конверт необхідно відкрити (тобто дешифрувати).

Значення Kс залишається продавцю невідомим. Тому продавець не зможе прочитати повідомлення яке включає до себе ІП.

*2. Інформація про замовлення.* Ця інформація потрібна продавцю і містить наступні дані.

•                  Дані IЗ.

•                  Профіль повідомлення ІП (h(ІП)).

•                  Дуальний підпис, обчислений для сукупності ІЗ і IП і підписаний з використанням особистого ключа підпису покупця.

Значення h(ІП) необхідно для того, щоб продавець міг перевірити дуальний підпис, як це було наведено вище. Усі зазначені елементи шифруються за допомогою алгоритма DES та ключа Kс.

*3. Сертифікати власника платіжної картки.* Ця частина повідомлення містить сертифікати відкритого ключа цифрового підпису власника платіжної картки, а також сертифікат відкритого ключа власника картки для ключового обміну. Цісертифікати необхідні як продавцю, так і шлюзу платіжної мережі.

Після одержання повідомлення “запит на купівлю” (Purchase Request) продавець виконує такі дії (рис. 4)

1.               Перевіряє сертифікати власника платіжної картки за допомогою підписів центрів сертифікації.

2.               Перевіряє дуальний підпис за допомогою відкритого ключа цифрового підпису власника платіжної картки. Це дозволяє переконатися в тому, що замовлення не було змінено під час пересилання і було підписано власником платіжної картки.

3.               Опрацьовує замовлення і пересилає платіжну інформацію шлюзу платіжної мережі для авторизації платежу (відповідний процес буде описаний нижче).

4.               Відправляє повідомлення Purchase Response (відповідь на вимогу на закупівлю) власнику платіжної картки.

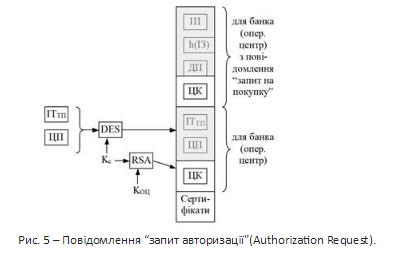
Повідомлення Purchase Response (“відповідь на запит на покупку”) містить блок відповіді, що підтверджує замовлення і посилається на відповідний номер транзакції. Цей блок підписується продавцем за допомогою його особистого ключа цифрового підпису. Після цього блок разом з підписом, а також сертифікат підпису продавця відправляються власнику платіжної картки.

Коли програмне забезпечення, встановлене на комп'ютері власника платіжної картки, одержує повідомлення Purchase Response, воно перевіряє спочатку сертифікат продавця, а потім підпис блоку відповіді. Зрештою, у залежності від змісту відповіді, виконується відповідна дія, наприклад, відображається на екрані деяке повідомлення для користувача чи обновляється інформація про стан замовлення в базі даних.

*Повідомлення “Запит авторизації”.*

Під час опрацювання замовлення, що надійшло від власника платіжної картки, продавець виконує авторизацію транзакції (одержання дозволу на оплату) за допомогою шлюзу платіжної мережі. Таке одержання дозволу на оплату (авторизація платежу) означає санкціонування транзакції емітентом платіжної картки. Авторизація дає продавцю гарантію того, що він одержить плату за проданий товар, і тому продавець може виконати доставку товарів чи послуг покупцю. Обмін даними для одержання дозволу на оплату формується з двох повідомлень: Authorization Request (запит авторизації) і Authorization Response (відповідь на запит авторизації).

Розглянемо повідомлення Authorization Request (запит авторизації) (рис. 5).



Повідомлення Authorization Request (запит авторизації), що відправляється продавцем шлюзу платіжної мережі, складається з таких блоків інформації.

1. Інформація про платіж. Ця інформація була отримана від покупця і містить наступні дані.

•                  Дані ІП

•                  Профіль повідомлення ІЗ (h(ІЗ)).

•                  Дуальний підпис, обчислений для сукупності ІЗ і IП і підписаний з використанням особистого ключа підпису покупця.

•                  Цифровий конверт.

2.         Інформація авторизації. Ця інформація генерується продавцем і містить такі дані:

•                  Блок авторизації, що включає ідентифікатор транзакції (ІТТП), підписаний особистим ключем цифрового підпису продавця і зашифрований одноразовим ключем схеми симетричного шифрування, що генерується продавцем.

•                  Цифровий конверт, сформований шляхом шифрування одноразового ключа за допомогою відкритого ключа шлюзу платіжної мережі, призначеного для обміну ключами.

3.         Сертифікати. Продавець включає в повідомлення сертифікат цифрового підпису власника платіжної картки (служить для перевірки дуального підпису), сертифікат ключа свого цифрового підпису (дозволяє перевірити підпис продавця) і сертифікат свого ключа для обміну ключами (необхідний для відповіді шлюзу платіжної мережі).

Одержавши ці дані, шлюз платіжної мережі виконує такі дії:

1.               Перевіряє всі сертифікати.

2.               Дешифрує спочатку цифровий конверт блоку дані авторизації, щоб одержати ключ для схеми симетричного шифрування, а потім дешифрує блок даних авторизації.

3.               Перевіряє підпис продавця для блоку даних авторизації.

4.               Дешифрує спочатку цифровий конверт блоку платіжної інформації, щоб одержати ключ для схеми симетричного шифрування, а потім дешифрує блок платіжної інформації.

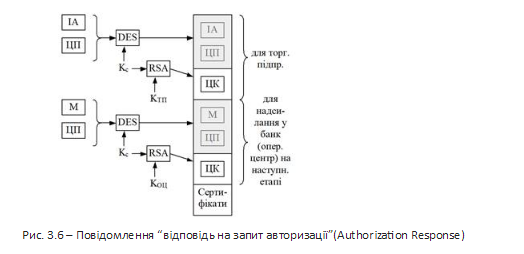
5.               Перевіряє дуальний підпис блоку платіжної інформації.

6.               Перевіряє збіг ідентифікатора транзакції, отриманого від продавця, з ідентифікатором, включеним до складу даних IП, що надійшли (через продавця) від власника платіжної картки.

7.               Запитує й одержує дозвіл на оплату в емітента платіжної картки.

*Повідомлення “Відповідь на запит авторизації”.*

Одержавши дозвіл на оплату в емітента платіжної картки, платіжний шлюз повертає продавцю повідомлення AuthorizationResponse (відповідь на запит авторизації) (рис. 6).



Це повідомлення складається з таких блоків інформації:

1.               Інформація авторизації (ІА). Включає блок авторизації, підписаний особистим ключем цифрового підпису шлюзу платіжної мережі і шифрований згенерованим шлюзом платіжної мережі одноразовим ключем для схеми симетричного шифрування. Крім того, включає цифровий конверт, що містить цей одноразовий ключ, шифрований за допомогою відкритого ключа продавця, використовуваного для обміну ключами.

2.               Мандат на одержання платежу (М) (capture token). Ця інформація буде використана для здійснення платежу згодом. Даний блок має ту ж форму, що і попередній, тобто містить підписаний і шифрований мандат з цифровим конвертом. Цей мандат не обробляється продавцем, а повинний бути просто повернутий ним у тому ж вигляді шлюзу платіжної мережі в запиті на оплату.

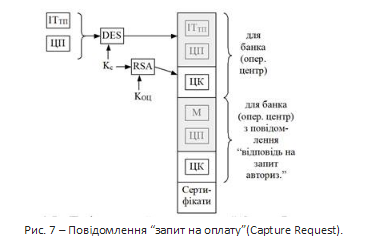
3.               Сертифікати. Сертифікат цифрового підпису шлюзу платіжної мережі.

Одержавши підтвердження авторизації платежу від шлюзу платіжної мережі, продавець може виконати доставку товарів чи послуг покупцю.

*Повідомлення “запит на оплату”.*

Щоб одержати плату за товари чи послуги, продавець звертається до шлюзу платіжної мережі з ініціативою виконання транзакції одержання платежу, що складається з двох повідомлень: повідомлення запиту на одержання оплати і повідомлення відповіді на запит на одержання оплати.

Структура повідомлення “запит на оплату” (Capture Request) представлена на рис. 7.



Для повідомлення Capture Request(запит на оплату) продавець генерує, підписує і шифрує блок даних запиту на оплату, що включає суму платежу й ідентифікатор транзакции (ІТТП). Дане повідомлення повинне також включати раніше отриманий (у повідомленні Authorization Response) шифрований мандат на одержання платежу для даної транзакции і, крім того, сертифікати ключів продавця для цифрового підпису й обміну ключами.

Одержавши це повідомлення, шлюз платіжної мережі дешифрує і перевіряє блок даних запиту на оплату, а також дешифрує і перевіряє блок мандата на одержання платежу. Потім перевіряється відповідність між даними цих двох блоків. Після цьогошлюз платіжної мережі створює розрахунковий запит, що відсилається емітенту платіжної картки по закритій платіжній мережі. У результаті цього запиту кошти переказують на рахунок продавця.

Потім шлюз за допомогою повідомлення Capture Response (відповідь на запит на оплату) сповіщає продавця про перерахування коштів. Повідомлення містить підписаний і шифрований шлюзом блок даних відповіді на запит на оплату. Крім того, це повідомлення містить сертифікат цифрового підпису шлюзу платіжної мережі. Програмне забезпечення,встановлене на комп'ютері продавця, одержавши дане повідомлення, зберігає його для використання в програмах обліку коштів, що надходять від операційного центра.

**6. Перспективи захисту платежів в Інтернет.**

Visa оголосила про те, що колись популярний протокол SET вже не відповідає сучасним вимогам безпеки і повинен бути заміщений більш досконалими системами, такими як - Verified by Visa, що працює на основі протоколу 3D Secure і SecurePayment Application (SPA) від MasterCard.

**Verified by Visa** – це нова система захисту, яка сповіщає онлайн продавців та банки, що Ви справжній власник картки, коли Ви робите онлайн-покупки. Вона дозволяє Вам використовувати персональний пароль, щоб підтверджувати Вашу особу та захищати Вашу картку Visa, коли Ви використовуєте її в Інтернеті, забезпечуючи більшу впевненість та надійність.

До неї легко підключитися, її легко використовувати, ця безкоштовна послуга діє для всіх карток Visa.

 ЯК ЦЕ ПРАЦЮЄ?

* Ви можете інсталювати свій пароль Verified by Visa та активувати свою картку всього за декілька хвилин.
* Щойно Ви активуєте картку, система Verified by Visa захищатиме Вас у будь-якому Інтернет-магазині, підключеному до цієї системи.
* Якщо Ви займаєтеся шопінгом у магазинах системи, Вашу картку автоматично впізнає та захищає система Verified by Visa.
* У момент, коли Ви закінчуєте робити покупку, Ваш банк-емітент перевіряє Ваш пароль

**Що означає «Перевірено Visa»?**  
Додатковий захист «Verified by Visa» («Перевірено Visa») Гарантує, що за допомогою вашої картки Visa тільки ви можете здійснювати покупки он-лайн. Цю послугу легко активувати для вашої існуючої картки, дана функція безкоштовна.  
  
**Принцип роботи**

* Через банк, який видав вам картку Visa, встановіть метод перевірки та активуйте картку протягом декількох хвилин. Ваш банк запропонує вам два варіанти на вибір: встановити пароль або використовувати код, що відправляється текстовим повідомленням на номер мобільного телефону.
* Після активації послуга «Verified by Visa» надає захист у всіх інтернет-магазинах, які є учасниками даної програми.
* При здійсненні покупки в інтернет-магазині, який є учасником програми, ваша картка буде автоматично розпізнана як картка з захистом «Verified by Visa».
* Перевірте деталі транзакції. Переконайтесь, що порядок здійснення покупки відповідає встановленому емітентом вашої картки.
* Дотримуйтесь інструкцій, щоб завершити транзакцію.
* Емітент вашої картки перевірить введені дані, та при успішній перевірці транзакція буде виконана.

**Лекція 7. ХАРАКТЕРИСТИКА ПІДСИСТЕМИ «ОПЕРАЦІЙНИЙ ДЕНЬ БАНКУ»**

## 7.1. Характеристика документів

Усі обліково-операційні роботи банку виконуються в підсистемі «Операційний день банку (ОДБ)». Підсистема ОДБ є ядром АБС. Інформаційно і функціонально вона пов’язана з усіма іншими підсистемами АБС. Основними функціями ОДБ є обробка платіжних документів. У підсистемі можуть оброблятись різні платіжні документи, формуватись інформаційні повідомлення, дебетові та інформаційні запити. Основними первинними документами ОДБ є платіжні та касові документи. До них, зокрема, належать платіжні (вимоги) доручення, меморіальні ордери, видаткові та прибуткові касові ордери.

Платіжні документи, з якими працює ОДБ, можна розподілити на внутрішні, зовнішні та транзитні.

*Внутрішні* документи — це документи, проведення по яких виконується по особових рахунках банку.

*Зовнішні* — це міжбанківські документи, проведення по яких виконується між кореспондентськими рахунками та особовими рахунками банку. Зовнішні документи, в свою чергу, ще поділяються на початкові та зворотні. Початкові документи — це документи, сформовані в банку для відправлення в СЕП. Зворотні — це документи, що надійшли з СЕП у банк.

*Транзитні* — це документи, по яких не виконуються проведення.

За ознакою проведення по рахунках документи розподіляються на: проведені по рахунках та не допущені до проведення з різних причин.

*Не допущені* до проведення, в свою чергу, діляться на документи, які резервують кошти на рахунку для майбутнього проведення, та на документи, які не резервують кошти. Документи, які резервують кошти, зберігаються в картотеках № 2, № 3 та картотеці планових платежів. Документи, які не резервують кошти, зберігаються в картотеці нез’ясованих сум та картотеці № 1.

*Картотека № 1* — це картотека попереднього акцепта. До неї заносяться документи за бажанням клієнта.

В *картотеку № 2* заносять документи при недостатності коштів на особовому рахунку під час проведення.

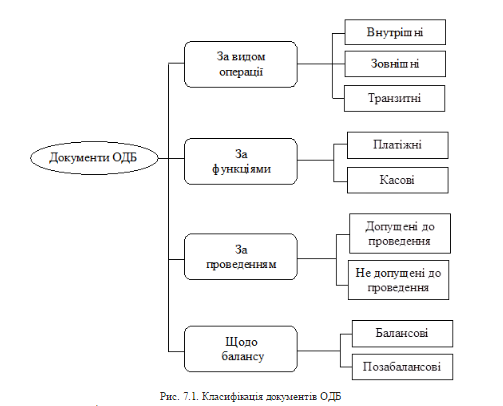
*Картотека № 3* вміщує документи, які були відкладені з причини фінансового контролю.

Щодо балансу документи поділяються на балансові та позабалансові.

Загальну класифікацію документів ОДБ наведено на рис. 7.1.

## 7.2. Функції ОДБ

Підсистема ОДБ — це багатофункціональна система, яка надає користувачеві широкий спектр функцій. Вона повинна забезпечувати здійснення таких операцій: перегляд, введення і редагування даних про клієнтів; перегляд відомостей про рахунки клієнта, що відкриті в банку; відкриття нових рахунків і закриття вже існуючих; обробка пакетів платіжних документів, які надійшли безпосередньо від клієнтів, чи по системі «Клієнт-банк»; ведення картотек; підтримка реальних залишків по рахунках протягом усього банківського дня; формування актуального балансу банку на будь-який момент часу; формування вихідних повідомлень за поточний і будь-який попередній банківський день; підтримка роботи віддалених робочих місць та безбалансових відділень; забезпечення функціонування банку в СЕП; формування звітності для НБУ та податкових органів.



Усі функції ОДБ можна згрупувати і представити таким чином:

*1. Функція ведення рахунків*

1.1. Відкриття рахунків.

1.2. Закриття рахунків.

1.3. Арешт рахунку.

1.4. Модифікація параметрів рахунку.

1.5. Перегляд залишку та руху коштів на рахунку за відповідний період.

*2. Робота з усіма видами документів (платіжні доручення, ордери, документи по заключних оборотах щодо прибутків/видатків на позабалансових рахунках тощо)*

2.1. Введення документа.

2.2. Статистика введення.

2.3. Перегляд документів (отриманих / сплачених / несплачених / вибраних / окремих / за повним макетом чи у вигляді реєстру).

2.4. Друкування документів (отриманих / сплачених / несплачених / вибраних / окремих / за повним макетом чи у вигляді реєстру).

2.5. Відбір документів для передачі у зовнішні системи («Клієнт-банк» і т.п.).

2.6. Модифікація введених документів.

2.7. Вилучення введених документів.

2.8. Обробка (розблокування, оплата тощо) введених документів.

*3. Ведення картотеки інформаційно-дебетових документів*

3.1. Перегляд дебетових документів.

3.2. Сплата документів (з дозволу / за розпорядженням посадової особи з відповідними повноваженнями).

3.3. Друкування дебетових документів.

3.4. Вилучення з перегляду окремих документів.

*4. Робота з документами нез’ясованих сум*

4.1. Аналіз нез’ясованих рахунків.

4.2. Сплата з’ясованої суми.

4.3. Повернення нез’ясованої суми.

*5. Робота із зовнішними підсистемами*

5.1. Робота з документами, що надійшли по системі «Клієнт-Банк».

5.1.1. Перегляд документів (отриманих / сплачених / несплачених / відхилених / повернених / вибраних / окремих за повним макетом чи у вигляді реєстру).

5.1.2. Друкування документів (отриманих / сплачених / несплачених / відхилених / повернених / вибраних / окремих за повним макетом чи у вигляді реєстру).

5.1.3. Оплата документів.

5.1.4. Повернення відхилених документів клієнтові з поясненням причин їх забракування.

*6. Формування, перегляд та друкування статистичних відомостей і відомостей нарахування відсотків*

6.1. Формування балансу за поточний день (за період, на дату, місяць, квартал, рік).

6.2. Формування відомостей по особових рахунках за поточний день (за період, на дату, за місяць, квартал, рік, по виконавцях, за типами рахунків, вибірково за певними рахунками).

6.3. Формування оборотно-сальдових відомостей за поточний день (за період, на дату, за місяць, квартал, рік, по виконавцях, за типами валют, по національній валюті, по іноземній валюті, за типами рахунків, по всіх рахунках, вибірково за певними рахунками, за позабалансовими рахунками).

6.4. Формування відомостей по кореспондентському рахунку банку за поточний день (за період, на дату, по клієнтах, по виконавцях, по валюті).

6.5. Формування згрупованих документів ОДБ (реєстр початкових, реєстр зворотніх, реєстр дебетових сплачених, реєстр дебетових необроблених, реєстр позабалансових, документи для системи «Клієнт-банк», касові документи).

6.6. Формування файлів звітності для НБУ та податкових органів.

***7. Перегляд та модифікація довідників***

7.1. Довідник банків (МФО).

7.2. Довідник плану рахунків.

7.3. Довідник клієнтів.

7.4. Довідник валют.

7.5. Довідник касових символів.

7.6. Довідник країн.

7.7. Довідник відповідальних працівників банку.

7.8 Довідник секторів економіки.

7.9. Довідник галузей економіки.

7.10. Довідник видів економічної діяльності.

7.11. Довідник видів власності.

7.12. Довідник ознак інсайдера.

7.13. Довідник податкової інспекції.

7.14. Довідник з параметрів нарахування відсотків.

7.15. Довідник з видів кредитів.

7.16. Довідник з емітентів цінних паперів.

7.17. Довідник з видів цінних паперів.

Програмний комплекс ОДБ в переважній більшості випадків складається з таких АРМів: АРМ операціоніста, АРМ технолога (адміністратора системи), АРМ контролера. Такий розподіл обумовлений необхідністю впорядкування та раціонального розподілу робіт між виконавцями. Іноді АРМ контролера не виділяється як окреме робоче місце, і тоді функції контролера покладаються на АРМ технолога.

### 7.2.1. Характеристика АРМ технолога

Основні роботи з ОДБ виконуються на робочому місці технолога. Основні функції технолога протягом банківського дня такі:

    відкриття ОДБ та ініціалізація банківського дня;

    реєстрація клієнтів і відкриття рахунків;

    контроль над введенням документів на робочих місцях;

    обробка документів банківського дня, їх оплати та проведення;

    виправлення виконаних помилкових проведень;

    закриття ОДБ і банківського дня, друкування звітних форм;

    формування звітних форм відповідно до існуючих вимог для податкових органів.

*1. Відкриття банківського дня в ОДБ*

Під час відкриття ОДБ та ініціалізації банківського дня виконуються такі операції:

    встановлення поточної календарної дати;

    створення необхідних для роботи каталогів;

    полям дебетових та кредитових оборотів у файлі бази даних, яка вміщує дані оборотів за день, присвоюється значення нуля;

    обнулювання на перший день нового місяця (кварталу, року) оборотів за відповідний період і формування файлів вхідних залишків на початок наступного періоду.

*2. Реєстрація клієнтів і відкриття рахунків*

Реєстрація клієнтів і відкриття рахунків — це робота, яка виконується під час залучення нового клієнта в банк. Послідовність її виконання така:

    присвоєння реєстраційного номера клієнту, для якого відкривається рахунок і виконується формування запису файла «Довідник клієнтів» (КLIENT);

    відкриття рахунку з цим реєстраційним номером та формування запису файла відповідного рахунку. У цьому режимі також вводяться такі додаткові реквізити по рахунку: дата погашення; ознака строку позички по позичкових рахунках; символ звітності; характер рахунку; відомості для звітності в податкову інспекцію тощо.

### 3. Робота з первинними документами

Технолог має можливість контролю за введенням документів на робочих місцях. Безпосередній прийом документів та їх введення виконується на робочих місцях операціоністами, кожен з яких має свій ідентифікаційний номер і виконує обслуговування певних, закріплених за ним, клієнтів. Введені, проконтрольовані та прийняті до обробки пакети документів з робочого місця операціоністів передаються по мережі на обробку на робоче місце технолога. Технолог має можливість перевіряти файли операціоністів. Технолог також працює з документами, що надійшли по системі «Клієнт-банк».

Основною функцією АРМ-технолога є обробка документів банківського дня, їх оплата та проведення.

Під час роботи в цьому режимі технологу надається можливість:

    обробки файлів СЕП, що надійшли в банк, формування файлів для відправки в СЕП;

    оплата (проведення) документів, тобто зміна залишку на рахунках у відповідності з введеними (внутрішніми і початковими) та прийнятими по СЕП (зворотними) документами дня.

Початкові документи, введені з клавіатури, проводяться автоматично в момент запису документа в базу. Документи, що надійшли з АРМ-3, проводяться також автоматично.

Умови виконання проведення по внутрішніх документах банку такі:

    наявність в базі даних ОДБ обох рахунків, по яких необхідно виконати проведення;

    проведення не повинно викликати «червоне» сальдо на рахунках.

Проведення по зворотних міжбанківських документах та формування файлів початкових платежів виконується з урахуванням контролю по кореспондентському рахунку в РРП. Умовами виконання проведення по зовнішніх (міжбанківських) документах банку є наступні:

    початкові проведення, які призводять до «червоного» сальдо на кореспондентському рахунку, не виконуються і відповідно документи не включаються у файл початкових платежів для відправки в СЕП;

    проведення по прийнятих зворотних платежах в ОДБ здійснюється лише після отримання інформації з РРП про їх зарахування на кореспондентський рахунок.

Документи, які надійшли по каналах зв’язку з системи «Клієнт-банк», обробляються, і технологу надається можливість:

    сплатити документ частково;

    вмістити його на картотеку 1 чи картотеку 2;

    передати на розгляд одному з відповідальних осіб (головному бухгалтеру, кредитному інспектору і т.п.);

    зняти без оплати.

Позабалансовим документам під час введення автоматично надається відповідний статус і водночас виконується проведення.

Для касових документів існують два варіанти обробки:

    проведення по касових операціях для внутрішньобанківських рахунків виконуються під час введення, у момент запису документа в базу даних;

    проведення для внутрішньобанківських рахунків виконуються після оплати документів;

    для касових операцій з обліку цінностей, бланків строгої звітності водночас із здійсненням проведень виконується зарахування чи списання на позабалансових рахунках.

Обробка касових документів має ряд особливостей:

    документи під час введення не формуються, а створюються автоматично, в момент закриття дня по касі;

    меморіальні ордери, отримані під час обробки документів «чужого» клієнта, оплачуються перед закриттям ОДБ.

Технологу надається можливість переглядати документи і встановлювати їм відповідний статус. Залежно від типу документа і статусу, наданого йому після введення в систему, формується реальне проведення по балансу, яке може відрізнятися від проведення, запропонованого в документі.

Документ, що обробляється, можна сплатити або ухвалити по ньому рішення:

    сплатити частково;

    вмістити на картотеку 1;

    вмістити на картотеку 2;

    зняти з картотеки №1 до певного терміну;

    передати на розгляд;

    зняти без оплати;

    відкласти розгляд.

Технологу також повинна надаватись можливість перегляду та коректування введених документів. Він повинен мати можливість:

    переглянути документ та всю, пов’язану з ним інформацію, включаючи поточний стан закріплення документа за особовими рахунками;

    внести зміни в номер документа, призначення платежу, код відправки, номер пачки, суму документа (неоплаченого);

    ухвалити рішення щодо документа (якщо користувач — головний бухгалтер або керівник банку і документ відправлений йому на розгляд);

     вилучити неоплачений документ;

    сторнувати документ, тобто десальдувати залишки (кошти повертаються на рахунок).

*4. Оплата документа*

Оплата документа — це процедура його бухгалтерського проведення, в результаті якої змінюється залишок на рахунку. Під час оплати виконуються такі операції:

    обробка файла залишків на кореспондентському рахунку (тип К), який надійшов до банку, і видача на екран повідомлення про стан коррахунку в РРП і коррахунку, який ведеться в ОДБ;

    вибір з поштової скриньки файлів зворотних міжбанківських платежів рахунку (типу В), їх оплата та формування на них файла квитанції рахунку (тип S). З файлу типу В також формується файл для передачі клієнту по системі «Клієнт-банк». Дебетові запити, що надходять з CЕП, автоматично не оплачуються, вони розташовуються в окремому файлі і підлягають аналізу технолога;

    оплачені документи початкових платежів формуються у файл початкових платежів (тип А) і надсилаються до поштової скриньки для відправки у СЕП. Відібрані для відправки в СЕП документи реєструються у файлі «Картотека початкових проведень», яка потім використовується для квітовки (подокументальної звірки) з файлами-квитанціями (тип Т), які надходять з СЕП як підтвердження на файли типу А;

    якщо на якийсь відправлений файл типу А прийшов «відбійний» файл типу Т, то документам цього файлу автоматично змінюється статус і вони переходять у розряд невідібраних;

    якщо є неоплачені документи, то вони видаються в протокол неоплачених документів з поясненням причин неоплати.

*5. Виправлення помилкових проведень*

Виявлені помилки проведень можна виправити лише через спеціально передбачений для цього режим, який має назву «Коротке відновлення» (КВ). При його виконанні виконується повернення на початок дня, і всі документи у файлі операцій OPER переводяться в стан неоплачених, а також відновлюється вхідне сальдо (SALDO) за його станом на початок банківського дня. Після виконаного відкату проводять заново відкриття дня, і лише після цього робляться відповідні виправлення документів. Режим КВ також використовується під час отримання «відбійного» файлу типу Т.

Такий режим виправлення помилкових проведень можна застосовувати лише для внутрішніх документів банку.

Виправлення зовнішніх документів, оплачених документів, можливе до їх відправки в РРП, тобто тих, які лише відібрані для відправлення у файл початкових платежів типу А. При цьому технолог повинен зняти позначку про відбір документа у файл А і лише після цього провести необхідні виправлення.

Крім виправлень помилок, протягом дня технологу надається можливість провести виправлення за інші дні, виконавши повернення в режимі «Довге відновлення». У цьому режимі можна робити один чи кілька відкатів на кілька днів назад з перерахуванням усіх цих днів. Для того щоб можна було скористатися цим режимом, необхідно мати копії всіх попередніх банківських днів. Користуватися режимом довгого відновлення необхідно лише у разі крайньої необхідності, для виправлення помилок попередніх днів краще користуватися коригуючими проведеннями.

Коригуючі проведення виконуються за допомогою меморіальних ордерів. При друкуванні меморіальних ордерів для коригуючого проведення на ньому буде додатковий рядок з надписом «Коригуючий».

*6. Закриття банківського дня в ОДБ*

Під час закриття банківського дня технолог повинен виконати ряд робіт інформаційно-технологічного характеру. Основними операціями є такі:

    перевірити наявність балансу; якщо баланс не сформований, то закрити день неможливо;

    провести накопичення денних оборотів по балансових рахунках і сформувати відомості: «Баланс на місяць (квартал, рік), «Баланс з початку року до поточного дня»;

    провести накопичення даних по касових проведеннях дня;

    провести накопичення плат за касове та розрахункове обслуговування;

    сформувати виписки по особових рахунках й відправити їх в архів;

    створити архівні копії дня;

    провести формування всіх звітних форм та файлів.

### 7.2.2. Характеристика АРМ операціоніста

Усі платіжні документи на паперових носіях, що надійшли в банк від клієнта, повинні пройти стадію первинного контролю і попередньої оцінки фінансового стану клієнта.

При первинному контролі операціоністом вводиться номер особового рахунку клієнта. Якщо номер введено правильно, то на екран видаються дані про назву клієнта, вхідний залишок на його рахунку, дані про поточні обороти, вихідний залишок і залишок, що контролюється.

Після первинного контролю надається можливість введення даних платіжних документів. Іноді в системі вводиться обмеження на кількість документів, що вводяться одночасно. Наприклад, операціоністу дозволяється одночасно ввести до 100 платіжних документів. Після введення кожного рядка відбувається автоматичне коригування поточного стану особового рахунку клієнта в базі даних і висвітлення його перед операціоністом, оскільки за час набору могли надійти документи по електронних каналах і змінити поточний залишок на рахунку клієнта. Для кожного виду документа існує певний макет, згідно з яким виконується введення даних.

З первинного документа вводяться наступні поля: код банку контрагента, номер особового рахунку контрагента, ознака дебет/ кредит (означає, що сума по документу буде проведена по дебету чи кредиту особового рахунку клієнта), сума платежу по документу,призначення платежу.

Після введення даних одного документа змінюється автоматично сума залишку, що контролюється. Залишок, що контролюється, — це той залишок, що прогнозується на рахунку, тобто той, який матиме рахунок, якщо даний документ буде сплачено.

Якщо значення поля «Призначення платежу» часто повторюється, то його можна занести у відповідний довідник і вибирати звідти при завантаженні даних платіжних документів. Аналогічним чином можна оперувати з контрагентами, тобто з клієнтами, яким адресуються платежі. Якщо якийсь контрагент досить часто зустрічається в первинних документах, то його слід занести і зберігати у відповідному довідниковому файлі бази даних, що дасть змогу надалі не вводити його вручну, а вибирати з довідника контрагентів.

Після закінчення введення пачки документів система може запитати контрольну суму (КС) по цій пачці, якщо використовується технологія обробки документів пачками.

Система має бути спроектованою таким чином, щоб це не потребувало спеціальної підготовки оператора. Всі поля введення, значення яких можна перевірити, контролюються.

До виконання остаточного оновлення стану рахунків оператор може переглянути всю транзакцію і виправити помилки, якщо вони є.

Без повторного введення всіх даних на всіх важливих етапах запитується підтвердження.

Операціоніст може вилучати й коригувати введені ним документи до передачі їх на наступну обробку технологу.

### 7.2.3. Характеристика АРМ контролера

Функції контролера полягають у регулюванні потоків початкових документів на РРП. Тобто він може дозволяти або забороняти оплату початкових документів з файлу OPER та відбір їх до файлу типу А (файл початкових платежів).

Вводиться поняття «Блокованого» і «Неблокованого» початкового документа. Початкові міжбанківські документи будуть оплачуватися тільки в тому разі, якщо вони неблоковані.

Використання АРМ контролера в ОДБ має значення тільки при роботі в мережі. Його функції будуть полягати в перегляді документів, які надходять з робочих станцій операціоністів, їх аналізі та визначенні параметрів «блокований» — «неблокований» перед тим, як передати документи на оплату на АРМ технолога.

Як вже зазначалося, використання АРМ контролера є необов’язковим, якщо не виникає потреба регулювання черговості проходження початкових платежів.

## 7.3. База даних ОДБ

Усі файли, що використовуються в ОДБ, умовно можна розподілити на такі групи: основні файли, оперативні файли, файли СЕП, нормативно-довідкові файли НБУ.

До *основних файлів* належать: файл залишків коштів на балансових рахунках в національній валюті (SALDO); файл залишків коштів на балансових рахунках в іноземній валюті (SALDOV); файл залишків коштів на позабалансових рахунках (SALDONB); файл гривневих рахунків оновлених, відкритих чи закритих протягом банківського дня (SCHETAS); файл валютних рахунків оновлених, відкритих чи закритих протягом банківського дня (SCHETAV); файл позабалансових рахунків оновлених, відкритих чи закритих протягом банківського дня (SCHETANB); довідник клієнтів (KLIENT); список клієнтів, які були оновлені (відкриті чи закриті протягом банківського дня) (KLITAS); накопичувальний файл оборотів по рахунках в розрізі всіх місяців (BALANS); накопичувальний файл касових оборотів за поточний і попередній місяць (VKAS); довідник валют і курсів (TABVAL).

До *оперативних файлів* належать: файл документів дня по балансових рахунках в національній валюті (OPER); файл документів дня по балансових рахунках в іноземній валюті (OPERV); файл документів дня на позабалансових рахунках (OPERNB).

*Файли СЕП:* файл «Картотека початкових платежів» (vA); файл «Картотека зворотних платежів» (vB); файл «Картотека стану кореспондентського рахунку» (vК).

*Нормативно-довідкові файли СЕП*: довідник банків-учасників СЕП (S\_UCH); довідник призначень платежу (S\_NR); довідник кодів помилок (S\_ER); довідник субкореспондентів шлюзових банків (S\_SNG).

Розглянемо структури основних файлів ОДБ.

ФАЙЛ ЗАЛИШКІВ КОШТІВ НА БАЛАНСОВИХ РАХУНКАХ В НАЦІОНАЛЬНІЙ ВАЛЮТІ (SALDO)

| № п/п | Назва реквізиту | Тип | Довжина |
| --- | --- | --- | --- |
| 1 | Номер виконавця | N | 2 |
| 2 | Ознака (активний/пасивний) | L | 1 |
| 3 | Номер рахунку | C | 14 |
| 4 | Залишок на рахунку | N | 16 |
| 5 | Ліміт по рахунку | N | 16 |
| 6 | Сума дебетових оборотів за день | N | 16 |
| 7 | Сума кредитових оборотів за день | N | 16 |
| 8 | Дата попереднього руху по рахунку | D | 8 |
| 9 | Час попереднього руху по рахунку | N | 6 |
| 10 | Тип рахунку | N | 3 |
| 11 | Символ звітності | N | 3 |
| 12 | Відсоткова ставка | С | 7 |
| 13 | Ознака терміну списання | N | 2 |
| 14 | Ознака заключних оборотів | L | 1 |
| 15 | Реєстраційний номер клієнта | N | 6 |
| 16 | Дата відкриття рахунку | D | 8 |
| 17 | Номер шкали (параметр) при нарахуванні відсотків | С | 3 |
| 18 | Вид оплати рахунку (0 — з поточного залишку, 1 — з залишку попереднього дня) | N | 2 |
| 19 | Коефіцієнт ризику при кредитуванні | N | 6 |
| 20 | Дата списання відсотків | D | 8 |
| 21 | Назва рахунку | С | 38 |

ФАЙЛ ЗАЛИШКІВ КОШТІВ НА БАЛАНСОВИХРАХУНКАХ В ІНОЗЕМНІЙ ВАЛЮТІ (SALDOV)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Номер виконавця | N | 2 |
| 2 | Ознака (активний/пасивний) | L | 1 |
| 3 | Код валюти | N | 3 |
| 4 | Номер рахунку | C | 14 |
| 5 | Залишок на рахунку в іноземній валюті | N | 16 |
| 6 | Сума дебетових оборотів в іноземній валюті за день | N | 16 |
| 7 | Сума кредитових оборотів в іноземній валюті за день | N | 16 |
| 8 | Відсоткова ставка | N | 6,2 |
| 9 | Дата попереднього руху по рахунку | D | 8 |
| 10 | Час попереднього руху по рахунку | N | 6 |
| 11 | Залишок на рахунку в національній валюті | N | 16 |
| 12 | Обороти по рахунку в національній валюті дебетові | N | 16 |
| 13 | Обороти по рахунку в національній валюті кредитові | N | 16 |
| 14 | Реєстраційний номер клієнта | N | 6 |
| 15 | Ознака типу відсоткової ставки | L | 1 |
| 16 | Дата відкриття рахунку | D | 8 |
| 17 | Ознака списання відсотків | L | 1 |
| 18 | Ознака переоцінки | L | 1 |
| 19 | Дата останнього списання відсотків | D | 8 |
| 20 | Вид рахунку | N | 2 |
| 21 | Ліміт |  |  |
| 22 | Назва рахунку | С | 38 |

ФАЙЛ ЗАЛИШКІВ КОШТІВ НА ПОЗАБАЛАНСОВИХРАХУНКАХ В ІНОЗЕМНІЙ ВАЛЮТІ (SALDONB)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Реєстраційний номер клієнта | N | 6 |
| 2 | Дата відкриття рахунку | D | 8 |
| 3 | Номер виконавця | N | 2 |
| 4 | Код валюти | N | 3 |
| 5 | Номер позабалансового рахунку | C | 14 |
| 6 | Ознака (активний/пасивний) | L | 1 |
| 7 | Номер особового рахунку | C | 14 |
| 8 | Назва рахунку | С | 38 |
| 9 | Залишок на рахунку в іноземній валюті | N | 16 |
| 10 | Залишок на рахунку в національній валюті | N | 16 |
| 11 | Сума дебетових оборотів в іноземній валюті за день | N | 16 |
| 12 | Сума дебетових оборотів в національній валюті за день | N | 16 |
| 13 | Сума кредитових оборотів в іноземній валюті за день | N | 16 |
| 14 | Сума кредитових оборотів у національній валюті за день | N | 16 |
| 15 | Дата останнього руху по рахунку | D | 8 |

Структури файлів SCHETAS, SCHETAV і SCHETANB аналогічні відповідно структурам файлів SALDO, SALDOV, SALDONB. Файли SCHETAS, SCHETAV і SCHETANB очищаються кожний день при відкритті банківського дня.

ФАЙЛ ДОВІДНИК КЛІЄНТІВ (KLIENT)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Реєстраційний номер клієнта | N | 8 |
| 2 | Назва клієнта | С | 38 |
| 3 | Характеристика контрагента | N | 1 |
| 4 | Код групи країн по ISO | С | 3 |
| 5 | Код платника податків | С | 14 |
| 6 | Ознака інсайдера | С | 2 |
| 7 | Інституційний сектор економіки | С | 5 |
| 8 | Форма власності | С | 2 |
| 9 | Галузь економіки | С | 5 |
| 10 | Вид економічної діяльності | С | 5 |
| 11 | Код клієнта | С | 4 |
| 12 | Поштова скринька | С | 8 |
| 13 | Код по ЕДРПОУ | С | 10 |
| 14 | Тип державної реєстрації (0 — юридична особа, 1 — фізична особа) | N | 1 |
| 15 | Дата реєстрації в держадміністрації | D | 8 |
| 16 | Номер реєстрації в держадміністрації | N | 9 |
| 17 | Дата реєстрації в податковій інспекції | D | 8 |
| 18 | Юридична адреса | С | 50 |
| 19 | Прізвище, ім’я та по-батькові директора | С | 30 |
| 20 | Телефон директора | С | 15 |
| 21 | Головний бухгалтер | С | 30 |
| 22 | Телефон головного бухгалтера | С | 15 |
| 23 | Назва клієнта на англійській мові | С | 38 |
| 24 | Формат виписки для клієнта | С | 1 |
| 25 | Назва за статутом | С | 50 |
| 26 | Назва виконкому | С | 13 |
| 27 | Код обласної податкової інспекції | N | 2 |
| 28 | Код районної податкової інспекції | N | 2 |
| 29 | Ознака для системи «Клієнт-банк» | L | 1 |
| 30 | Дата закриття клієнта | D | 8 |
| 31 | Ознака закриття клієнта | L | 1 |

Файл KLITAS використовується для зберігання даних по клієнтах, які були добавлені, змінені чи закриті протягом дня. Файл KLITAS оновлюється щодня перед початком нового банківського дня. За своєю структурою він аналогічний файлу KLIENT.

Файл BALANS – використовується для нагромадження даних щодо оборотів на рахунках в розрізі усіх місяців під час закриття банківського дня. Він включає такі атрибути: особовий рахунок; код валюти; реєстраційний номер клієнта; тип валюти (0 — гривня, 1 — іноземна грошова одиниця); дебетові обороти за 1-й місяць; кредитові обороти за 1-й місяць; дебетові обороти за 2-й місяць; кредитові обороти за 2-й місяць; … дебетові обороти за 12-й місяць; кредитові обороти за 12-й місяць.

**ФАЙЛ ДЛЯ НАКОПИЧЕННЯ ДАНИХ ПО КАСОВИХ ОБОРОТАХ ЗА ПОПЕРЕДНІЙ І ПОТОЧНИЙ МІСЯЦІ (VKAS)**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Дата | D | 8 |
| 2 | Номер особового рахунку | С | 14 |
| 3 | МФО «чужого» банку (0 — для свого) | N | 9 |
| 4 | Номер особового рахунку клієнта | С | 14 |
| 5 | Касовий символ | N | 2 |
| 6 | Сума | N | 15 |

Довідник валют і курсів (TABVAL) використовується під час роботи з іноземною валютою. Його структуру наведено нижче.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Код валюти по ISO | С | 2 |
| 2 | Код валюти | N | 3 |
| 3 | Міжнародна абревіатура | С | 3 |
| 4 | Назва країни | С | 15 |
| 5 | Еталонна сума | N | 5 |
| 6 | Дата встановлення поточного курсу | D | 8 |
| 7 | Дата встановлення офіційного курсу | D | 8 |
| 8 | Поточний офіційний курс | N | 12 |
| 9 | Попередній офіційний курс | N | 12 |
| 10 | Рахунок технічної переоцінки | С | 14 |
| 11 | Рахунок валютної позиції банку | С | 14 |
| 12 | Рахунок гривневого еквівалента валютної позиції | С | 14 |
| 13 | Рахунок переоцінки валютної позиції банку | С | 14 |
| 14 | Рахунок доходів по операціях з валютою | С | 14 |
| 15 | Рахунок витрат по операціях з валютою | С | 14 |
| 16 | Поточний курс купівлі | N | 12 |
| 17 | Попередній курс купівлі | N | 12 |
| 18 | Поточний курс продажу | N | 12 |
| 19 | Попередній курс продажу | N | 12 |
| 20 | Базова валюта | N | 12 |
| 21 | Назва «копійок» | С | 3 |
| 22 | Код валюти для СЕП | С | 1 |
| 23 | Транзитний рахунок для міждержавних розрахунків | С | 14 |
| 24 | Країна-емітент | С | 3 |

*Оперативні файли*

ФАЙЛ ДОКУМЕНТІВ ДНЯ ПО БАЛАНСОВИХ РАХУНКАХ В НАЦІОНАЛЬНІЙ ВАЛЮТІ (OPER)

| № п/п | Назва реквізиту | Тип | Довжина |
| --- | --- | --- | --- |
| 1 | Номер макета | N | 1 |
| 2 | Номер пачки | N | 3 |
| 3 | Ознака документа (0-дебетовий, 1-кредитовий) | L | 1 |
| 4 | Номер робочого місця операціоніста | N | 2 |
| 5 | МФО банка кореспондента | N | 9 |
| 6 | Номер документа | С | 10 |
| 7 | Вид документа | N | 2 |
| 8 | Номер особового рахунку по дебету | С | 14 |
| 9 | Номер особового рахунку по кредиту | С | 14 |
| 10 | Сума документа | N | 16 |
| 11 | Касовий символ | N | 2 |
| 12 | Дата валютування | D | 8 |
| 13 | Час документа | N | 8 |
| 12 | Дата надходження в банк | D | 8 |
| 13 | Ознака електронного надходження в банк | N | 1 |
| 14 | Номер сеансу відбору в файл типу А | С | 5 |
| 15 | Ознака стадії обробки документа | N | 2 |
| 16 | Ознака для нез’ясованих сум | N | 5 |
| 17 | Ознака заключних оборотів | N | 1 |
| 18 | Ознака дебетового запиту / документа | N | 1 |
| 19 | Ознака блокований / неблокований документ | N | 1 |
| 20 | Ідентифікатор виконавця, що ставить електронний цифровий підпис | С | 6 |
| 21 | Електронний цифровий підпис | С | 64 |
| 22 | Ознака для «Клієнт-банк» | L | 1 |
| 23 | Порядковий номер документа, що прийшов із системи «Клієнт-банк» | С | 3 |
| 24 | Код ЕДРПОУ відправника | С | 14 |
| 25 | Дата документа | D | 8 |
| 26 | Назва відправника | С | 38 |
| 27 | Назва отримувача | С | 38 |
| 28 | Призначення платежу | С | 160 |
| 29 | Рахунки для нарахування плати за розрахунково-касове обслуговування | С | 14 |

ФАЙЛ ДОКУМЕНТІВ ДНЯ ПО БАЛАНСОВИХ РАХУНКАХ В ІНОЗЕМНІЙ ВАЛЮТІ (OPERV)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Номер особового рахунку по дебету | С | 14 |
| 2 | Код валюти по дебету | N | 3 |
| 3 | Номер особового рахунку по кредиту | С | 14 |
| 4 | Код валюти по кредиту | N | 3 |
| 5 | Код валюти, у якій визначена сума | N | 3 |
| 6 | Сума по документу в валюті | N | 16 |
| 7 | Сума по документу в гривнях | N | 16 |
| 8 | Номер пачки | N | 3 |
| 9 | Номер документа | N | 3 |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 10 | Ознака курсу (1 — курс купівлі, 2 — курс продажу, 3 — офіційний, 4 — інший) | N | 1 |
| 11 | Ознака стадії обробки документа | N | 2 |
| 12 | Номер робочого місця, що сформувало проведення | N | 2 |
| 13 | Номер макета | N | 1 |
| 14 | Дата проведення | D | 8 |
| 15 | Призначення платежу | С | 220 |
| 16 | Код країни | N | 3 |
| 17 | Код призначення платежу | С | 4 |
| 18 | Номер сеансу відбору в файл типу А | С | 3 |
| 19 | Ознака блокований / неблокований документ | N | 1 |
| 20 | Рахунок для гривневого проведення по обмінних операціях | С | 14 |
| 21 | Касовий символ для гривневої каси | N | 2 |
| 22 | Рахунок для валютного проведення по обмінних операціях | С | 14 |
| 23 | Касовий символ для валютної каси | N | 2 |

ФАЙЛ ДОКУМЕНТІВ БАНКІВСЬКОГО ДНЯНА ПОЗАБАЛАНСОВИХ РАХУНКАХ (OPERNB)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Ознака проведення документа | N | 1 |
| 2 | Номер паки | N | 3 |
| 3 | Вид документа | N | 4 |
| 4 | Код валюти | N | 3 |
| 5 | Номер документа | С | 10 |
| 6 | Дата проведення | D | 8 |
| 7 | Позабалансовий рахунок по дебету | С | 14 |
| 8 | Особовий рахунок по дебету | С | 14 |
| 9 | Позабалансовий рахунок по кредиту | С | 14 |
| 10 | Особовий рахунок по кредиту | С | 14 |
| 11 | Сума по документу | N | 16 |
| 12 | Номер робочого місця | С | 2 |
| 13 | Призначення платежу | С | 100 |

### 

7.4. **Затвердження "Вимог Національного   
              банку України до програмного комплексу   
                 "Операційний день банку" (ОДБ)"**

     З метою  підвищення  надійності та безпеки внутрішньої роботи банків-учасників системи електронних платежів (СЕП)  Національного банку України та відповідно до статті 54 Закону України "Про банки і    банківську    діяльність"     (     [872-12](http://zakon2.rada.gov.ua/laws/show/872-12)     )    Правління

**П О С Т А Н О В Л Я Є**: 

     1. Затвердити   "Вимоги   Національного   банку   України  до програмного комплексу "Операційний день банку" (ОДБ)"  (додається) як нормативний документ Національного банку України.

     2. Довести  цей  документ  до  усіх   банків-учасників   СЕП, розробників  програмного  забезпечення "Операційний день банку" та систем  "клієнт-банк",  запропонувати  банкам-учасникам   СЕП   до 01.07.96 р.  привести свої програмні комплекси ОДБ у відповідність до вимог Національного банку України  щодо  програмного  комплексу "Операційний день банку".

 Голова Правління                                       В.А.Ющенко 

**Вимоги   
       Національного банку України до програмного комплексу   
                 "Операційний день банку" (ОДБ)"**

     Під ОДБ  у цьому документі розуміється та частина програмного комплексу автоматизації роботи банку-учасника системи  електронних платежів (СЕП) України, яка:

     - веде  внутрішню  базу  даних,  що  містить  інформацію  про обслуговування   розрахункових   рахунків   клієнтів,   про   стан коррахунку в НБУ та іншу;

     - має можливість здійснювати платіжні операції через СЕП;

     - може мати систему "клієнт-банк",  як складову частину,  або взаємодіяти з нею.

     НБУ висуває кілька вимог, яким має відповідати наведений вище програмний  комплекс (ОДБ).  Дотримання цих вимог в повному обсязі повинно забезпечити:

     - систематизацію механізмів обміну платіжними документами між комерційними банками та СЕП;

     - цілісність та інформаційну безпеку стикування ОДБ з СЕП;

     - надійність сукупного функціонування ОДБ і СЕП;

     - розширення асортименту інформаційних послуг СЕП.

**Вимоги до ОДБ розподіляються на такі групи:**

     1. Вимоги до інтерфейсу з АРМ-3 СЕП.

     2. Вимоги  щодо  інформаційної  безпеки   підготовки   файлів   
інтерфейсу з СЕП у середовищі ОДБ.

     3. Вимоги  до  ОДБ  щодо  внутрішньої  інформаційної  безпеки   
банку.

     4. Вимоги щодо інформаційної безпеки системи "клієнт-банк".   
  
**1. Вимоги до інтерфейсу з АРМ-3 СЕП**

     1.1. ОДБ комерційного банку  обмінюється  інформацією  з  СЕП через єдину копію АРМ-3 СЕП тільки за допомогою файлів,  структура та функціональне призначення яких описані в  документі  "Інтерфейс між ОДБ і АРМ-3 системи електронних платежів (СЕП)".   
     1.2. ОДБ не звертається безпосередньо до внутрішніх баз АРМ-3 СЕП, а саме, не виконує ніяких операцій читання та модифікації баз даних АРМ-3.

     1.3. ОДБ веде внутрішній  довідник  банків-учасників  СЕП  на базі файла ^U.

     1.4. ОДБ протягом банківського дня  веде  внутрішнє  значення кореспондентського  рахунку  (КР)  і порівнює його інформацією про стан коррахунку в регіональній  розрахунковій  палаті  (РРП),  яка надається у файлах СЕП (^K, ^V).

     На початок банківського  дня  внутрішнє  значення  КР  в  ОДБ повинно  співпадати  зі  значенням  КР в РРП та зі значенням КР на кінець попереднього банківського дня.

     Протягом банківського   дня   внутрішнє   (що  прогнозується) значення КР в ОДБ відрізняється від значення КР в РРП на  величину оборотів за файлами початкових/зворотних платежів,  обробка яких в ОДБ і/або РРП не завершена.

     Наприкінці банківського  дня  внутрішнє  значення  КР  в  ОДБ повинно співпадати зі значенням КР в РРП.

     1.5. Протягом   банківського   дня   ОДБ   виконує   звірення інформації про файли ^A,  ^B,  що існує в ОДБ,  з інформацією  про них, яка надається у файлах ^T, ^K, ^Z, ^V.

     В разі завершення банківського дня ОДБ виконується підсумкове звірення  взаємодії  СЕП  і  ОДБ:  за файлом ^Z - за кожним файлом окремо, за файлом ^V - за платіжками та за файлами.

     Метою звірення є:

     а) виявляти суперечності у інформації в РРП і ОДБ, щодо:

     - розбіжностей  у  реквізитах  файла (дата та час формування, кількість інформаційних рядків,  суми за пакетом, кодів завершення обробки файлу, електронного підпису;

     - появи інформації про пакети, які не надсилалися (^A) або не приймалися (^B) в ОДБ;

     б) слідкувати за нерозривністю та несуперечністю значення  КР в РРП і ОДБ.

     1.6. Завершення  обробки  файла  ^A  у  СЕП,  і,  відповідно, завершення  проводок  (транзакцій)  в ОДБ за платежами цього файла виконується тільки після  одержання  підтвердження  про  прийняття цього  файла в РРП з нульовими кодами завершення,  яке надається у файлі ^T.  У разі необхідності завершення обробки  файла  ^A  може бути також виконане на підставі інформації про файл ^A у файлах ^K і ^V, яка дублює зміст файла ^T.

     1.7. Завершення обробки прийнятого пакету зворотних платіжних документів (^B),  який нормально підтверджений квитанцією  ^S,  і, відповідно,  завершення  проводки виконується лише після одержання підтвердження про зміну  коррахунку  в  РРП  за  цим  файлом,  яке надходить у файлі ^K з нульовими кодами завершення про цей файл. У разі необхідності завершення обробки  файлу  ^B  може  бути  також виконане на підставі інформації про файл ^B у файлах ^K і ^V,  яка дублює зміст файлу ^S.

     1.8. ОДБ,   які   підтримують   обслуговування   1-ї   моделі консолідованого коррахунку для головного банку,  виконують у  всіх філіях головного банку, які працюють у 1-й моделі, такі звірення:

     - нерозривності технічного коррахунку та  його  відповідності відісланим/прийнятим файлам (по файлах ^K, ^F, ^T);

     - відповідність переліку відісланих/прийнятих файлів платежам філії (за файлами ^K і ^V).

     1.9. У  разі  появи  будь-яких  розбіжностей  в   інформації, виявлених при перевірках пп.1.4, 1.5, 1.8, ОДБ однозначно, негайно та  надійно  інформує  банківський   персонал   і   блокує   обмін інформацією з СЕП до отримання дозволу на продовження роботи.

     1.10. ОДБ  надає  можливість   виведення   (друку)   реєстрів платіжних  документів  СЕП  (як  відісланих,  так  і  одержаних) з розшифровкою закодованих реквізитів типу "Призначення  платежу"  і "Допоміжні  реквізити"  і,  при необхідності,  з усіма реквізитами інформаційного рядку файлів ^A,  ^B (крім електронного підпису  та контрольної суми).

     1.11. В    ОДБ    кожному    клієнту    надано     унікальний ідентифікаційний код клієнта в межах України (ідентифікаційний код з  "Державного  реєстру  звітних/статистичних  одиниць   України", "Державного  реєстру  фізичних  осіб-платників"  чи інший,  згідно діючому законодавству України).

     При формуванні  початкових  платежів  ОДБ повинен автоматично заносити  ідентифікаційний  код  клієнта-відправника   платежу   в електронний    платіжний    документ   після   звірення   його   з ідентифікаційним кодом, який указав клієнт в платіжному документі.

     При отриманні  зворотних  платежів  ОДБ  повинен  автоматично заносити  ідентифікаційний  код   клієнта-отримувача   платежу   в електронний платіжний документ.

     ОДБ не  надає  можливості  ручного  вводу   або   коригування ідентифікаційного   коду   клієнта   в   електронному   платіжному документі. 

**2. Вимоги щодо інформаційної безпеки підготовки   
             файлів інтерфейсу з СЕП в середовищі ОДБ**

     2.1. В  ОДБ повинно бути виділено відокремлене автоматизоване робоче місце (умовна назва "АРМ бухгалтера електронних  платежів", на  якому  відповідальний  працівник  банку  може  виконувати такі функції:

     - перегляд та друк всіх файлів і платіжних документів,  якими обмінювались ОДБ та АРМ-3 протягом банківського дня;

     - перевірка електронного підпису від АРМ-2 СЕП файлів ^T, ^B, ^V, ^K;

     - створення  квитанції  ^S  на відповідний файл ^B або хоча б накладання електронного підпису на адресу АРМ-2 на файл  ^S,  який був створений іншим функціональним блоком ОДБ;

     - накладання електронного підпису  на  адресу  АРМ-2  СЕП  на файли ^A, в разі передачі файлу ^A в АРМ-3 СЕП.

     2.2. АРМ   бухгалтера   електронних    платежів    забезпечує автоматичне  ведення  протоколу  (та  захист  цього  протоколу від модифікації) найбільш критичних  моментів  роботи  АРМ  бухгалтера електронних   платежів   (вхід,   формування   пакетів   платіжних документів, проводки, відкат та інші); архівування цього протоколу в разі закриття банківського дня.

     2.3. ОДБ  забезпечує  неможливість  доступу  з  інших   машин (терміналів),  у  тому  числі  з  робочих міст операціоністів,  до пакетів   платіжних   документів,   сформованих   АРМ   бухгалтера електронних  платежів  для  відправлення  в  АРМ-3 і отриманих від АРМ-3,  та модифікацію цих пакетів.  АРМ бухгалтера фіксує  спроби несанкціонованого   доступу  до  баз  даних  і  пакетів  платіжних документів. 

**3. Вимоги до ОДБ щодо внутрішньої інформаційної   
                          безпеки банку**

     3.1. ОДБ забезпечує розподіл доступу до системних ресурсів (з допомогою  програмних  засобів  або  парольного   захисту),   який організований   за   принципом   надання   мінімальної   кількості повноважень, які необхідні для роботи даного користувача.

     3.2. ОДБ  забезпечує  ідентифікацію  користувача  на  кожному робочому місці.

     3.3. ОДБ  блокує  роботу  програмного забезпечення на кожному робочому  місці  при  багаторазовій  спробі  неправильного   вводу пароля.

     3.4. ОДБ забезпечує автоматичне ведення протоколу (та  захист цього  протоколу від модифікації) парольних входів в ОДБ з кожного робочого місця  і  передачу  платіжних  документів  відповідно  до технологічної  схеми  обробки  електронних  платіжних документів в ОДБ; автоматичне архівування протоколів наприкінці дня.

     3.5. ОДБ  забезпечує  можливість ідентифікації точки введення та проходження платежу в  ОДБ  від  одного  виконавця  до  другого відповідно  до  технологічної  схеми обробки електронних платіжних документів (для платежів, які надходять від операціоністів, АРМ-3, АРМ    клієнтів    банку),    і   включення   програмних   модулів накладення/перевірки  електронного  підпису  на  кожному  робочому місці  для  захисту  платіжних  документів  від  модифікації та їх суворої  аутентифікації.  Для  ОДБ,  які  працюють   у   захищених середовищах,   що  мають  міжнародний  сертифікат  або  сертифікат державних служб України,  і які забезпечують наведений вище захист власними      засобами,      включення      програмних     модулів накладення/перевірки електронного цифрового підпису операціоністів необов'язкове.

     3.6. ОДБ має  бути  створено  таким  чином,  щоб  виконувався контроль  цілісності    програмного   забезпечення   внутрішніми програмними засобами  ОДБ  під  час  запуску  програми.  Наявність внутрішніх  програмних  засобів  контролю цілісності для ОДБ,  які працюють у захищених середовищах,  що мають міжнародний сертифікат або   сертифікат  державних  служб  України,  і  які  забезпечують програмного забезпечення власними засобами, необов'язкова.

     3.7. ОДБ  забезпечує  неможливість  нефіксованих  відкатів на попередні дні  з  перерахунком  (корекцією)  балансів  операційних днів.

     3.8. ОДБ  забезпечує  перевірку  усіх  початкових   платіжних документів    (включаючи   внутрібанківську   проводку)   протягом банківського дня на унікальність (неповторність) пари  реквізитів: номер  особистого  рахунку клієнта-відправника та номер платіжного документа (реквізит "Номер (операційний)  платежу"  інформаційного рядка файла ^A).

     3.9. ОДБ  забезпечує  коректну   обробку   транзакції   після апаратних  та  програмних збоїв,  відкатів та подібного,  протягом операційного дня (з точки зору подвоєння та втрати інформації).

**4. Вимоги щодо інформаційної безпеки системи   
                          "клієнт-банк"**

     4.1. Система    "клієнт-банк"   не   може   мати   можливості безпосередньої передачі або приймання платіжних документів в АРМ-3 банку   або   АРМ   іншого   клієнта,  минуючи  АРМ  операціоніста (бухгалтера).

     4.2. Система   "клієнт-банк"   забезпечує  механізм  звірення (квитовки) файлів початкових і зворотних платежів між банком  (АРМ операціоніста  або  бухгалтера) і АРМ клієнта,  підготовку виписки про платіжні операції з клієнтом в банку протягом банківського дня та   звірення   цієї  інформації  з  інформацією  із  АРМ  клієнта наприкінці дня.

     4.3. Система  "клієнт-банк"  забезпечує  передачу повідомлень між клієнтом  та  банком  у  зашифрованому  вигляді  за  допомогою сертифікованих засобів захисту.

     4.4. Система  "клієнт-банк"  забезпечує  автоматичне  ведення протоколу  (та захист цього протоколу від модифікації) передавання платіжних документів між банком і клієнтом як у банку, так і в АРМ клієнта; автоматичне архівування протоколів наприкінці дня.

     4.5. АРМ клієнта системи  "клієнт-банк"  забезпечує  механізм звірення  (квитовки)  зворотних  платіжних документів і виписки за платіжними операціями клієнта.

     4.6. АРМ  клієнта системи "клієнт-банк" забезпечує накладання електронних цифрових підписів головного  бухгалтера  та  керівника підприємства   (установи)   на   кожному  електронному  платіжному дорученні  клієнта;  банківська  частина   системи   "клієнт-банк" забезпечує  перевірку  наведених  електронних  підписів на кожному електронному платіжному дорученні клієнта.

     4.7. АРМ  клієнта  забезпечує  автоматичне  ведення поточного стану власного рахунку в банку,  враховуючи проведені початкові та зворотні платежі.

**Лекція 8. АВТОМАТИЗАЦІЯ УПРАВЛІННЯ КРЕДИТНИМИ РЕСУРСАМИ**

## 8.1. Характеристика та класифікація кредитів

Кредит — це позичковий капітал банку в грошовій формі, що передається у тимчасове користування на умовах забезпеченості, повернення, строковості, платності та цільового характеру використання.

Кредити, що перевищують 10 відсотків власного капіталу, належать до так званих великих кредитів. Про ці кредити комерційні банки звітують перед Національним банком. Жодний з наданих великих кредитів не повинен перевищувати 25 відсотків власних коштів банку. Загальний обсяг наданих кредитів не може перевищувати восьмикратного розміру власних коштів банку.

Кредити можна класифікувати за багатьма ознаками. Класифікацію кредитів наведено на рис. 8.1.

*За терміном користування* кредити поділяються на:

 короткострокові — до 1 року;

 середньострокові — до 3-х років;

 довгострокові — понад 3 роки.

Строк кредиту, а також відсотки по ньому, як правило, розраховуються з моменту отримання кредиту до повного погашення суми позички та відсотків за її користування .

Короткострокові кредити можуть надаватись банками у разі тимчасових фінансових труднощів, що виникають у зв’язку із витратами виробництва та обігу, не забезпечених надходженнями коштів у відповідні періоди.

Середньострокові кредити можуть надаватись на оплату обладнання, поточні витрати, на фінансування капітальних вкладень.

Довгострокові кредити можуть надаватись для формування основних фондів. Об’єктами кредитування можуть бути капітальні витрати на реконструкцію, модернізацію та розширення вже діючих основних фондів, на нове будівництво, на приватизацію тощо.

*За формою забезпечення* кредити поділяються на:

 забезпечені заставою (майном, майновими правами, цінними паперами);

 гарантовані (банками, фінансами чи майном третьої особи);

 з іншим забезпеченням (поручительством, свідоцтвом страхової організації);

 незабезпечені (бланкові).

*За ступенем ризику*кредити поділяються на: стандартні, під контролем, субстандартні, сумнiвні, безнадiйні.

*За формою надання*кредити бувають: строковий, револьверний, кредитна лiнiя, овердрафт, субординований борг, iншi кредити.

Субординований борг — це позика (забезпечена або незабезпечена), за якою в договірному порядку погоджено, що в разі ліквідації чи банкрутства боржника сплата буде здійснена після задоволення вимог усіх інших кредиторів.

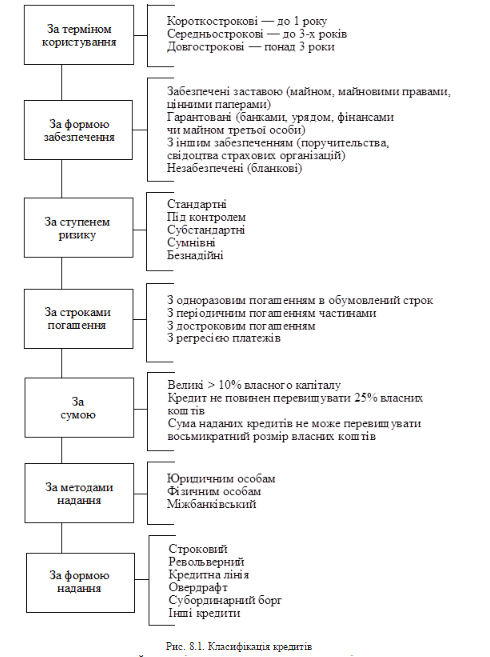
*За строками погашення*кредити поділяються на:

 кредити, що погашаються одноразово, тобто кредит повертається у повній сумі у певний термін;

 кредити, для яких передбачається періодичне погашення суми позички і відсотків по ній певними частинами, що пов’язане з періодичністю надходження виручки від реалізації продукції (проведення робіт, надання послуг);

 кредити, що погашаються достроково ( за вимогою кредитора або за заявою позичальника);

 кредити з регресією платежів.



Для укладення кредитного договору та прийняття рішення про надання кредиту клієнт повинен подати у кредитний відділ такі документи:

1 Заявку на кредит.

2. Копію установчих документів, засвідчених нотаріусом.

3. Баланс (форма № 1 за ДКУД), завірений податковою інспекцією.

4. Звіт про фінансові результати підприємства (форма № 2 за ДКУД).

5. Довідку податкової інспекції про відсутність заборгованості.

6. Цільове призначення кредиту та техніко-економічне обгрунтування заходу, на який береться кредит (бізнес-план).

7. Копії контрактів по угоді, на реалізацію якої береться кредит.

8. Гарантії повернення кредиту і оплати відсотків: гарантія банку, страховий поліс, застава або змішані форми гарантії.

9. Довідка банку про сплату раніше взятих кредитів.

10. Довідка про майно, яке має позичальник.

11. Виписки (завірені банком) по рахунках, що відкриті в інших банках.

12. Довідка позичальника про те, де знаходяться його розрахунковий рахунок і дозвіл для ознайомлення з його станом в будь-який момент часу.

Погашення заборгованості за кредитом та відсотків за ним здійснюється у черговості, яка встановлюється сторонами при укладанні угоди про надання кредиту.

Кошти для погашення заборгованості спрямовують насамперед для сплати відсотків за користування кредитом, потім простроченої заборгованості, а залишки суми направляються на погашення основної суми кредиту.

В банку існують підрозділи, які повинні розглядати кредитну заявку і приймати рішення про надання кредиту. До таких служб належать кредитний, юридичний відділи та відділ безпеки. Кредитний відділ розглядає заявку та супроводжуючі її документи, піддає аналізу стан розрахункового рахунку та рух коштів по ньому, оцінює баланс підприємства й визначає його кредитоспроможність.

Юридичний відділ розглядає юридичний бік угоди, аналізує договори, контракти та інші документи, які надаються позичальником.

Відділ безпеки забезпечує вирішення питань, пов’язаних із забезпеченням безпеки угоди.

Банк здійснює контроль за виконанням умов кредитної угоди, цільовим використанням кредиту, своєчасним та повним його погашенням.

## 8.2. Характеристика підсистеми «Управління кредитними ресурсами банку»

Надаючи великого значення та вагомості управління процесами кредитування, особливу увагу слід приділяти питанням автоматизації задач управління кредитними ресурсами банку. Всі функціональні задачі управління процесами кредитування в комерційному банку виділені в окрему функціональну підсистему «Управління кредитними ресурсами банку».

Підсистема «Управління кредитними ресурсами банку» (далі просто «Кредити») необхідна для автоматизації робіт працівників кредитного, юридичного, аналітичного відділу та відділу безпеки, діяльність яких пов’язана з перевіркою кредитної заявки й установчих документів, прийняттям рішення про кредитування, укладенням кредитного договору та контролем його виконання.

Процес кредитування складається з певної послідовності операцій, які можуть бути згруповані таким чином:

 подання клієнтом-позичальником кредитної заявки та пакета документів, необхідних для отримання кредиту;

 розгляд банком та якісний аналіз кредитної заявки і відповідного пакета документів;

 аналіз кредитоспроможності клієнта-позичальника і оцінка ризику кредитування (кількісний аналіз);

 на основі якісного та кількісного аналізу визначення рейтингу позичальника й прийняття рішення про надання кредиту;

 за умови позитивного для позичальника закінчення попередніх етапів підготовка до укладення кредитної угоди. Цей етап називається структуризацією позички. В процесі структуризації банк визначає такі параметри позички: вид кредиту, суму, строк, спосіб видачі та погашення, забезпечення, ціну кредиту, інші деталі. По закінченні роботи щодо структуризації позички кредитний інспектор банку розпочинає переговори про складання кредитної угоди;

 укладення кредитного договору;

 надання позички оформляється розпорядженням кредитного банку своїй бухгалтерії про відкриття позичкового рахунку;

 контроль за виконанням кредитного договору;

 аналіз кредитного портфелю, формування резервів та необхідної звітності.

Перелічені етапи процесу кредитування не в однаковій мірі можуть бути формалізованими і відповідно автоматизованими. Так, наприклад, операції першого етапу, які полягають у розгляді заявки на кредит та оцінці її обгрунтованості, пов’язані з якісним аналізом і не підлягають автоматизації. Переважна більшість операцій, які виконуються на наступних етапах, досить легко можуть бути формалізованими і вирішеними з використанням ЕОМ.

Підсистема «Кредити» повинна забезпечувати автоматизоване виконання таких функцій:

 аналіз фінансового стану позичальника, визначення його кредитоспроможності, оцінка ризику при кредитуванні;

 ведення файлу кредитних договорів та всієї інформації, що стосується кожного договору;

 ведення й коригування розпоряджень (графіків) на виплату кредитів;

 ведення та коригування строкових зобов’язань (графіків) на погашення кредиту;

 ведення та коригування процентних ставок та графіків оплати відсотків по кредитному договору;

 нарахування відсотків по кредиту та облік їх сплати;

 автоматизований пошук та видача інформації про кредитний договір, розпорядження на оплату і зобов’язання про погашення кредитної заборгованості;

 перегляд залишків на позичкових рахунках, контроль своєчасності погашення позик клієнтами-позичальниками та визначення заборгованості;

 аналіз кредитного портфеля, класифікація кредитів та визначення розміру резервування.

Перелічені функції реалізуються в межах наступних комплексів-задач підсистеми «Кредити»:

1. Оцінка кредитоспроможності позичальника і визначення ступеня ризику його кредитування.

2. Визначення параметрів кредиту та формування кредитного договору.

3. Облік та контроль погашення кредитної заборгованості.

4. Аналіз кредитного портфеля, визначення розміру резервування та формування звітності по кредитуванню.

## 8.3. Автоматизація визначення оцінки кредитоспроможності позичальника і визначення ступеня ризику його кредитування

### 8.3.1. Характеристика задачі

Проводити оцінку кредитоспроможності позичальника необхідно для визначення ступеня ризику його кредитування та прийняття рішення про доцільність або недоцільність його кредитування.

*Кредитоспроможнiсть* — наявнiсть передумов для отримання кредиту i спроможність позичальника вчасно і в повному обсязі погасити позику та відсотки. Кредитоспроможність позичальника визначається показниками, якi характеризують його акуратнiсть при розрахунках за ранiше отриманими кредитами, його поточне фiнансове становище, спроможнiсть у разі необхiдностiмобiлiзувати кошти з рiзних джерел, забезпечення оперативних конверсій активів у ліквідні кошти.

Операції з аналізу стану потенційного позичальника та оцінки ризику його кредитування можна розподілити на дві групи: операції, що не підлягають формалізації, та операції, які можуть бути формалізованими.

До операцій, які складно формалізувати, належать процедури аналізу документальних та недокументальних відомостей про позичальника. Проводиться всебічний аналіз потенційного позичальника. Основним джерелом даних для проведення такого аналізу є документи, які надає клієнт в банк разом із заявкою на кредитування. Крім вивчення основних напрямів діяльності клієнта та його майнового стану, застави чи гарантійних зобов’язань, необхідно звернути увагу на такі фактори, як репутація клієнта, його професіоналізм, ставлення до своїх кредитних зобов’язань в минулому тощо. Тобто для проведення неформального, якісного аналізу, крім інформації, яку надає клієнт, та інформації, що зберігається про нього в архівних файлах бази даних, необхідно використовувати інші джерела інформації: публікації в періодичних виданнях, відомості з виставок, презентацій, рекламних буклетів, дані податкових інспекцій та інші дані.

Формалізована частина аналізу і оцінки кредитоспроможності позичальника залежить насамперед від структури, розмірів банку, його кредитної політики. Тому кожний банк виробляє свою методику оцінки кредитоспроможності позичальника, при розробці якої враховуються рекомендації НБУ, затверджені постановою Правління НБУ № 323 від 29 вересня 1997 р.

Розглянемо аналіз кредитоспроможності, заснований на визначенні ряду коефіцієнтів, що характеризують фінансовий стан клієнта та його зміни в часі.

### 8.3.2. Вхідна інформація

Вхідна інформація, що використовується для автоматизованого проведення такого аналізу, являє собою первинні документи і файли з інформацією про клієнта, що зберігаються в базі даних.

Для вирішення задачі використовуються такі інформаційні файли:

довідник статей балансу (STAT\_B). Він містить код рядка статті балансу, назву статті балансу, нормативне значення показника;

довідник статей звіту про фінансові результати підприємств (STAT\_Z). Він містить: код рядка звіту, назву рядка звіту, нормативне значення показника;

файл «Договір» (KRED\_DOG) містить дані кредитних договорів, які брав клієнт раніше;

файл «Проведень» (PROW) містить дані про кредитну дисципліну клієнта за раніше укладеними договорами;

файл «Клієнтів» (KLIENT) містить дані про клієнтів та їхні характеристики. Цей файл формується на основі установчих документів.

Основними первинними документами для розрахунку є бухгалтерські документи, які надаються клієнтом, а саме: «Баланс підприємства» (Форма № 1 за ДКУД) і «Звіт про фінансові результати підприємства» (Форма № 2 за ДКУД). Ці документи, завірені податковою інспекцією, надаються банку за станом на кінець передостаннього і останнього звітного періоду у формах, відповідних вимогам державних стандартів 19.2-75 «Система обліково-статистичної, первинної облікової, фінансової та іншої документації».

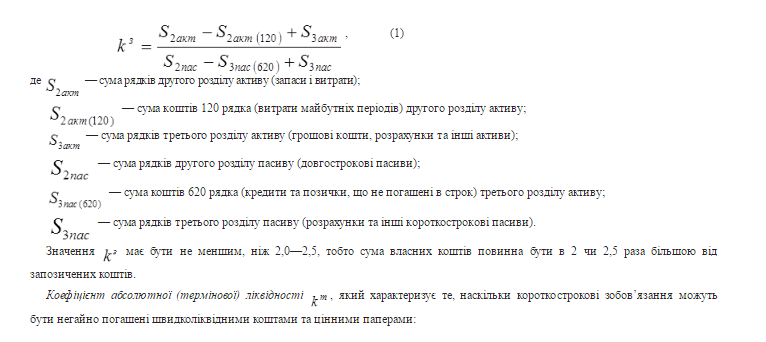
Якщо документи подаються у першому кварталі, то для аналізу подаються також дані за останній рік і передостанній квартал.

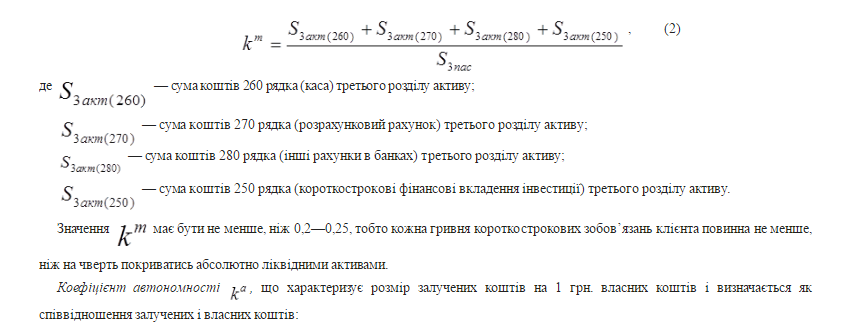
На підставі зазначених первинних документів формуються файли бази даних «Баланс» (BALANS) і «3віт» (ZWIT). Файл «Баланс» (BALANS) та «3віт» (ZWIT) подібні за своєю структурою. Вони містять: код ЕДРПОУ, дату, код статті (рядка), фактичне значення статті (рядка).

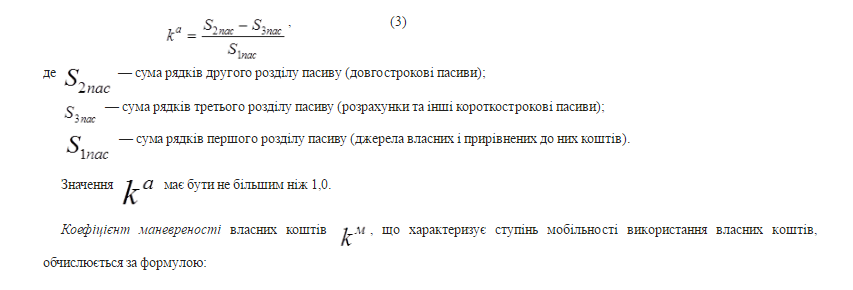
### 8.3.3. Алгоритм визначення показників кредитоспроможності

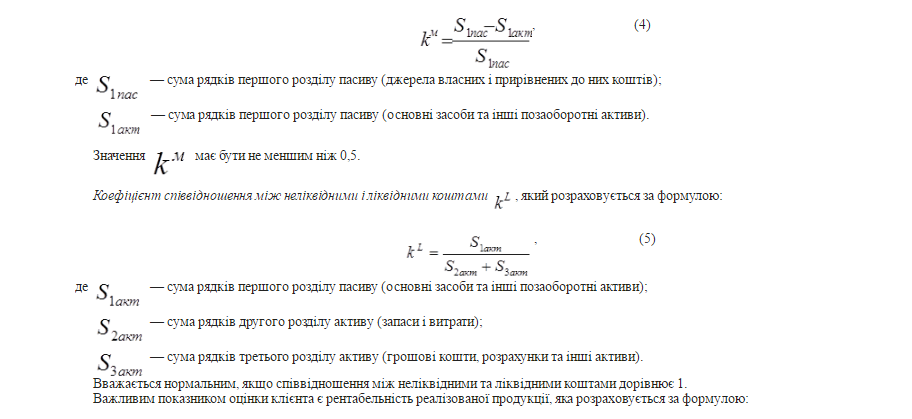
Якщо позичальниками є юридичні особи, то згідно з рекомендаціями НБУ для визначення кредитоспроможності, розраховуються такі коефіцієнти.

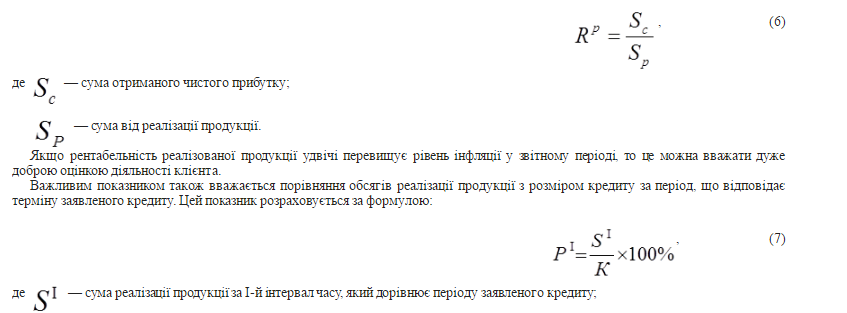
*Коефіцієнт загальної ліквідності*  характеризує наскільки обсяг поточних зобов’язань за кредитами і розрахунками можна погасити за рахунок усіх мобілізаційних активів:











*К* — сума заявленого кредиту.

Дуже добрим вважається цей показник, якщо він дорівнює 200%%.

Також мають бути враховані фактори суб’єктивного характеру:

 ефективність менеджмента позичальника;

 стан позичальника на ринку та його залежність від циклічності, структурних змін в економіці та галузі;

 погашення кредитної заборгованості позичальником в минулому;

 наявність державних замовлень та державна підтримка позичальника;

 професіоналізм керівництва.

*Оцінка фінансового стану позичальника — комерційного банку* здійснюється на підставі:

 аналізу прибутків та збитків;

 аналізу якості активів та пасивів;

 створення резервів;

 виконання зобов’язань комерційним банком у минулому;

 аналізу якості банківського менеджменту.

*Оцінка фінансового стану позичальника —*фізична особа повинна враховувати:

 наявність реальної застави;

 вік та здоров’я клієнта;

 загальний матеріальний стан клієнта, його доходи та витрати;

 інтенсивність користування банківськими позиками в минулому та своєчасність погашення їх і відсотків за ними, а також користування іншими банківськими послугами.

Згідно з оцінкою фінансового стану позичальника та перспективами його розвитку кредити слід віднести до таких категорій:

 клас «А» — фінансова діяльність дуже добра і дає змогу погашати основну суму кредиту та відсотків по ній у встановлені строки. Водночас можна зробити висновок, що фінансова діяльність надалі здійснюватиметься на такому ж високому рівні;

 клас «Б» — фінансова діяльність добра або дуже добра, але немає можливості підтримувати її на цьому рівні протягом тривалого часу;

 клас «В» — фінансова діяльність задовільна, але спостерігається чітка тенденція до погіршення;

 клас «Г» — фінансова діяльність погана і спостерігається її чітка циклічність протягом коротких періодів часу;

 клас «Д» — фінансова діяльність свідчить про збитки, і очевидно, що ні основна сума кредиту, ні відсотки по ній не можуть бути сплачені.

Згідно з оцінкою фінансового стану позичальника та перспектив його розвитку кредити оцінюються й поділяються на класи:5 балів — «дуже добре» — клас А; 4 — «добре» — клас Б; 3 бали — «задовільно» — клас В; 2 — «погано» — клас Г; 1 бал — «дуже погано» — клас Д.

Крім формальної оцінки за коефіцієнтами, підставою для віднесення до того чи іншого класу є такі характеристики:

 період діяльності фірми з часу державної реєстрації;

 період діяльності фірми з дня останньої структурної реорганізації або понад 20%% змін у складі акціонерів (власників);

 наявність (відсутність) фактів неповернення або несвоєчасного повернення кредитів;

 наявність (відсутність) фактів несплати відсотків або несвоєчасної їх сплати;

 прибуткова (збиткова) діяльність позичальника.

Зведену оцінку фінансового стану позичальника наведено в таблиці 8.1. Кожній з характеристик, за якою проводиться оцінка, присвоюється певний ваговий коефіцієнт, відповідно до ролі характеристик в загальній оцінці кредитоспроможності. Вагові коефіцієнти визначаються експертним шляхом аналітиками кредитного відділу. Вони можуть змінюватись залежно від економічної ситуації та стану ринку кредитних ресурсів.

*Таблиця 8.1*

**ТАБЛИЦЯ ОЦІНОК КРЕДИТОСПРОМОЖНОСТІ ПОЗИЧАЛЬНИКА**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Характеристики | Вага | Оцінка | | | | |
| «Дуже добре»(5 балів) Клас А | «Добре» (4 бали) Клас Б | «Задовільно» (3 бали) Клас В | «Погано» (2 бали) Клас Г | «Дуже погано» (1 бал) Клас Д |
| 1 | Період діяльності фірми (з часу реєстрації) | 4 | Більше5 років | Від 3 до 5 років | Від 1 до 3 років | Від 0,5 до 1 року | Менше 0,5 року |
| 2 | Період діяльності фірми з дняостанньої структурноїреорганізації або зміни в складі акціонерів(власників) понад 20%% | 3 | Більше 1,5 року | Від 1 до 1,5 року | Від 0,5 до 1 року | Від 3 місяців до 0,5 року | Менше 3 місяців |
| 3 | Наявність фактівнеповернення або несвоєчасного повернення кредитів | 7 | Відсутні | Відсутні | Присутні | Присутні | Присутні |
| 4 | Факти несплати відсотків або несвоєчасної їх сплати | 7 | Відсутні | Відсутні | Присутні | Присутні | Присутні |
| 5 | Перекриття суми кредиту сумою застави по найменшій із двох (балансова і ринкова вартість) | 10 | Більше як 200%% | Від 125%% до 200%% | Від 100%% до 125%% | Від 50%% до 100%% | Менше 50%% |
| 6 | Прибуткова (збиткова) діяльністьпозичальника | 5 | Прибуток більше3 років | Прибуток від 1 до 3 років | 0 | Збитки менше1 року | Збитки більше1 року |
| 7 | Економічна оцінка фінансової діяльності позичальника (*kз*,*km*, *ka*, *kM*, *kL*) | 3 | Виконано 4 або 5 коефіцієнтів | Виконано 3 коефіцієнти | Виконано 2 коефіцієнти | Виконаний1 коефіцієнт | Не виконано жодного коефіцієнта |
| 8 | Обсяг реалізаціїпорівняно з розміром кредиту (за період, що дорівнює терміну кредиту) | 7 | Більш як 200%% | Від 100 до 200%% | 100%% | Менше 100%% | Менше 50%% |
| 9 | Рентабельність роботи підприємства за період, що дорівнює терміну кредиту і довше (відношення чистого прибутку до обсягу реалізації) | 4 | Більше рівня інфляції в 2 рази у звітному періоді | Більше рівня інфляції у звітному періоді | Дорівнює рівню інфляції у звітному періоді | Менше рівня інфляції у звітному періоді | Менше рівня інфляції у звітному періоді |
| **Всього** балів: | | **50** | **250** | **200** | **150** | **100** | **50** |

### 8.3.4. Вихідні повідомлення

В результаті розв’язку задачі формується вихідна інформація й видається по групах показників за попередній і останній звітний періоди. Крім того, видається інформація про допустимі значення зазначених показників, на що слід орієнтуватися при їх аналізі. Під час розв’язання задачі формуються такі вихідні дані:

1. Вихідний документ «Відомість аналізу взаємовідносин банку з клієнтом-позичальником» (WED1). Цей документ формується на основі масиву проведень (PROW) та масиву кредитних договорів (KRED\_DOG). Документ призначений для аналізу взаємовідносин банку з позичальником, які були ра-ніше, а також для того, щоб мати уявлення про даного клієн-та до розрахунку оціночних показників його діяльності. Ця відомість може бути сформована у випадку, якщо клієнт, що звернувся за кредитом, має кредитну історію в даному банку. Якщо кредитна історія є незадовільною, то відразу може бути прийняте рішення про відмову клієнту у наданні позички.

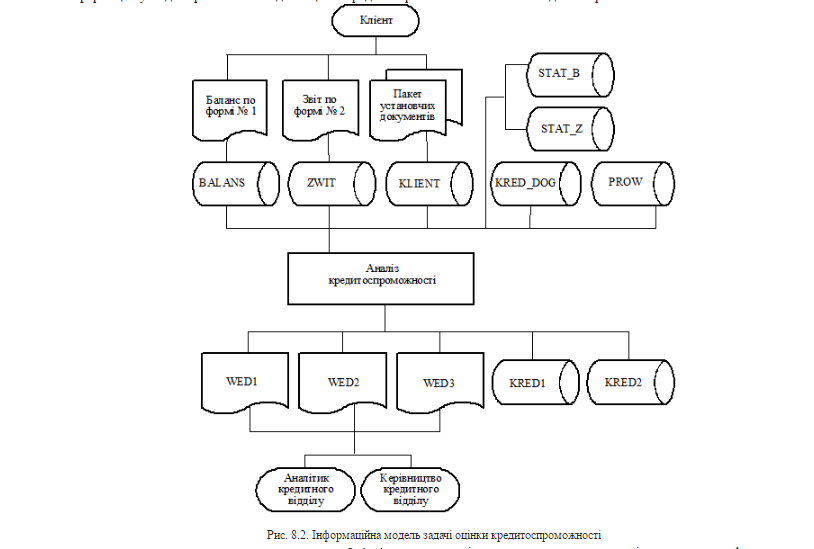
2. Вихідний документ «Відомість показників, що характеризують всю діяльність клієнта» (WED2) містить показники, які розраховуються згідно з описаними в алгоритмі формулами і свідчать про ефективність діяльності, їх динаміку та відповідність допустимим значенням. Цей документ формується в тому випадку, коли результати відомості WED1 були оцінені як такі, що дають підставу для розгляду питання про надання позички клієнту.

3. Вихідний документ «Відомість загальних показників діяльності клієнта» (WED3), що містить рейтингову оцінку щодо основних груп показників, на підставі якої працівник і керівник кредитного відділу приймають рішення про кредитування.

Названі відомості подаються на розгляд кредитної комісії, яка приймає остаточне рішення.

За структурами аналогічних відомостей WED2 та WED3 формуються і зберігаються вихідні файли бази даних KRED1, KRED2.

Інформаційну модель розв’язання задачі оцінки кредитоспроможності клієнта наведено на рис. 8.2.



## 8.4. Автоматизація визначення параметрів кредиту та формування кредитного договору

Комплекс задач щодо визначення параметрів та формування кредитного договору складається з таких основних функціональних задач:

 Формування кредитних договорів.

 Формування календарного графіка видачі кредиту.

### 8.4.1. Автоматизація формування кредитних договорів

Однією з основних задач підсистеми є задача формування кредитних договорів та їх ведення. Основними функціями програм, що автоматизують формування кредитного договору, є надання можливості користувачу модифікувати типову форму договору й отримати необхідну кількість його друкованих копій, формування файлу кредитних договорів (KRED\_DOG), ведення архіву договорів, групування їх за певними ознаками, автоматизований пошук та видача інформації про певний кредитний договір.

Усі кредитні договори ідентифікуються унікальними номерами і закріплюються за конкретними кредитними інспекторами, які мають право вводити, коригувати, вилучати і закривати закріплені за ними договори.

Перед розв’язанням задачі необхідно ввести в файл «Довідник клієнтів» (KLIENT) відповідні дані про клієнта, якому надається кредит, якщо ці дані про нього не були введені раніше. Дозапис у файл KLIENT виконується у випадку, якщо клієнт не обслуговується в даному банку. Формування і ведення до-відника клієнтів виконується в підсистемі «Операційний день банку».

Після прийняття рішення про надання кредиту співробітником кредитного відділу оформляється розпорядження про відкриття позичкового рахунку та рахунку відсотків, на які буде нарахована сума кредиту та сума відсотків по кредиту. Інформація про відкриті рахунки записується у файл «Рахунок» (SCHETAS). Кредитні рахунки відкриваються також в підсистемі «Операційний день банку». У разі необхідності в цій же підсистемі відкривається рахунок прострочки.

Після формування файлів KLIENT, SCHETAS розпочинають складання кредитного договору, і відповідно формується файл KRED\_DOG.

### 8.4.2. Автоматизація формування календарного графіка видачі кредиту

Залежно від виду кредиту видача коштів клієнту може виконуватись одноразовим перерахуванням всієї суми з позичкового рахунку на його розрахунковий рахунок чи частинами в міру надання позичальником документів на придбання товарів та послуг.

Якщо сума кредиту надається частинами, то після формування кредитного договору розробляється календарний графік його видачі клієнту, який містить дати та конкретні суми, що будуть надаватись позичальнику. При формуванні графіка видачі кредиту клієнту враховуються перш за все фінансові можливості банку. Календарний графік видачі кредиту в роздрукованому вигляді надається клієнту, а у вигляді відповідного файла (GRAF\_K) зберігається в базі даних.

Згідно з цим графіком на АРМ кредитного інспектора формуються розпорядження щодо перерахування банком клієнту певної суми позички, яка надається в операційне відділення банку. Форму розпорядження наведено на рис. 4.3.

Розпорядження на оплату по договору №\_\_\_\_\_\_

Рахунок №\_\_\_\_\_\_\_\_\_\_\_\_ Клієнт\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| Дата оплати | Сума до оплати | Залишилось сплатити | Валюта |
|  |  |  |  |

Рис. 8.3. Форма розпорядження на оплату по кредитному договору

## 8.5. Автоматизація обліку та контролю погашення кредитної заборгованості

Комплекс задач з обліку та контролю за погашенням кредитної заборгованості складається з таких задач.

 Формування календарного графіка нарахування та виплати відсотків по кредитній угоді.

 Формування календарного графіка погашення кредиту.

### 8.5.1. Автоматизація формування календарного графіка нарахування та виплати вісотків по кредитній угоді

Формуванню календарного графіка нарахування та виплати відсотків по кредитній угоді передує розрахунок сум відсотків.

Календарний графік нарахування та виплати відсотків по кредитній угоді містить суми та дати погашення відсотків по ньому. Цей графік у вигляді файла бази даних (GRAF\_V) зберігається в базі даних. Роздрукований екземпляр графіка видається клієнту.

Форми документа наведено на рис. 8.4.

Якщо погашення відсотків по кредиту виплачується одночасно і повністю, то даний документ буде вміщувати лише один рядок.

Графік сплати відсотків по договору №\_\_\_\_\_\_

Рахунок №\_\_\_\_\_\_\_\_\_\_\_\_ Клієнт\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дата погашення (планова) | Сума нарахованих відсотків | Дата погашення (фактична) | Сума погашення відсотків | Валюта |

Рис.8.4. Графік сплати відсотків по кредитному договору

Відсоткова ставка та порядок нарахування відсотків по кре-дитному договору залежить від умов, які визначаються в договорі на кредитування.

Відсоткова ставка може бути таких видів: проста (постійна); змінна в часі (по даті установки); залежна від залишку, змінна в часі і залежна від суми залишка (дата + залишок). Відсоткові ставки та порядок їх нарахування можуть бути різними по рахунку кредиту та рахунку прострочки.

Сума плати за кредит може бути розрахована за формулою:

*W* = (*S*  *D*  *P*) / (365  100),

де*W* — сума нарахованих відсотків;

*S* — сума наданої позички;

*D* — термін (в днях), на який надано кредит;

*P* — річна відсоткова ставка, під яку було надано кредит.

Відсоткова ставка може бути змінена в результаті зміни ставки рефінансування НБУ чи зі зміною ситуації на ринку кредитних ресурсів.

### 8.5.2. Автоматизація формування календарного графіка погашення кредиту

Календарний графік погашення кредиту містить дати та суми погашення кредитної заборгованості*.*Форма його подібна формі графіка погашення відсотків. Аналогічно, як у попередньому випадку, формується файл графіка погашення суми позички за кредитним договором (GRAF\_K), а роздрукований екземпляр графіка передається клієнту.

Форму графіка наведено на рис. 8.5.

Графік погашення суми позички по кредитному договору №\_\_\_\_\_\_

Рахунок №\_\_\_\_\_\_\_\_\_\_\_\_ Клієнт\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Дата погашення (планова) | Сума, що підлягає погашенню | Дата погашення (фактична) | Сума погашення (фактична) | Залишилось сплатити | Валюта |

Рис. 8.5. Графік погашення кредиту

Якщо погашення кредитної заборгованості має виконуватись одночасно і повністю, то даний документ міститиме лише один рядок.

Сформовані календарні плани — графіки видачі кредиту, погашення відсотків та погашення кредитної заборгованості за окремими кредитами повинні накладатись на зведені графіки по всіх кредитах банку, що дасть змогу оцінити й узгодити можливості клієнта і банку, оцінити фінансовий стан банку та його ресурси.

Погашення відсотків та позички по кредитному договору клієнтом виконується через операційний відділ за допомогою платіжних доручень. Отже, існує певний розподіл операцій між кредитним та операційним відділами банку.

За операційним відділом закріплюється виконання наступних функцій: обслуговування видачі кредиту, проведення платежів по погашенню позички та відсотків, пені за несвоєчасну сплату позичок та відсотків.

Якщо позичальник порушив умови платежів, то кредитним інспектором приймається рішення про переведення договору на рахунок прострочки, по якому нараховується пеня. При наявності відповідної заяви позичальника з обгрунтуванням причин прострочки проводиться пролонгування договору й відповідне коригування графіків сплати відсотків та сплати позички.

Для аналізу погашення кредитної заборгованості може ще видаватись кредитний журнал, який надає кредитному інспектору повну картину про стан погашення позички та відсотків по ній. Форму кредитного журналу наведено на рис. 8.6.

*Таблиця 8.2*

**КРЕДИТНИЙ ЖУРНАЛстаном на \_\_\_\_\_\_\_ 20\_ р.**

**Операціоніст\_\_\_\_\_\_**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Назва клієнта—позичальника | | № договору | Дата укладення договору | | Дата закінчення строку договору | | Відсоток по договору | | Сума | Дата початку нарахування відсотків | | Дата закінчення нарахування відсотків | |
| Сума погашення основного боргу | Сума заборгованості по основному боргу | | | Сума погашення відсотків | | Сума заборгованості по відсотках | | Сума пені (штрафу) за прострочення платежів | | | Дата пролонгації | | Кількість днів пролонгації |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Рис. 8.6. Кредитний журнал

Крім зазначеного вище журналу на запит користувача система повинна сформувати і видати на екран чи на друкування такі вихідні повідомлення: відомість погашених кредитів за період; відомість прострочених і не погашених кредитних договорів; відомість пролонгованих кредитів; відомість кредитних договорів з простроченими відсотками та ін.

## 8.6. Автоматизація аналізу кредитного портфеля, визначення розміру резервування та формування звітності по кредитуванню

### 8.6.1. Автоматизація аналізу кредитного портфеля

Під час автоматизації аналізу кредитного портфеля проводиться аналіз його структури. Кредитному інспектору та керівництву банку надається можливість переглянути й проаналізувати зведені показники по діючих кредитах в розрізі заданих групувальних ознак. Основні групувальні ознаки, за якими проводиться аналіз та оцінка кредитного портфеля, такі:

 по валютах;

 по термінах користування (довгострокові, середньострокові, короткострокові, пролонговані, прострочені);

 по строках погашення;

 за видами забезпечення;

 за категоріями ризику;

 в розрізі відсоткових ставок;

 за видами (клієнтські, міжбанківські);

 по договорах;

 по позичальниках.

При виборі групувальної ознаки, за якою проводиться оцінка, на екран користувача видається відповідна форма, яку в разі необхідності він може роздрукувати. Нижче наводяться деякі з вихідних форм, за якими проводиться аналіз та оцінка кредитного портфеля:

**СТРУКТУРА КРЕДИТНОГО ПОРТФЕЛЯ ПО ВИДАХ ВАЛЮТ станом на \_\_\_\_\_\_\_\_**

                                                                                          дата

|  |  |  |
| --- | --- | --- |
| Валюта | | Сума |
| Назва | Позначення |
|  |  |  |

**СТРУКТУРА КРЕДИТНОГО ПОРТФЕЛЯ ПО СТРОКАХ ТА ВАЛЮТАХ**

**станом на \_\_\_\_\_\_\_\_\_\_\_**

                                                                                                  дата

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Строк | Сума | | | |
| В гривнях (UAH) | В доларах США (USD) | В німецьких марках (DEM) | В російських рублях (RUR) |
|  |  |  |  |  |

**СТРУКТУРА КРЕДИТНОГО ПОРТФЕЛЯ ПО КЛІЄНТАХ ТА ДОГОВОРАХстаном на \_\_\_\_\_\_\_\_\_\_\_**

                                                                                               дата

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Назваклієнта | Секторекономіки | Номердоговору | Датапогашеннякредиту | Сумакредиту | Сумазаборгованості |
|  |  |  |  |  |  |

### 8.6.2. Автоматизація визначення розміру резервування

Одним із способів управління кредитним портфелем банку є створення внутрішнього банківського резерву для покриття можливих збитків від результатів кредитної діяльності.

Створення резерву регламентується положенням про порядок формування і використання резерву для відшкодування можливих втрат за кредитними операціями комерційних банків, затвердженого постановою Правління Національного банку України № 122 від 27 березня 1998 р.

Згідно з цим положенням комерційні банки повинні на перше число кварталу розглянути кредитний портфель банку з метою оцінки кредитних ризиків і формування резерву.

Резерв поділяється на загальний та спеціальний:

*загальний резерв*нараховується на стандартні кредити;

*спеціальний* — на нестандартні кредити, а саме: під контролем, субстандартні, сумнівні, а також на безнадійні кредити.

Комерційні банки зобов’язані створювати резерви длявідшкодування можливих втрат щодо основного боргу (без відсотків комісій) за всіма видами наданих кредитів, за винятком бюджетних кредитів, а також кредитів та депозитів між установами в системі одного комерційного банку.

Для визначення резерву комерційний банк здійснює класифікацію виданих кредитів та оцінку кредитних ризиків з урахуванням таких критеріїв:

 оцінки фінансового стану позичальника;

 стану погашення позичальником кредитної заборгованості за основним боргом та відсотків по ньому.

Критерії оцінки фінансового стану позичальника та порядок їх розрахунку при визначенні резерву методично збігаються з показниками, які обчислюються при визначенні кредитоспроможності клієнта. Але, враховуючи те, що балансові показники та техніко-економічні показники діяльності не є сталими в часі, оцінку фінансового стану позичальника необхідно робити кожного кварталу на підставі звітних документів про результати діяльності за квартал.

Крім оцінки фінансового стану, необхідно проводити аналіз погашення кредитної заборгованості та відсотків по ній. На основі такого аналізу проводиться оцінювання процесу погашення заборгованості та класифікація кредитних договорів. Погашення позичальником кредитної заборгованості за основним боргом та відсотків по ній є:

 *добрим,*якщо заборгованість за кредит та відсотки по ньому сплачуються у встановлені строки, та за кредит, пролонгований один раз на строк не більше 90 днів;

 *слабким*, якщо прострочена заборгованість за кредит та відсотки за ним становлять не більше 90 днів або заборгованість за кредит, пролонгований на строк понад 90 днів, якщо відсотки сплачуються;

 *недостатнім*, якщо прострочена заборгованість за кредит і відсотки по ньому становлять понад 90 днів або заборгованість за пролонгований кредит понад 90 днів та відсотки не сплачуються.

Класифікацію кредитного портфеля наведено в таблиці 4.3.

*Таблиця 8.3*

**КЛАСИФІКАЦІЯ КРЕДИТНОГО ПОРТФЕЛЯ**

|  |  |  |  |
| --- | --- | --- | --- |
| ПогашенняСтан (клас) | Добре | Слабке | Недостатнє |
| А | Стандартний | Під контролем | Субстандартний |
| Б | Під контролем | Субстандартний | Сумнівний |
| В | Субстандартний | Сумнівний | Безнадійний |
| Г | Сумнівний | Безнадійний | Безнадійний |
| Д | Безнадійний | Безнадійний | Безнадійний |

За кредитами, якщо прострочена заборгованість (або загальний строк пролонгації) становить від 180 до 360 днів, до розрахунку резерву приймається не більше 25%% вартості майна та майнових прав визначеної договором застави.

За кредитами, якщо прострочена заборгованість (або загальний строк пролонгації) перевищує 360 днів, резерв формується на всю суму основного боргу за кредитом незалежно від наявності застави.

Оцінка ризику та відсотки резервування по групах кредитів наведено в таблиці 4.4.

*Загальний резерв* за стандартними кредитами формується у повному обсязі щоквартально за рахунок прибутку минулого року.

*Спеціальний резерв* за кредитами під контролем, субстандартними, сумнівними та безнадійними формується за рахунок відрахувань, що відображаються за групою рахунків «Відрахування в резерви».

*Таблиця 8.4*

**ТАБЛИЦЯ СТУПЕНІВ РИЗИКУ ТА ВІДСОТКІВ РЕЗЕРВУВАННЯ**

|  |  |
| --- | --- |
| Група кредитів | Рівень резерву (ступінь ризику) |
| Стандартні кредити | 2%% |
| Кредити під контролем | 5%% |
| Субстандартні кредити | 20%% |
| Сумнівні кредити | 50%% |
| Безнадійні кредити | 100%% |

Спеціальний резерв формується згідно з певним графіком:

за безнадійними кредитами резерв в повному обсязі формується в кварталі наступному за тим, в якому було виявлено безнадійний кредит;

за кредитами під контролем, субстандартними та сумнівними резерв нараховується згідно з формулою:

*S* = 12,5%%  *N*  *C*,

де 12,5%% — постійний відсоток, що забезпечує формування резерву рівними частками у встановлений строк (100%% : 8 кварталів);

*N* — кількість кварталів з початку формування резерву;

*C* — сума розрахункового резерву, що встановлюється на відповідну квартальну дату.

В результаті розв’язання задачі формується ряд вихідних повідомлень, зокрема такі:

**ВІДОМІСТЬ РОЗРАХУНКУ РЕЗЕРВУ ЗА КРЕДИТНИМИ ОПЕРАЦІЯМИна \_\_\_квартал 20\_\_\_р.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Групи за категоріями ризику | Заборгованість за кредитами на початок кварталу | Вартість гарантії та застави | Чиста сума (2—3) | Рівень резервування (%%) | Рівеньрезервування | | |
| Сума резерву, що має бути сформована на квартал | Фактично сформований резерв | Відхилення (+), (-) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Стандартні |  |  |  |  |  |  |  |
| Під контролем |  |  |  |  |  |  |  |
| Субстандартні |  |  |  |  |  |  |  |
| Сумнівні |  |  |  |  |  |  |  |
| Безнадійні |  |  |  |  |  |  |  |

**ЗВІТ ПРО ЗМІНИ В РЕЗЕРВІза \_\_\_\_\_\_\_ квартал 20\_\_\_р.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

                                                           назва банку                    адреса банку

|  |  |  |  |
| --- | --- | --- | --- |
| Аналіз змін у резервах на покриття збитків за кредитами та фінансовим лізингом | Загальний резерв | Спеціальний резерв | Усього |
| Залишок на початок кварталу |  |  |  |
| Збільшення резерву за рахунок: |  |  |  |
| 1. Збільшення загального обсягу резерву відповідно до щоквартальних уточнень |  |  |  |
| 2. Повернення раніше списаної заборгованості |  |  |  |
| Зменшення резерву за рахунок: |  |  |  |
| 1. Зменшення загального обсягу резерву відповідно до щоквартальних уточнень |  |  |  |
| 2. Списання безнадійної заборгованості |  |  |  |
| Залишок на кінець звітного кварталу |  |  |  |

За результатами оцінки кредитного портфеля і визначення резервів формуються звіти, які надаються НБУ:

звіти «Про класифіковані кредити за формами власності» та «Про розрахунок резерву та можливі втрати за кредитами комерційного банку» складаються на підставі аналізу кредитного портфеля і відображають рівні ризику та резервування на наступний квартал;

звіти «Про зміни в резервах» та «Про списану безнадійну заборгованість» складаються на підставі обліку проведених операцій за минулий квартал.

## 8.7. База даних підсистеми «Кредити»

Підсистема «Кредити» інформаційно повинна бути інтегрована в АБС. Файли, які використовуються для автоматизованого розв’язання задач підсистеми «Кредити», умовно поділимо на дві групи: файли загального та файли спеціального призначення.

До першої групи файлів належать файли, які зберігаються на сервері АБС, тобто це файли, які формуються іншими підсистемами, зокрема ОДБ.

До другої групи належать файли, пов’язані із специфікою кредитування, формуються в підсистемі «Кредити» і потрібні в роботі лише співробітникам кредитного підрозділу. Ці файли доцільно зберігати в БД на сервері кредитного відділу.

До першої групи файлів належать такі: залишок на рахунках;довідник клієнтів, довідник банків; довідник валют і курсів; довідник форм власності; довідник податкових інспекцій; довідник секторів економіки; довідник організаційно-правових норм господарювання; довідник галузей економіки; довідник видів економічної діяльності.

Перші чотири файли з наведеної групи розглянуті в підсистемі ОДБ. Зупинимося на файлах-довідниках цієї групи, які використовуються під час формування довідника клієнтів, для ведення аналітичного обліку та для аналізу кредитного портфеля.

*«Довідник форм власності*» — код форми власності, назва форми власності. Формується згідно з Державним класифікатором України ДК-001-94 під назвою «Класифікатор форм власності». Він затверджений наказом № 288 Держкомстату України від 22 листопада 1994 р. і включає такі параметри: державна власність; приватна власність; колективна власність. Державна власність розподіляється на загальнодержавну і комунальну власність, власність інших держав, власність міжнародних організацій та юридичних осіб інших держав.

«*Довідник податкових інспекцій*» — код податкової інспекції, назва податкової інспекції.

*«Довідник секторів економіки*» — код сектора економіки, назва сектора економіки.

Сектор економіки визначається для клієнтів-резидентів відповідно до «Методичних рекомендацій щодо класифікації інституційних секторів економіки», затверджених наказом № 172 Мінстату України від 25 липня 1994 р. Для клієнтів-резидентів може приймати такі значення: банки; небанківські фінансові установи; центральний уряд; місцеві органи самоуправління; державні нефінансові установи; недержавні нефінансові установи; домашні господарства; некомерційні організації, що обслуговують домашні господарства.

«*Довідник організаційно-правових норм господарювання*» — код організаційно-правової норми господарювання, назва організаційно-правової норми господарювання.

Організаційно-правова норма господарюваннявизначається згідно з Державним класифікатором України ДК-002-94 під назвою «Класифікатор організаційно-правових норм господарювання», який затверджений наказом № 288 Держстату України від22 листопада 1994 р.

«*Довідник галузей економіки*» — код галузі, назва галузі.

Цей довідник заповнюється відповідно до «Номенклатури статистичної звітності по кредитах банків України», затвердженої постановою Правління НБУ № 80 від 29 березня 1996 р.

«*Довідник видів економічної діяльності*» — код виду економічної діяльності, назва виду економічної діяльності.

Види економічної діяльностівизначаються згідно з «Класифікатором видів економічної діяльності» відповідно до реєстраційної картки суб’єкта господарської діяльності або фізичної особи.

До другої групи файлів належать такі: кредитний договір (KRED\_DOC); пролонгації (PROL); довідник видів кредиту (W\_KRED); довідник цільових призначень кредиту; довідник видів забезпечення кредиту (Z\_KRED); довідник категорій ризику (RISK); довідник причин прострочування; довідник джерел фінансування; довідник цільового призначення кредиту; довідник типів стягнення; довідник статей балансу; довідник статей фінансового звіту; баланс; звіт.

Основним файлом БД даних є файл «Кредитний договір» (KRED\_DOC), який містить такі поля: номер кредитного договору; код валюти; код кредитного інспектора; реєстраційний номер клієнта; кредитний рахунок; рахунок прострочки; дата видачі кредиту; планова дата повернення; початковий строк розміщення (розраховується як різниця між плановою датою повернення і датою видачі кредиту); кількість пролонгацій; дата закриття; тип договору; код форми надання; код виду кредиту; код джерела кредитування; код виду забезпечення; код причини неплатежів; код категорії ризику; код цільового призначення кредиту; сума кредиту; відсоткова ставка; відсоток прострочки; код типу стягнення.

Під час формування кредитного договору використовується ряд файлів нормативно-довідкової інформації (НДІ). Розглянемо основні із них.

*Пролонгація* — номер кредитного договору; номер рахунку пролонгації; процентна ставка пролонгації; дата початку пролонгації; кінцева дата пролонгації.

*«Довідник видів кредиту»*— код виду кредиту; назва виду кредиту. Довідник містить інформацію про види кредитів (строковий, револьверний, у межах кредитної лінії і т. п.).

«*Довідник видів забезпечення кредиту»* — код виду забезпечення; назва виду забезпечення. Основними видами забезпечення є такі: застава майна; гарантія чи поручительство; страховка та ін. При використанні такої форми забезпечення, як застава майна банк укладає з клієнтом договір застави. При забезпеченні кредиту гарантією клієнт подає в банк гарантійний лист, який дає організація, з якою клієнт підписав гарантійний договір. Гарантом можуть виступати будь-які фінансові організації чи банки.

«*Довідник ступенів ризику*» — код ступеня ризику, назва ступеня ризику.

«*Довідник причин прострочування*» — код причини; назва причин прострочування кредиту.

Основними причинами прострочування кредиту можуть бути: порушення договірних умов; складності реалізації продукції; збої в постачанні, збої у виробництві; затримки у розрахунках; фінансові ускладнення та ін.

«*Довідник цільового призначення кредиту*» — код цільового призначення кредиту; назва цільового призначення кредиту.

Коди цільового призначення кредиту, як правило, відповідають стандартно прийнятій системі групування кредитів за призначенням. Наприклад, на поповнення матеріальних запасів і витрат на виробництво, на оплату обладнання, оплату товарів, кредити на потреби приватизації тощо.

«*Довідник типів стягнення*» — код типу стягнення; назва стягнення.

«*Довідник статей балансу*» — код рядка балансу; назва рядка балансу; нормативне значення показника.

«*Довідник статей* *фінансового**звіту*» — код рядка звіту; назва рядка звіту; нормативне значення показника.

**Лекція 9. Автоматизація операцій з цінними паперами.**

## 9.1. Види цінних паперів

В Україні випускаються й знаходяться в обігу такі види цінних паперів (ЦП): акції, казначейські зобов’язання, ощадні сертифікати, векселі, приватизаційні папери, облігації.

*Акції* — це цінні папери, які визначають частку в статутному фонді акціонерного товариства. Акції не мають встановленого терміну обігу. Акції підтверджує членство її власника в акціонерному товаристві та право на участь в управлінні ним. Власник акцій має право на одержання частини прибутку у вигляді дивідендів, а також на участь в розподілі майна при ліквідації акціонерного товариства.

*Казначейські зобов’язання* — це цінні папери на пред’явника, що розміщуються виключно на добровільних засадах серед населення, засвідчують внесення їх власниками грошових коштів до бюджету і дають право на отримання фіксованого доходу.

Рішення про випуск та встановлення продажної вартості казначейських зобов’язань приймається Міністерством фінансів України.

*Ощадний сертифікат* — письмове свідоцтво банку про депонування грошових коштів, яке засвідчує право вкладника на одержання після закінчення встановленого строку депозиту і відсотків по ньому. Іменні сертифікати обігу не підлягають, а їх продаж (відчуження) іншим особам є недійсним.

*Вексель —*цінний папір, який засвідчує боргове зобов’язання векселедавця сплатити після настання певного строку визначену суму грошей власнику векселя (векселедержателю).

Порядок випуску та обігу векселів визначається Кабінетом Міністрів України.

*Облігація* — цінний папір, який свідчить про внесення його власником грошових коштів і підтверджує обов’язок емітента відшкодувати йому номінальну вартість цього ЦП в передбачений строк з оплатою фіксованого відсотка (якщо інше не передбачено умовами випуску).

В Україні випускаються облігації таких видів:

     облігації внутрішніх і республіканських позик;

     облігації підприємств.

Всі цінні папери поділяються на дві групи: боргові документи, що засвідчують виникнення кредиторсько-дебіторських відносин та документи, що підтверджують участь (членство), тобто певні права власності.

Боргові цінні папери не дають права на участь у справах емітента. До цієї категорії належать різні облігації, векселі, казначейські зобов’язання, ощадні сертифікати тощо.

Цінними паперами, що підтверджують участь (членство), є всі види акції та їх похідні опціони, ф’ючерси й інші аналогічні цінні папери.

За формою випуску цінні папери поділяються на такі види:

 цінні папери в документарній формі;

 цінні папери в електронній формі, тобто у вигляді електронних записів на депо-рахунках (бездокументарна форма).

## 9.2. Фондовий ринок та його характеристика

*Фондовий ринок* — це ринок цінних паперів. Він охоплює таку частину кредитного ринку, як ринок боргових інструментів та ринок боргових зобов’язань і повністю ринок інструментів власності, тобто інтегрує та регулює всі операції, пов’язані з випуском і обігом боргових інструментів та інструментів власності.

Ринок цінних паперів складається з первинного і вторинного, біржового і позабіржового.

*Первинний ринок цінних паперів*обслуговуєвипуски (емісії) і початкове розміщення цінних паперів серед інвесторів. Тобто цей ринок охоплює лише найперші акти купівлі та продажу цінних паперів. На цьому етапі організація, що здійснила випуск цінних паперів (емітент), передає цінні папери покупцеві (інвестору), а той в свою чергу сплачує за них певну суму коштів для інвестицій.

*Вторинний ринок цінних паперів* обслуговує обіг та операції з цінними паперами, які були випущені раніше і розміщені на первинному ринку. На вторинному ринку інвестор має можливість перепродати раніше куплені цінні папери з метою отримання прибутку чи розміщення отриманих коштів у більш привабливі активи.

*Біржовий ринок —*це ринок цінних паперів (як правило, вторинний), організований на фондовій біржі. Такий ринок характеризується більш високим рівнем організації і сприяє мобільності капіталу та формуванню реальних ринкових цін.

*Позабіржовий ринок* — це ринок, що охоплює операції з цінними паперами, які виконуються поза біржею. У переважній більшості випадків на цьому ринку відбувається первинне розміщення цінних паперів, а також їх перепродаж.

## 9.3.    Банківські операції з цінними паперами

Банки є активними учасниками фондового ринку. Маючи відповідну ліцензію, комерційні банки можуть виконувати практично всі операції на ринку ЦП, одночасно виконуючи роль емітента і інвестора, фінансового посередника і консультанта. Банки також можуть виконувати функції зберігача цінних паперів, тобто відкривати депозитарні рахунки (депо-рахунки) та приймати на зберігання всі види цінних паперів в документарній (паперовій) та електронній формі.

Всю сукупність операцій, що виконують банки з цінними паперами, можна поділити на: інвестиційні, емісійні, комісійні та сервісні операції.

***Інвестиційні операції*** банки проводять, коли вони виступають в ролі інвестора, купуючи за власні кошти цінні папери інших емітентів. Інвестиційні операції — це балансові активні операції банку. Метою виконання цих операцій є формування власного інвестиційного портфеля. Інвестиційні операції з цінними паперами виконуються для отримання прибутку та для підтримки ліквідності банку. Однак, незважаючи на привабливість і необхідність проведення інвестиційних операцій, переважна більшість операцій банків з цінними паперами проводиться ними не за власні кошти, а на комісійній основі.

***Емісійні операції*** банк виконує як позичальник (емітент), випускаючи власні акції. Емісію власних цінних паперів банк виконує при формуванні статутного капіталу або з метою додаткового його збільшення. Крім того, банки можуть емітувати боргові зобов’язання — векселі, депозитні та ощадні сертифікати і розміщують їх на ринку з метою залучення додаткових коштів для здійснення власної діяльності. Емісійні операції банку — це балансові пасивні операції. До цього класу операцій можна віднести також операції, пов’язані з викупом власних акцій у клієнтів.

***Комісійні*** — це позабалансові операції з цінними паперами, які виконуються за дорученням клієнтів. До комісійних операцій банків відносяться:

 купівля та продаж цінних паперів за дорученням клієнтів (на вторинному ринку);

 оформлення заявок на участь від імені клієнта в аукціонах по первинному розміщенню державних і корпоративних цінних паперів;

 довірче управління цінними паперами клієнта;

 первинне розміщення цінних паперів, емітованих клієнтом;

 консультаційне обслуговування з питань кон’юнктури фондового ринку;

 формування портфеля цінних паперів для клієнта.

***Сервісні операції*** — це за характером теж комісійні операції, але вони виділяються в окрему групу. До цієї групи входять операції по здійсненню банками реєстраційної та депозитарної діяльності та інші сервісні функції по збереженню цінних паперів.

До цих сервісних операцій відносяться:

 зберігання цінних паперів;

 емісія акцій і зберігання глобального сертифікату випуску акцій;

 організація первинного розміщення цінних паперів і реєстрації держателів акцій;

 підготовка і ведення реєстру акціонерів;

 розрахунок, розподіл і виплата дивідендів;

 перереєстрація власників цінних паперів;

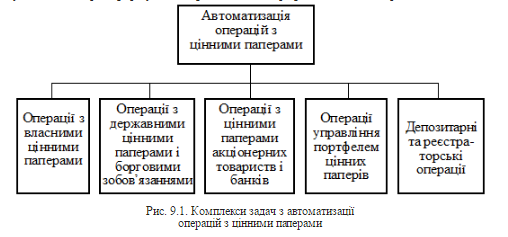
 оформлення сертифікатів на власників цінних паперів;

 облік прав власності на цінні папери та ін.

Виконанням банківських операцій з цінними паперами займається у банку фондовий відділ або відділ цінних паперів. Що стосується автоматизації роботи даних підрозділів, то вони виконуються в межах підсистеми «Управління цінними паперами».

Основні операції, які можуть бути автоматизованими в цій підсистемі, можна згрупувати наступним чином у відповідні комплекси задач (див. рис. 5.1).

Комерційні банки можуть працювати з власними, державними і корпоративними цінними паперами. Для роботи з кожним видом цінних паперів доречно виділяти окремий АРМ. В окремі АРМи виділяються також задачі управління портфелем цінних паперів та депозитарні і реєстраційні операції. Операції управління портфелем полягають у визначенні фінансового стану емітентів, оцінці та прогнозуванні стану ринку цінних паперів, формуванні ефективного портфеля цінних паперів.



Ефективність та обсяги операцій банку з цінними паперами залежать від стану фондового ринку. Розглянемо автоматизацію операції з облігаціями внутрішньої державної позики (ОВДП).

## 9.4. Автоматизація операцій з ОВДП

### 9.4.1. Характеристика облігацій внутрішньої державної позики

Облігації внутрiшньої державної позики (ОВДП) — це визначенi чинним законодавством України державні цiннi папери.

ОВДП — це засіб впровадження неінфляційного механізму ліквідації бюджетного дефіциту, коли емітуються не гроші, а цінні боргові папери, під які залучаються відповідні кошти.

Державні цінні папери — це фінансові інструменти, які випускаються і гарантовано погашаються урядом. Початком створення ринку боргових зобов’язань в Україні можна вважати 1995 рік, коли були емітовані перші випуски облігацій внутрішньої державної позики.

Облігації внутрішньої державної позики випускаються у вигляді строкових боргових зобов’язань як один з інструментів управління державним боргом. Створення ринку ОВДП вирішує такі задачі:

 фінансування бюджету з неінфляційного джерела (залучення фінансових ресурсів з ринку);

 визначення реальної вартості обслуговування державного боргу (відсоткова ставка ОВДП визначається ринком);

 встановлення орієнтира для ринкових ставок за іншими інструментами фінансового та грошового ринків;

 надання в розпорядження НБУ інструмента для проведення грошово-кредитної політики через операції на фондовому ринку;

 організація широкої мережі комерційних посередників, які охоплюють значні верстви інвесторів;

 впровадження сучасної електронної технології торгівлі, розрахунків та депозитарного обліку.

ОВДП обертаються в безпаперовій формі — у вигляді електронних записів на рахунках власників, що різко звужує коло можливих махінацій, виключає можливість крадіжок та підробок.

Депозитарний облік передбачає аналітичний та синтетичний облік цінних паперів. Аналітичний облік ведеться на рахунках цінних паперів, які називаються рахунками-ДЕПО.

ОВДП всіх випусків мають однакову номінальну вартість. Номінальна вартість — це сума основного боргу за облігацією, сплату якої називають погашенням. Ціни на облігації встановлюються у відсотках до номіналу або облігації розміщуються з дисконтом, тобто за ціною, яка нижча від номіналу.

Такий спосіб випуску дає змогу зробити дешевшим обслуговування позики, а також уникнути низки проблем, пов’язаних із зміною облікових ставок.

### 9.4.2. Учасники ринку ОВДП

Емітентом ОВДП є Міністерство фінансів України. Національний банк України є генеральним агентом Міністерства фінансів по обслуговуванню випуску ОВДП. Він гарантує своєчасність погашення випущених облігацій.

Усі операції щодо розміщення та обігу, враховуючи розрахунки та облік власників облігацій, здійснюються через установи НБУ або уповноважені організації — ділери, які визначаються Нацбанком.

Ділером вважається будь-яка юридична особа, яка є інвестиційним інститутом (за діючим законодавством) і має відповідний дозвіл Державної комісії з цінних паперів та фондового ринку, а також ліцензію Національного банку України.

Ділер виконує такі функції:

****виступає посередником при укладанні угод купівлі-продажу на ринку ОВДП;

****веде облік власників облігацій; для цього кожний ділер стає членом депозитарія й організує власний субдепозитарій, забезпечує своєчасність і точність розрахунків за своїми операціями і операціями своїх клієнтів. Ділер також стає членом розрахункової системи за щоденними угодами з облігаціями і забезпечує такий режим функціонування рахунків ділерів, за якого неможливе укладення угод без покриття.

*Інвестором* вважається будь-яка юридична чи фізична особа, яка має право на володіння ОВДП. Для того щоб придбати або продати облігацію, необхідно укласти договір з одним з дилерів, бо тільки ділери мають доступ до торгової системи і право на укладення угод з облігаціями.

В Національному банку створено електронний депозитарій для обліку роботи з ОВДП.

*Депозитарій*забезпечує облік власників облігацій та рух облігацій між ними.

На ринку ОВДП використовується дворівнева система депозитарного обліку, яка складається з центрального депозитарія та мережі субдепозитаріїв.

В центральному депозитарії відкриваються рахунки зареєстрованих ділерів. Існують два типи рахунків: рахунок «А» та рахунок «В». На рахунку «А» враховуються облігації, що належать ділеру, а на рахунку «В» — облігації клієнтів. Рахунки відкриваються окремо за кожним аукціоном, який характеризується власним номером, кодом цінних паперів, терміном обігу облігацій. На рахунку кожного ділера в центральному депозитарії є спеціальний «торговий» субрахунок, призначений для резервування (блокування) облігацій, з якими ділер має намір здійснити операції по їх продажу в даний торговий день.

*Розрахункова система* — це організація, яка має право на ведення розрахункових операцій та уповноважена забезпечувати грошові розрахунки за облігаціями. Кожний ділер відкриває рахунок в розрахунковій системі, через яку він здійснює платежі. Розрахунки за угодами з облігаціями здійснюються протягом одного дня. Залежно від того, має ділер банківську ліцензію чи ні, йому в розрахунковій системі відкривається кореспондентський рахунок або спеціальний рахунок з правом його використання тільки для розрахунків за облігаціями.

Учасники розрахункової системи можуть мати в своїх офісах робочі місця, спеціально обладнані технікою, через яку вони можуть передавати платіжні доручення в систему і отримувати всю звітну документацію.

*Торговельна система* — це організація, уповноважена НБУ забезпечувати технічні засоби і регламент здійснення угод за облігаціями. Система не має права виступати в ролі покупця й продавця або посередника на ринку облігацій.

Операції з ОВДП можуть виконуватись на первинному та вторинному ринках (біржовий та позабіржовий).

Первинний ринок ОВДП проходить у формі аукціонів, які організує НБУ.

На біржовому ринку можуть виконуватись операції купівлі та продажу ОВДП.

На позабіржовому ринку комерційні банки та їх клієнти можуть укладати такі угоди:

****купівлі-продажу;

****«репо» (угоди з продажу облігацій з правом їх зворотнього викупу) ;

****застави під час надання кредиту на міжбанківському ринку;

****рефінансування комерційних банків НБУ під заставу ОВДП (ломбардне кредитування).

Нині на УМВБ (Українська міжбанківська валютна біржа, яка має у своєму складі Фондову секцію) відбувається вторинний обіг облігацій у вигляді електронних торгів. Вторинне розміщення ОВДП також може виконуватись через українську фондову біржу (УФБ).

### 9.4.3. Характеристика автоматизованої системи обслуговування фондового ринку

Забезпечення функціонування первинного та вторинного ринку ОВДП виконується за допомогою розробленої НБУ автоматизованої системи комплексного обслуговування учасників фондового ринку. Ця система об’єднує НБУ, комерційні банки, біржові та позабіржові торговельні майданчики. До складу системи входять такі програмні комплекси: «ЛІГА», «ДЕПО-ОБЛІК»,«ВТОРИН», «ДЕПО-ЗАПИТ».

Програми «ЛІГА», «ВТОРИН» повинні встановлюватись у комерційному банку на єдиному робочому місці, АРМ-КБ «ДЕПО-ОБЛІК» та АРМ «ДЕПО-ЗАПИТ» можуть встановлюватись на іншому або тому ж самому робочому місці.

Загальну схему взаємодії учасників ринку ОВДП представлено на рис. 9.3.

Депозитарний облік на рівні НБУ здійснюється в електронному депозитарії програмним комплексом «ДЕПО-ОБЛІК». Для взаємодії електронного депозитарію НБУАРМ «ДЕПО-ОБЛІК» встановлюються в комерційних банках та на торговельних майданчиках.

АРМ-КБ «ДЕПО-ОБЛІК» не є локальним депозитарієм комерційного банку. Він є інтерфейсним засобом для взаємодії з депозитарієм НБУ і забезпечує отримання комерційним банком інформації про стан депо-рахунків в депозитарії НБУ та роботу банку на біржовому і позабіржовому ринках з відображенням кожної депо-операції.

Для виконання більшості позабіржових операцій необхідна наявність в депозитарії таких двох документів — депо-розпорядження та депо-повідомлення, що надсилаються в депозитарій учасниками угод. Реквізитний склад розпоряджень депонентів та повідомлень в Національній депозитарній системі повинен відповідати міжнародним стандартам ISO 7775 та/або SWIFT Securities Messages, національним стандартам та чинному законодавству.

Програма АРМ «ДЕПО-ОБЛІК» надсилає розпорядження та повідомлення в депозитарій НБУ. Депозитарій при обробцірозпорядження, або повідомлення, що потребує пари (повідомлення або розпорядження), направляє інформацію банку-кореспонденту.

Під час проведення операцій між банком та його клієнтом також необхідно сформувати два документи.

Депо-операція визначається по відношенню до банку, який формує депо-розпорядження. Наприклад, банк А продає цінні папери клієнту банку Б. У такому разі депо-розпорядження на позабіржовий продаж направляє банк А, а депо-повідомлення направляє банк Б.

Усі операції, які потребують наявності пари депо-документів (розпорядження-повідомлення), повинні бути завершені в один робочий день. При невиконанні цієї умови електронний депозитарій виконує розблокування цінних паперів.

Депо-повідомлення не формуються під час виконання операцій блокування-розблокування цінних паперів для формування фонду страхування.

При бажанні провести операцію продажу цінного паперу на торговельному майданчику необхідно вказати в розпорядженні вид цінного паперу, кількість та ідентифікатор майданчика. Депозитарій перевіряє можливість проведення такої операції (наявність на рахунку достатньої кількості цінних паперів), виконує блокування на відповідному торговельному рахунку та направляє інформацію про це на торговельний майданчик. Ця технологія забезпечує виконання принципу «поставки після платежу».

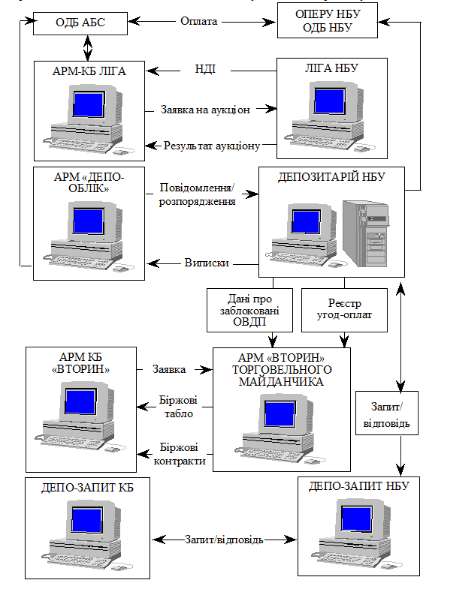


Рис. 9.3. Схема взаємодії учасників ринку ОВДП

#### 9.4.3.1 Характеристика програмного комплексу «ДЕПО-ОБЛІК»

Наприкінці дня депозитарій НБУ передає комерційним банкам виписки про стан їхніх особових депозитарних рахунків. Після отримання файлів-виписок програма АРМ-КБ «ДЕПО-ОБЛІК» автоматично будує всі вихідні форми.

#### 9.4.3.2 Характеристика програмного комплексу «ЛІГА»

Програмний комплекс «ЛІГА» функціонує на двох рівнях: в аукціонному комітеті НБУ та в комерційному банку встановлюється АРМ КБ «ЛІГА». Призначення цього комплексу організація аукціонів з первинного розміщення ОВДП.

Програмний комплекс «ЛІГА» НБУ надсилає електронні повідомлення в банки про проведення аукціонів ОВДП, а також інформує банк та депозитарій НБУ про результати його проведення.

АРМ КБ «ЛІГА», прийнявши та проаналізувавши повідомлення про проведення аукціону, формує й надсилає заявки на участь в аукціоні.

#### 9.4.3.3. Характеристика програмного комплексу «ВТОРИН»

Програмний комплекс «Вторин» встановлюється в КБ та на торговельних майданчиках. Він забезпечує проведення торгів на вторинному ринку ОВДП. Усі заявки купівлі-продажу формуються та модифікуються безпосередньо в комерційному банку і передаються на торговельний майданчик засобами електронної пошти.

АРМ-КБ «Вторин» виконує формування заявок купівлі та продажу по видах цінних паперів за дорученням банку або клієнта, а також забезпечує прийом інформації з торговельних майданчиків про хід та результати торгівлі.

#### 9.4.3.4. Характеристика програмного комплексу  «ДЕПО-ЗАПИТ»

Програмний комплекс «ДЕПО-ЗАПИТ» працює в емісійно-кредитному департаменті НБУ і дає змогу оперативно контролювати стан депозитарного обліку у розрізі регіонів, комерційних банків, видів цінних паперів, депозитарних рахунків.

Програмний комплекс «ДЕПО-ЗАПИТ» складається з АРМ НБУ та АРМ КБ. АРМ КБ дає змогу користувачу сформулювати запит та надіслати його на АРМ НБУ. Можна сформулювати й отримати відповідь:

 про залишки в розрізі депо-рахунків та кодів випуску ОВДП;

 про обіг ОВДП в депозитарії на будь-який момент часу.

АРМ «ДЕПО-ЗАПИТ» НБУ безпосередньо взаємодіє з електронним депозитарієм НБУ.

#### 9.4.3.5. Технологія первинного розміщення ОВДП

Після прийняття рішення про проведення аукціону НБУ надсилає в КБ нормативно-довідкову інформацію (НДІ) про дату проведення аукціону, код цінного паперу, номер аукціону, кількість облігацій, що підлягають розміщенню, номінальну вартість однієї облігації, термін погашення облігації, термін сплати відсотків і суму відсотків, що припадає на одну облігацію, місце та час проведення аукціону.

Аукцiон може проводитись за одним з двох критерiїв на пiдставi введення цiнових умов продажу облiгацiй чи рiвня дохідностi за облiгацiями.

Згiдно з цими критерiями до заявок можуть включатися цiни придбання облiгацiй або рiвень їх дохідностi.

НДІ надходить в комерційні банки і приймається на АРМ-КБ «ЛІГА». Після прийому НДІ на АРМ-КБ «ЛІГА» виконується формування заявок на аукціон.

Заявки поділяються на два види — конкурентні та неконкурентні.

*В конкурентній заявці* вказується цiна або фiксований рiвень дохідностi облігацій.

*В неконкурентній заявці* за ціну придбання облігації береться середньозважена цiна аукцiону або середньозважений рiвень дохідностi.

Заявка включає наступні атрибути: МФО банку, що надіслав заявку, номер аукціону та дату його проведення, назву та код цінного паперу, умови придбання облігацій за конкурентними та неконкурентними пропозиціями. По кожній пропозиції окремо вказується кількість облігацій, що купується, а також тип власника. По конкурентних пропозиціях обов’язково вказується ціна купівлі чи рівень дохідності облігації.

Заявка на придбання ОВДП може надаватись від імені банку за власний рахунок, а також за дорученням і за рахунок іншої особи.

*Середньозважена ціна аукціону*— цiна, яка визначається під час проведення аукцiону на пiдставi цiн за конкурентними заявками за умови, що ці цiни за значенням бiльші або дорiвнюють цiнi вiдсiку.

*Цiна вiдсiку* — цiна, що встановлюється Мiнiстерством фiнансiв України, нижче якої конкурентнi заявки не задовольняються.

*Встановлений рiвень дохідностi* — дохіднiсть облiгацiй, що визначається Мiнiстерством фiнансiв України, вище якої конкурентнi заявки не задовольняються.

Під час проведення аукціону на АРМ НБУ «Ліга» відкриваються заявки банків та визначається список учасників аукціону. Задоволення заявок, поданих на аукціон, залежить від попиту та пропозиції. При проведенні аукціону пріоритет надається конкурентним заявкам, тобто вони задовольняються в першу чергу. Конкурентна заявка може бути не задоволена, якщо її ціна менша за ціну відсіку або дохідність вища за встановлений Міністерством фінансів рівень дохідності.

Неконкурентні заявки можуть задовольнятись не в повному обсязі, а пропорційно їх обсягам в межах залишку від задоволення конкурентних заявок.

Неконкурентні заявки не задовольняються в разі покриття всіх пропозицій конкурентними заявками.

Під час аукціону АРМ-НБУ «ЛІГА» роздруковує аналітичну таблицю можливих результатів, що вміщує варіанти встановлення ціни відсіку (рівня дохідності). Відповідальні особи Міністерства фінансів, що обов’язково беруть участь в аукціоні, знайомляться з цими аналітичними даними та надають письмове доручення НБУ на проведення аукціону, в якому вказується ціна відсіку (рівень дохідності) та середньозважена ціна аукціону (середньозважена дохідність). Після отримання цього доручення в автоматизованому режимі на АРМ НБУ «ЛІГА» проходить розподіл облігацій за заявками і формується зведена відомість розподілу облігацій між покупцями.

**ЗВЕДЕНА ВІДОМІСТЬ**

**розподiлу облiгацiй за їх власниками**

|  |
| --- |
| Код аукціону |

Дата проведення операцій з розміщення облігацій «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ \_\_р.     Код аукціону

|  |
| --- |
| Код |

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | Код |

  (назва облігації та параметри її випуску)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код банку | Назва банку | Кiлькiсть облiгацiй, що придбана (штук) | | | | | | Вартiсть облiгацiй, що  придбана (грн.) | | | |
| Усього | За конкурентними заявками | За неконкурентними заявками | За власний рахунок | За рахунок клієнтів-резидентів | За рахунок клієнтів – нерезидентів | Усього | За власний рахунок | За рахунок клієнтів-резидентів | За рахунок клієнтів-нере-зидентів |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

Ця відомість зберігається в НБУ в складі документів за кожним аукціоном.

Результати аукціонів засобами телекомунікації також надсилаються комерційним банкам. На АРМ КБ «ЛІГА» ці результати роздруковуються у вигляді такої відомості.

##### ***ПРО РЕЗУЛЬТАТИ ПРОВЕДЕНИХ АУКЦІОНІВ***

 «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ \_\_р.

Дані про задоволення заявок за результатами аукціонів з розміщення облігацій.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код ЦП | № аукціону | № заявки | Тип заявки (конкурентна, неконкурентна) | Кількість ОВДП, що придбано (шт.) | | | | Цінові умови придбання (дохідність відсотків) | Суми сплат за придбані ОВДП (грн.) | | | |
| всього | в тому числі за рахунок | | | всього | в тому числі  за рахунок | | |
|  |  |  |  |  | За власний рахунок | За рахунок клієнтів-резидентів | За рахунок клієнтів-нерезиден-тів |  |  | За власний рахунок | За рахунок клієнтів-резидентів | За рахунок клієнтів-нерезидентів |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

Ця відомість є підставою для проведення подальших платежів і розрахунків за облігації.

За правилами комерційний банк зобов’язаний виконати необхідні платежі протягом терміну, зазначеного в результатах аукціону. Після надходження коштів за облігації від комерційних банків НБУ здійснює перерахування коштів до Державного бюджету та зарахування ОВДП на депо-рахунки у Депозитарії.

Інформацію про продані на аукціоні облігації АРМ-НБУ «ЛІГА» направляє в депозитарій Національного банку. Комерційні банки можуть відслідковувати її по виписках депо-рахунків та реєстрах прав власності, які надсилає депозитарій НБУ на АРМ КБ «ДЕПО-ОБЛІК».

#### 9.4.3.6. Технологія вторинного розміщення ОВДП

Обіг облігацій на вторинному ринку здійснюється шляхом укладення угод купівлі-продажу безпосередньо між учасниками ринку. З АРМ КБ «ВТОРИН» ділери подають на торговельні майданчики заявки із зазначенням виду угоди (купівля або продаж), номера аукціону та коду облігацій, кількості, ціни облігацій, коду покупця або продавця та можливості задоволення заявки повністю або частково. Заявки можуть передаватись після того, як через АРМ КБ «ДЕПО-ОБЛІК» було виконано блокування необхідної кількості облігацій в депозитарії НБУ.

Заявки задовольняються в залежності лише від ціни і часу подачі, а розмір заявки на її пріоритет не впливає. Незалежно від часу подачі заявка, яка має більш вигідну ціну, задовольняється раніше, ніж заявка з менш вигідною ціною. При рівних цінах заявка, подана раніше, задовольняється в першу чергу. Якщо заявка задоволена не повністю, то її невиконана частина залишиться в черзі у вигляді окремої заявки.

Будь-яка заявка ділера може бути знята самим ділером, якщо вона до цього часу не була задоволена. При знятті невиконаної заявки кількість облігацій, заблокованих для забезпечення даної заявки, додається до кількості облігацій, які слугують забезпеченням наступних заявок для даного ділера.

За результатами кожного технологічного сеансу АРМ торговельного майданчика «ВТОРИН» направляє в комерційний банк електронне біржове табло, яке містить інформацію про угоди, укладені на торгах в розрізі видів цінних паперів із зазначенням кількісних і вартісних параметрів угод. В табло є блок, який відображає попит і пропозицію, а також прес-реліз, що містить інтегровану інформацію про кількість продавців, покупців, заявок, угод тощо.

Протягом торгового дня комерційний банк має можливість модифікувати відіслані раніше заявки. Причому дозволена модифікація вартісних умов тільки в напрямі зниження цін купівлі та продажу.

Після закінчення торгів торгова система визначає чисте сальдо грошових коштів, які мають бути переведені або зараховані на кореспондентський чи поточний рахунок кожного ділера в розрахунковій системі, а також чисте сальдо облігацій, які повинні бути переведені або зараховані на рахунки «депо» кожного ділера в депозитарії. Остаточна перереєстрація прав власноті на ОВДП виконується лише при надходженні інформації в депозитарій про їх оплату.

По закінченні торгової сесії (робочого дня) комерційний банк отримує файл «Біржових контрактів» та прес-реліз торгів.

#### 9.4.3.7. Погашення ОВДП

Погашення облігацій здійснюється шляхом перерахування НБУ суми коштів, яка дорівнює номінальній вартості облігацій, на рахунки банків-ділерів. Банки-ділери, в свою чергу, мають перерахувати на розрахункові рахунки клієнтів отримані від погашення ОВДП кошти за вирахуванням податку на прибуток.

Доход від ОВДП розраховується за формулою:

*D* = (*Zp* – *Zk*) /*Zk*\*365/*C*, де

*Zp*, – відповідно ціна погашення або продажу облігації;

*Zk* – ціна купівлі облігації; *С* –термін обігу облігацій.

Це загальна формула, яка не враховує податки, комісійні винагороди та інші чинники.

**Лекція 10. АВТОМАТИЗАЦІЯ ФОРМУВАННЯ ЗВІТНОСТІ КОМЕРЦІЙНОГО БАНКУ**

## 10.1. Загальна характеристика звітності

**Банківську звітність можна поділити на такі види:**

 фінансова звітність;

 статистична звітність для складання грошово-кредитної статистики;

 статистична звітність для складання платіжного балансу та міжнародної інвестиційної позиції України.

*До фінансової звітності* належать: бухгалтерський баланс, звіт про прибутки і збитки, звіт про рух грошових коштів та різні додатки, які визначаються потребами користувачів.

*Статистична звітність* для складання грошово-кредитної статистики має такі напрями:

 загальнобанківська статистика;

 монетарна (грошово-кредитна) статистика;

 статистика банківського нагляду;

 статистика операцій з іноземною валютою;

 емісійно-кредитна статистика;

 статистика готівково-грошового обігу.

Особливу роль у державній статистиці відіграє статистика платіжного балансу та міжнародної інвестиційної позиції України, яка є інструментом узагальнюючої оцінки економічного стану країни та ефективності її світогосподарських зв’язків. Функція складання платіжного балансу держави, розроблення методологічної і методичної бази для його аналізу і прогнозування та проведення відповідних розробок покладена на Національний банк України.

Своєчасні й достовірні *статистичні дані* про грошово-кредитну і фінансову діяльність банків *дають змогу*:

 аналізувати стан і перспективи розвитку банківської системи;

 спостерігати за ходом реалізації грошово-кредитної політики держави та прогнозувати розвиток її грошово-кредитного ринку;

 стежити за розвитком валютного ринку та операцій з іноземною валютою;

 здійснювати заходи щодо забезпечення стабільності національної грошової одиниці;

 здійснювати нагляд за діяльністю комерційних банків та інших фінансових небанківських організацій;

 моделювати рішення Національного банку України при виконанні ним регулюючих і наглядових функцій;

 забезпечувати взаємозв’язок грошово-кредитної та банківської статистики з іншими макроекономічними системами даних;

 забезпечувати порівняність з даними міжнародних фінансових і банківських організацій та центральних банків інших країн.

Усім користувачам необхідна інформація, яка допомогла б їм оцінити дійсний фінансовий стан, рентабельність та ризики банку. Також вони потребують інформацію, яка дала б можливість правильно розуміти операції, що здійснюються банком.

Первинною ланкою в системі формування звітності про діяльність банківської системи в Україні є комерційні банки. Для з’ясування суті формування звітності розглянемо структуру плану рахунків та особливості аналітичного обліку в комерційних банках.

## 10.2. Структура плану рахунків комерційного банку

Автоматизація обліку та формування звітності операцій банку повинна забезпечувати два його аспекти: аналітичний по особових рахунках і синтетичний по балансових рахунках. Аналітичний облік повинен забезпечувати отримання детальної інформації про кожного контрагента та кожну банківську операцію.

Синтетичний облік пов’язаний з необхідністю відображення інформації про операції в агрегованому вигляді для формування балансової та фінансової звітності. Синтетичний облік у банках ведеться на рахунках, план яких відповідає загальноприйнятим у міжнародній практиці принципам та стандартам бухгалтерського обліку. План рахунків складається з дев’яти класів:

*Балансові рахунки*

Клас 1. Казначейські та міжбанківські операції.

Клас 2. Операції з клієнтами.

Клас 3. Операції з цінними паперами та іншими активами і зобов’язаннями.

Клас 4. Довгострокові вкладення, основні засоби та нематеріальні активи.

Клас 5. Капітал банку.

*Рахунки доходів та витрат банку*

Клас 6. Доходи.

Клас 7. Витрати.

*Рахунки управлінського обліку*

Клас 8. Управлінський облік.

*Позабалансові рахунки*

Клас 9. Позабалансові рахунки.

*Перший клас* плану рахунків визначає відносини між Національним та комерційними банками, а також між комерційними банками, а саме: операції з готівкою, банківськими металами, кредитами, депозитами та цінними паперами, що рефінансуються НБУ.

*Другий клас* відображає операції з клієнтами, зокрема операції за розрахунками, наданими кредитами та залученими депозитами.

*Третій клас* передбачений для відображення операцій з цінними паперами (окрім цінних паперів, що рефінансуються НБУ, та довгострокових вкладень), а також операцій за іншими розрахунками, зокрема за господарськими операціями банку, операціями з формуванням банківських резервів, субординарного боргу, клірингових та транзитних рахунків, розрахунків між установами одного банку за іноземною валютою, банківськими металами тощо.

*Четвертий клас* відображає довгострокові вкладення установ та операції за основними засобами і нематеріальними активами.

*П’ятий* *клас* визначає капітал банку. Він включає привнесений капітал, нерозподілений прибуток та фонди і резерви, створені за рахунок прибутку.

*Капітал* — це різниця між активами та зобов’язаннями банку. *Прибуток* розглядається як економічний показник діяльності установи, а не як кошти. *Економічний прибуток* — це різниця між доходами і витратами.

*Шостий і сьомий класи* плану рахунків відображають відповідно доходи та витрати банку.

*У восьмому класі* відображаються операції, деталізація яких визначається банком самостійно. Дані восьмого класу не враховуються у фінансових звітах банків.

*Дев’ятий клас* передбачений для ведення обліку позабалансових операцій банку.

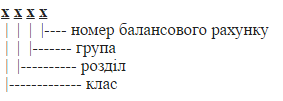
Кожний клас в свою чергу поділений на певну кількість розділів, а розділи — на групи. Згідно з таким розподілом визначаються:

рахунки II порядку (двозначні — розділ) ;

рахунки III порядку (тризначні — група) ;

рахунки IY порядку (чотиризначні — балансовий рахунок).

*Структура номера балансового рахунку* має такий вигляд:

****

Детальний аналітичний облік щодо кожного клієнта та кожної операції забезпечується за допомогою аналітичного обліку, що дає змогу уникнути використання зайвої кількості окремих балансових рахунків.

Між аналітичним та синтетичним обліком існує певна відповідність: кожний особовий (аналітичний) рахунок відкривається за певним балансовим рахунком, залишок по балансовому рахунку дорівнює сумі залишків по особових рахунках.

## 10.3. Особливості ведення та автоматизації  аналітичного обліку

Згідно з методичними вказівками НБУ щодо ведення параметрів аналітичного обліку для організації автоматизації аналітичного обліку вводяться параметри аналітичного обліку, які поділяються на параметри, що характеризують клієнтів (контрагентів) та безпосередньо параметри аналітичного обліку. При цьому кожному контрагенту може відповідати декілька аналітичних рахунків.

*Клієнтами (контрагентами)* банку вважаються ті суб’єкти господарської діяльності або фізичні особи, які мають встановлені банком постійні або тимчасові договірні відносини, що стосуються банківських операцій. Таким чином, контрагентами банку є його клієнти, банки-кореспонденти, банки чи інші особи, з якими укладені угоди на розміщення або залучення коштів тощо.

Всі параметри поділяються на *обов’язкові* та *необов’язкові.* Обов’язкові в свою чергу поділяються на *загальні* та *спеціальні*. *Обов’язкові* — це параметри, які є обов’язковими для заповнення при формуванні інформації про нових клієнтів та при відкритті аналітичного рахунку. Обов’язкові параметри використовуються при формуванні звітності для НБУ.

*Необов’язкові* параметри є рекомендованими для заповнення, і вони можуть використовуватись у банку для внутрішнього обліку та при поданні звітності іншим організаціям.

*Спеціальні* параметри використовуються для певних видів аналітичних рахунків і використовуються для ведення автоматизованого обліку окремих операцій та при формуванні звітності для НБУ.

### 10.3.1. Характеристика параметрів контрагентів

Розглянемо обов’язкові параметри контрагентів банку, їх коди та характеристики.

*Обов’язковими параметрами контрагентів* банку є такі: код контрагента, ідентифікаційний код, резидентність, код країни,ознака податкового номера суб’єкта господарської діяльності, ознака інсайдера, інституційний сектор економіки, форма власності, галузь економіки, види економічної діяльності.

Розглянемо характеристики та коди обов’язкових параметрів.

*Код контрагента* (К010) — містить код контрагента відповідно до реєстра контрагентів, який ведеться банком самостійно.

*Ідентифікаційний код* (К020) — містить код суб’єкта господарської діяльності відповідно до ЄДРПОУ або ідентифікаційний код платника податків для фізичних осіб.

*Резидентність* (К030) — параметр може приймати значення : резидент -1, нерезидент -2. Цей параметр визначається відносно контрагента, а не відносно власника коштів. Таким чином, кореспондентський рахунок в зарубіжному банку і поточний рахунок клієнта-нерезидента будуть мати однакову ознаку — нерезидент.

*Код країни* (К040) — містить тризначний код країни контрагента відповідно до класифікатора країн KL\_K040.

*Ознака* *інсайдера* (К060) — двозначний код, який характеризує клієнта. Iнсайдер — спорiднена щодо комерційного банку особа (фізична або юридична).

*Інституційний сектор економіки* (К070) — визначається для клієнтів-резидентів згідно з «Методичними рекомендаціями щодо класифікації інституційних секторів економіки», затверджених наказом № 172 Мінстату України від 25 липня 1994 р. Формат параметра — 5 цифр.

*Форма власності* (К080) — визначається лише для контрагентів суб’єктів господарської діяльності, згідно з Державним класифікатором України ДК-001-94 «Класифікатор форм власності», який затверджений наказом № 288 Держстату України від 22 лис­топада 1994 р. Параметр може приймати такі значення: приватна власність, колективна власність, державна власність розподіляється на загальнодержавну і комунальну власність, власність інших держав, власність міжнародних організацій та юридичних осіб інших держав. Формат параметра — 2 цифри.

*Галузь економіки* (К090) — визначається лише для контрагентів суб’єктів господарської діяльності, згідно з «Номенклатурою статистичної звітності по кредитах банків України», затвердженої постановою Правління НБУ №80 від 29 березня 1996 р. Формат — 3 цифри. Заповнюється з картки клієнта, причому заповнюється та галузь, яка зазначена першою в картці. Формат параметра — 5 цифр.

*Види економічної діяльності* (К110) — визначаються лише для контрагентів суб’єктів господарської діяльності, згідно з карткою клієнта відповідно до «Класифікатора видів економічної діяльності». У картці може стояти кілька видів діяльності відповідно до реєстраційної картки суб’єкта господарської діяльності. Під час заповнення цього параметра береться з картки той, що проставлений першим. Формат параметра —5 цифр.

Необов’язковим параметром контрагента є :

*Ознака податкового номера суб’єкта господарської діяльності —* цей параметр необхідно заповнювати по мірі присвоєння податкових номерів клієнтам Державною податковою інспекцією. Він має таку структуру:

XXXXXXX NN MM K, де

XXXXXXX — ідентифікаційний код суб’єкта господарської діяльності;

NN — код області;

MM — код району;

К — ключовий розряд.

### 10.3.2. Характеристика параметрів аналітичного обліку

*Загальними обов’язковими параметрами аналітичного рахунку* є такі: номер аналітичного рахунку; номер балансового рахунку; код валюти; характеристика контрагента; код контрагента; характеристика аналітичного рахунку.

*Номер аналітичного рахунку* (R010) *—* це ідентифікатор рахунку, який проставляється у банківських документах. Номер включає до 14 цифр, перші п’ять з яких регламентовані, інші формуються банком самостійно, виходячи з його потреб.

Номер балансового рахунку (R020) — чотиризначний номер рахунку з довідника плану рахунків комерційного банку КL\_R020.

Код валюти (R030) — містить тризначний код валюти згідно з класифікатором валют КL\_R030.Цей параметр може включатись як складова номера рахунку.

*Код контрагента* — цей параметр є посиланням на довідник контрагентів. Він необхідний для встановлення інформаційного зв’язку і містить код власника рахунку.

Х*арактеристика аналітичного рахунку* (R050) вказує на належність рахунку до класу балансу і містить його характеристику. Наприклад, може приймати такі значення: 03- актив/пасив, 11 — актив, 12 — актив (контрактив), …. , 62 — доходи (пасив) і т.п.

Деякі обов’язкові параметри входять до складу коду аналітичного рахунку.

Розглянемо його структуру.

*Код аналітичних рахунків має таку структуру:*

ВВВВ К С NN . EEEEEE, де

 ВВВВ — номер балансового рахунку . Довжина номера рахунку не є фіксованою, вона може встановлюватись у діапазоні 8-14 знаків.

 К — контрольний розряд;

 С — характеристика контрагента;

 NN — порядковий номер аналітичного рахунку;

 EEEEEE — код клієнта може вміщувати до 6 знаків.

Параметри NN та EEEEEE визначаються банками самостійно.

*Спеціальні обов’язкові параметри аналітичного рахунку такі:* параметр нарахування відсотків, параметри для кредитних та депозитних рахунків, параметр для рахунків цінних паперів.

Параметр *нарахування процентів* (S010) вказується для рахунків, по яких виконується нарахування відсотків, зокрема для: позичкових, депозитних, рахунків цінних паперів, кореспондентських та розрахункових рахунків. Параметр S012 характеризує відсоткову ставку.

Для кредитних рахунків задаються такі параметри: вид кредиту (S020), вид забезпечення (S030), дата видачі кредиту (S040), дата повернення кредиту (S050), кількість пролонгацій (S070), категорія ризику (S080), код строку кредитних та депозитних рахунків (S180), код строковості (S181), код строку пролонгації та прострочки (S190), код джерела кредитування (S200).

Для рахунків цінних паперів задаються такі параметри: емітент (S110), місце емісії (S120), вид цінних паперів (S130), дата погашення (S140), ознака, котуються чи ні на біржі (S150), входять чи ні для обчислення бази при оподаткуванні (S160).

Для рахунків «Кошти в розрахунках» — код розрахунку (S170).

Для депозитних рахунків параметр вміщує такі характеристики: дата розміщення (залучення) (S090); дата повернення коштів (S100); початковий строк розміщення (S060).

*Необов’язкові параметри аналітичного рахунку*: вид рахунку, ліміт овердрафту.

Параметр *вид рахунку* характеризує вид рахунку відповідно до інструкції № 121 НБУ «Про порядок відкриття розрахункових, поточних та бюджетних рахунків в установах банків» від 27.06.96 р.

Параметр *ліміт овердрафту* вказує на поточний ліміт овердрафту, який дозволено для рахунку. Він може приймати значення величини ліміту.

Параметри аналітичного обліку кодуються. Їм присвоюється чотиризначний символьний код такого формату:

LNNN, де L та NNN можуть приймати такі значення:

L — [K, R, S, D, B, T, F], де:

K — позначення для параметрiв клiєнтiв;

R — позначення для загальних параметрiв рахункiв;

S — позначення для спеціальних параметрiв рахункiв;

D — позначення для параметрiв документів;

В — позначення для додаткових параметрів банків-нерезидентів;

T — позначення для iнших параметрiв, якi використовуються при формуванні економiчного показника;

F — параметри, які використовуються у формулах обчислення показників і вказують на підмножину рахунків, які включаються до показника.

### 10.3.3. Параметри для опису  характеристик показників та формул їх обчислення

Крім параметрів аналітичного обліку та контрагентів, є ряд параметрів, які використовуються для опису економічних показників звітності та формул їх обчислення.

Розглянемо групу параметрів, які характеризують вид-показник, вказуючи, що треба враховувати при його обчисленні. Коди цих параметрів починаються з літери Т, вони подані в таблиці 10.1.

#### Таблиця 10.1

| Код параметра | Назва параметра |
| --- | --- |
| Т010 | Дебетовий залишок в національній валюті |
| Т020 | Кредитовий залишок в національній валюті |
| Т030 | Кредити, кошти, надані в національній валюті |
| Т040 | Кредити, кошти, отримані в національній валюті |
| Т050 | Дебетові обороти в національній валюті |
| Т055 | Коригуючі дебетові обороти в національній валюті |
| Т060 | Кредитові обороти в національній валюті |
| Т065 | Коригуючі кредитові обороти в національній валюті |
| Т070 | Сума в національній валюті |
| Т011 | Дебетовий залишок в іноземній валюті |
| Т021 | Кредитовий залишок в іноземній валюті |
| Т051 | Дебетові обороти в іноземній валюті |
| Т056 | Коригуючі дебетові обороти в іноземній валюті |
| Т061 | Кредитові обороти в іноземній валюті |
| Т066 | Коригуючі кредитові обороти в іноземній валюті |
| Т070 | Сума в іноземній валюті |
| Т080 | Кількість (угод, клієнтів або рахунків та ін.) |
| Т090 | Середньозважена відсоткова ставка |

Коди параметрів, які використовуються в формулах для визначення підмножини рахунків, починаються з літери F.

F\_01 — поле у файлі KL\_R020, яке визначає перелік балансових рахунків, які необхідно включити у файли звітності 01 та 02. Якщо поле приймає значення 1, то рахунок включається як окремий показник.

F\_02 — поле у файлі KL\_R020, яке визначає перелік балансових рахунків, які необхідно включити у файли звітності 06 та 14. Якщо поле приймає значення 1, то рахунок включається як окремий показник.

Параметри F\_07, F\_08, F\_16 та F\_17 характеризують поле у файлі KL\_R020, яке визначає перелік балансових рахунків, які необхідно включити відповідно у наступні файли звітності 07, 08, 16 та 17. Якщо поле приймає значення 1, то рахунок включається як окремий показник.

Параметри F\_12, F\_13 характеризують поле у файлі KL\_D010, яке визначає перелік касових символів, які необхідно включити відповідно у наступні файли звітності 12 та 13. Якщо поле набуває значення 1, то символ включається як окремий показник.

## 10.4. Порядок формування економічних показників звітності

НБУ запровадив нову технологію надання звітності, яка базується на економічних показниках. Згідно з цією технологією звітна інформація надається електронною поштою у вигляді файлів з певним набором значень економічних показників. Надані комерційними банками економічні показники звітності зберігаються в спеціальному сховищі даних, яке має назву електронного репозитарію.

Файли, розроблені на базі показників форм звітності, згруповані за періодичністю надання та економічною суттю показників. Кожний файл має двозначний цифровий ідентифікатор, у якому задіяні номери від 01 до 55. Вихідні документи за формами звітності формуватимуться із значень економічних показників того чи іншого файлу.

Звітність складається в одиницях, встановлених для кожної форми окремо, з округленням сум до одиниць таким чином, щоб були збережені правильність підсумків та повний набір даних статистичних звітів і балансу.

Звітність подається за певними схемами, коди яких містяться в довіднику кодів схем KOD\_A011. *Код схеми* вказує на те, хто і кому подає звітність, та на ступінь її консолідації. Наприклад, якщо звітність подається філією, то код схеми знаходиться в межах 01-04 залежно від того, кому подається звіт (01-обласній дирекції банку, 02-головному банку як юридичній особі, 03-обласному управлінню НБУ, 04-ЦРП НБУ).

Звітність формується у вигляді файлів, які містять певні економічні показники. Кожний файл складається з однорідних показників. Перелік показників в розрізі кожного звітного файлу подається у довіднику показників EK\_POK\_1, структуру якого наведено в таблиці 10.3. (див. пункт 10.6).

Кожний параметр, який використовується для опису економічних показників, зберігається у відповідному довіднику, який характеризує розріз подання показника. Кодові позначення розрізів та довідники, які використовуються під час формування звітності, наведено в таблиці 10.2.

Економічний показник може бути сумою, кількістю, відсотковою ставкою i т. iн. Для опису показників звітності НБУ булорозроблено штучну мову опису показників, яка заснована на кодових позначеннях параметрів. Кожний показник має свою формулу розрахунку.

Формула розрахунку економiчного показника може включати суму за окремим балансовим рахунком (можливо, за iншимпараметром) чи певну її підмножину або алгебраїчну суму групи рахункiв.

Загальний опис формули розрахунку економiчного показника складається з таких п’яти наступних частин:

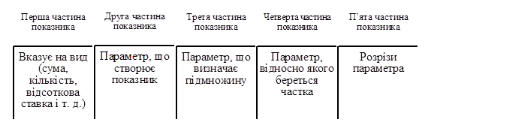


Рис. 10.4.1. Структура формули розрахунку показника

*Перша частина* розрахунку показника містить параметр, що починається на літеру Т (див. табл. 10.1).

Ця частина опису зберігається в полі PRM1 довiдника показників EK\_POK\_1.

*Друга частина* визначає параметр показника та вказує на те, чи описується показник одним параметром чи їх групою. Якщо друга частина опису показника складається тільки із значення параметра, то вказується цей параметр. Для визначення, чи параметр підлягає передачі повністю чи лише його певна підмножина, необхідно дивитись третю частину опису параметра.

Якщо ж в показник входить група значень параметра, то пiсля параметра в дужках йде значення параметра або перелiк значень параметра, якi входять до пiдрахунку показника. Перед значенням параметра може бути один із знаків: [>], [<], [>=], [<=], [#] (більше, менше, більше-дорiвнює, менше-дорiвнює, не дорiвнює). Знак [=] (дорiвнює) опускається.

Перелiк значень параметра може роздiлятися одним iз знакiв [,],[:]. При цьому [:] означає, що до пiдрахунку показника включаються значення параметра з початкового до кiнцевого включно. Ця частина опису розрахунку зберігається в полі PRM2 до­вiдника показників EK\_POK\_1.

*Приклади:* R020(1500:1505,1521,1523)

R020(>=2000,<2200)

R020(2200).

*Третя частина* опису показника має місце тоді, коли друга частина опису складається лише з параметра без переліку значень.

Якщо у файл для передачі входить вся множина значень параметра окремими економічними показниками, то третя частина опису не заповнюється (поле PRM3 — буде пусте).

Коли у файл для передачi входить пiдмножина значень параметра окремими економiчними показниками, опис складається з параметра, який визначає цю пiдмножину (F\_01,F\_06,F\_07,F\_08 для параметра R020, F\_12, F\_13 для параметра D010), а далi в дужках йде значення, при якому необхiдно включати значення параметра, вказаного в другій частині опису, для передачi окремим економiчним показником. Перед значенням параметра може бути один із знаків: [>], [<], [>=], [<=], [#]. Знак [=] опускається.

Наприклад, F\_01(1) F\_01(>2) F\_01(#1). Цей параметр є полем довідника, у якому зберігаються можливі значення параметра, який створює економічний показник. Всі записи із значенням 1 або >2 або #1 відповідно в полі F\_01 визначають цю підмножину.

Ця частина опису зберігається в полі PRM3 довiдника показників EK\_POK\_1.

*Четверта частина* вказує на розрізи параметра, якщо при формуванні показника вони використовуються не всі. В такому разі четверта частина опису складається з найменування параметра, за яким в дужках знаходиться перелiк можливих конкретних його значень. Перед значенням параметра може бути один із знаків: [>], [<], [>=], [<=], [#]. Перелiк значень параметра може роздiлятисяодним iз знакiв [,], [:]. Перелiк параметрiв з конкретними значеннями роздiлятиметься знаком [,]. Наприклад, необхідно подати дані по рахунках тільки за кодами валюти 840 та 980 і тільки за резидентами, тоді опис буде мати вигляд: R030(840,980),K030(1).

Ця частина опису зберігається в полі PRM4 довiдника показників EK\_POK\_1.

*П’ята частина* опису пiдрахунку показника містить перелiк розрiзiв, в яких необхiдно подавати показник (розрiз кодiв валют, форм власностi, секторiв економiки, галузей економiки, груп валют, груп країн, кодiв строкiв, строковостi, резидентностi тощо). Перелiк розрiзiв роздiляється знаком [,]. Наприклад, якщо економiчний показник надається в розрiзi резидентностi, то його загальна сума буде подiлена на двi частини, одна з яких вiдноситься до резидентiв, друга — до нерезидентiв. У файлi для передачiцi двi частини показника будуть подаватися двома записами. Якщо до розрiзу резидентностi ще додати розрiз груп валют, то кожна з цих двох частин показника може подiлитися ще на три частини по групах валют. У файлi для передачi може бути шiстьзаписiв для цих частин показника. За кожним наступним розрiзом розподiл економiчного показника буде аналогiчним. Ця частина опису зберігається в полі PRM5 довiдника показників EK\_POK\_1.

**Приклад 1.** Для файла з кодом 03, коду показника 1310KGR — щоденна сума за мiжбанкiвськими наданими кредитами в розрiзi кодiв строкiв, груп валют та резидентностi, формула пiдрахунку має вигляд: T030 R020(1521,1523,1524,1525) S180,R031, K030, де:

перша частина опису — T030 — суми, поданi в гривневому еквiвалентi

друга частина опису — R020(1521,1523,1524,1525) — показник є алгебраїчною сумою рахункiв, зазначених в дужках;

п’ята частина опису — S180,R031,K030 — розріз кодів строків, груп валют та резидентності.

Таблиця кодів розрізів у кодах показників та довідників, які використовуються при описі економічних показників, має такий вигляд.

#### Таблиця 10.2

| Код А016 | Зміст розрізу | Довідник | Поле |
| --- | --- | --- | --- |
| ВBBB | Балансовий рахунок | KL\_R020 | R020 |
| VVV | Код валюти | KL\_R030 | R030 |
| G | Група валюти | KL\_R031 | R031 |
| Z | Параметр R011 | KL\_R011 | R011 |
| Y | Група країн | KL\_К041 | К041 |
| S | Сектор економіки | KL\_К071 | К071 |
| F | Форма власності 1-го рівня | KL\_К081 | К081 |
| EE | Код галузі економіки 2-го рівня | KL\_К091 | К091 |
| A | Код галузі економіки 1-го рівня | KL\_К092 | К092 |
| K | Код строку | KL\_S180 | S180 |
| X | Строковість | KL\_S181 | S181 |
| R | Резидентність | KL\_К030 | К030 |
| I | Код строку прострочки (пролонгації) | KL\_S190 | S190 |
| W | Місце емісії | KL\_К041 | S120 |
| P | Параметр R013 | KL\_R013 | R013 |
| J | Ознака бюджетної організації | KL\_К130 | К130 |
| NNN | Символ бюджетної класифікації доходів | KL\_S230 | S230 |
| OOO | Символ міністерств і відомств | KL\_К120 | К120 |
| CC | Символ касових оборотів | KL\_D010 | D010 |
| LL | Розділ видів економічної діяльності | KL\_К111 | К111 |
| HHHHHHHHHH | Код банку- нерезидента | RC\_BNK | B010 |
| MMM | Код країни | KL\_К040 | К040 |
| T | Категорія ризику | KL\_S080 | S080 |
| Q | Джерело кредитування | KL\_S200 | S200 |
| UUU | Код ювілейної монети (для НБУ) | KL\_Z070 | Z070 |

## 10.5. Структура файлів звітності

Всі файли звітності мають однакову структуру:

1- рядок — службовий;

2- рядок — заголовковий;

3- рядок — підзаголовок для 1-го розрізу файла;

4+n — інформаційний рядок 1-го розрізу (n — загальна кількість рядків 1-го розрізу);

i-й рядок підзаголовок для k-го розрізу файла;

(i+1) –й … (i+m)-й — інформаційні рядки k-го розрізу файла.

Кожний рядок файла звітності ідентифікується за певними правилами. Розглянемо структуру інформаційних рядків на прикладі файлів 01 та 02.

*Структура* *iнформацiйних* *рядкiв* *файла* *звітності*:

NNNNNNNN=XXXXXXXXXX,

де: NNNNNNNN — код показника, який може приймати значення поля KOD\_EKPOK довiдника економiчних показникiвEK\_POK\_1 (див. табл. 7.2) в межах коду файла. Код показника в межах одного файла відносно даних філії або області має унікальне значення. Довжина коду показника для всіх кодів файлів може бути різною. В межах одного коду файла довжина всіх кодів показників однакова.

XXXXXXXXXX — значення показника. Довжина значення показника вказана в полях WIDTH та DEC довiдника економiчнихпоказникiв EK\_POK\_1.

*Опис показників відносно коду файлів.*

Код файла 01 — щоденнi данi про залишки на балансових рахунках в розрiзi кодiв валют та резидентностi.

Код одиницi вимiру даних — 21 (копiйки, сота частина одиниць валюти).

З даних файла 01 створюється форма 1Д-КБ.

Формат коду показника для файла 01 — DDBBBBVVVR, де:

DD — характеризує вид показника, який зберігається в полі PRM1 довідника показників EK\_POK\_1 і може приймати значення:

10 — дебетовий залишок в нацвалюті (гривневий еквiвалент);

11 — дебетовий залишок в інвалюті;

20 — кредитовий залишок в нацвалюті (гривневий еквiвалент);

21 — кредитовий залишок в інвалюті.

Сегмент, який визначає розрiзи надання iнформацiї:

BBBB — балансовий рахунок, який може приймати значення поля R020 довiдника плану рахункiв KL\_R020;

VVV — код валюти (поле R030 довiдника валют KL\_R030);

R — резидентність (поле K030 довiдника резидентності KL\_K030 в табл.7.11).

У довіднику EK\_POK\_1 для файлу 01 будуть наступнi коди показникiв:

10BBBBVVVR — для рахункiв з дебетовим залишком в нацвалюті;

опис: T010 R020 F\_01(1) R030,K030.

11BBBBVVVR — для рахункiв з дебетовим залишком в інвалюті;

опис: T011 R020 F\_01(1) R030,K030.

20BBBBVVVR — для рахункiв з кредитовим залишком в нацвалюті;

опис: T020 R020 F\_01(1) R030,K030.

21BBBBVVVR — для рахункiв з кредитовим залишком в інвалюті.

опис: T021 R020 F\_01(1) R030,K030.

Код файла 02**—**щомiсячнi дані про обороти та залишки на балансових рахунках в розрiзi кодiв валют та груп країн.

Код одиницi вимiру даних — 21 (копiйки, сота частка одиниць валюти).

З даних файла 02 створюється форма 1-КБ.

Формат коду показника для файла 02 –> DDBBBBVVVY, де

DD — характеризує вид показника, який зберігається в полі PRM1 довідника показників EK\_POK\_1 і може приймати значення:

10 — дебетовий залишок в нацвалюті (гривневий еквiвалент);

11 — дебетовий залишок в інвалюті;

20 — кредитовий залишок в нацвалюті (гривневий еквiва­лент);

21 — кредитовий залишок в інвалюті;

50 — дебетові обороти в нацвалюті (гривневий еквiвалент);

51 — дебетові обороти в інвалюті;

60 — кредитові обороти в нацвалюті (гривневий еквiвалент);

61 — кредитові обороти в інвалюті.

Сегмент, який визначає розрiзи надання iнформацiї:

BBBB — балансовий рахунок, який може приймати значення поля R020 довiдника плану рахункiв KL\_R020.

Сегмент, який визначає розрiзи надання iнформацiї:

VVV — код валюти (поле R030 довiдника KL\_R030);

Y — розподіл клієнтів за групами країн ( поле K041 довiдника груп країн KL\_K041).

У довіднику EK\_POK\_1 для файла 02 будуть такі коди показникiв:

10BBBBVVVY — для рахункiв з дебетовим залишком в нацвалюті;

опис: T010 R020 F\_01(1) R030,K041.

11BBBBVVVY — для рахункiв з дебетовим залишком в інвалюті;

опис: T011 R020 F\_01(1) R030,K041.

20BBBBVVVY — для рахункiв з кредитовим залишком в нацвалюті;

опис: T020 R020 F\_01(1) R030,K041.

21BBBBVVVY — для рахункiв з кредитовим залишком в інвалюті;

опис: T021 R020 F\_01(1) R030,K041.

50BBBBVVVY — для рахункiв з дебетовим оборотом в нацвалюті;

опис: T050 R020 F\_01(1) R030,K041.

51BBBBVVVY — для рахункiв з дебетовим оборотом в інвалюті;

опис: T051 R020 F\_01(1) R030,K041.

60BBBBVVVY — для рахункiв з кредитовим оборотом в нацвалюті;

опис: T060 R020 F\_01(1) R030,K041.

61BBBBVVVY — для рахункiв з кредитовим оборотом в інвалюті;

опис: T061 R020 F\_01(1) R030,K041.

## 10.6. Інформаційна модель формування файлів звітності 01 та 02

При формуванні файла 01 — «Щоденнi данi про залишки на балансових рахунках в розрiзi кодiв валют та резидентностi» та файла 02**—**«Щомiсячнi дані про обороти та залишки на балансових рахунках в розрiзi кодiв валют та груп країн» використовуються файли, які надає комерційному банку НБУ, та файли, що формуються в АБС, зокрема в підсистемі ОДБ. Схему інформаційної моделі формування файлів звітності 01 та 02 наведено на рис. 10.2.

На основі файла 01, який містить дані щоденної звітності про залишки на рахунках, можна сформувати такі звітні форми: «Баланс комерцiйного банку» (1Д-КБ), «Довiдка про залученi кошти та їх залишки для визначення розмiру обов’язкових резер­вiв» (381), «Звiт про вiдкритi валютнi позицiї на кiнець опера­цiйного дня» (540), «Розшифровка рахункiв за видами валют» (550Д). На основі даних файла 02, який містить дані щомісячної звітності про обороти та залишки на рахунках, можна сформувати такі звітні форми: «Баланс комерцiйного банку» (1\_КБ); «Оборотно-сальдовий баланс комерцiйного банку» (10-КБ); «Оборотно-сальдовий баланс фiлiй українських комерцiйних банкiв, що розташованi за межами України» (10-Н); «Балансовий звiт комерцiйного банку» (11); «Обороти за мiсяць за рахунками в iноземних валютах» (550).

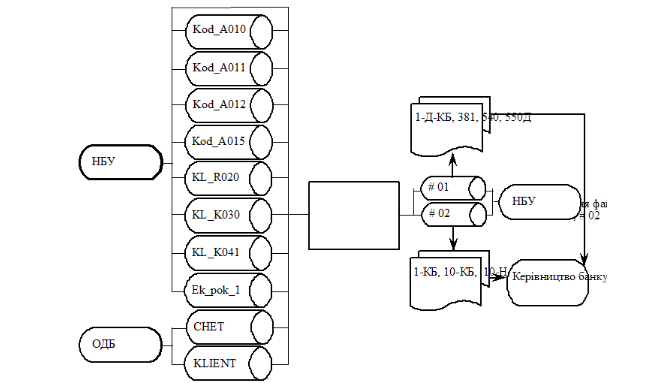


Рис. 10.2. Схема інформаційної моделі формування файлів звітності # 01,

 Структуру основних файлів, які задіяні в цьому процесі, наведено відповідно в таблицях 10.3–10.13.

#### Таблиця 10.3

**# 02СТРУКТУРА ФАЙЛА «ДОВІДНИК ПЕРВИННИХЕКОНОМІЧНИХ ПОКАЗНИКІВ» (EK\_POK\_1)**

| Назва поля | Ідентифікатор | Формат |
| --- | --- | --- |
| Код файла | A010 | С(2) |
| Код показника | Kod\_ekpok | С(24) |
| Назва показника | Name\_ ekpok | С(N6) |
| Чим є показник (сума, кількість, %% ставка) | Prm1 | С(10) |
| Параметр, який створює показник | Prm2 | С(N6) |
| Параметр, який визначає підмножину Prm2 | Prm3 | С(24) |
| Параметр, відносно якого береться частка Prm2 | Prm4 | С(200) |
| Розрізи показника | Prm5 | С(N6) |
| Тип даних показника | Typ | С(1) |
| Довжина даних показника | Width | N(3) |
| Точність даних показника | Dec | N(1) |
| Форма — джерело даних показника | Forma | С(24) |
| Дата створення показника | Data\_o | D(8) |
| Реквізити особи, відповідальної за показник | Fio\_tel | С(51) |
| Ознака формування показника з даних аналітичного обліку | Priznak | С(1) |
| Ким надається | Rem | С(3) |
| Дата закриття показника | Data\_c | D(8) |
| Дата змін показника | Data\_m | D(8) |

##### СТРУКТУРА ФАЙЛА « ДОВІДНИК КОДІВ ФАЙЛІВ» KOD\_A010

#### Таблиця 10.4

| Назва поля | Ідентифікатор | Формат |
| --- | --- | --- |
| Код файла | A010 | С(2) |
| Код схеми надання | A011 | С(5) |
| Код розрізу розташування | A012 | С(1) |
| Код періоду | A013 | С(1) |
| Розріз консолідації | A014 | С(1) |
| Одиниця виміру | A015 | С(2) |
| Тип файла передачі | A017 | С(1) |
| Назва файла | NAME\_F | С(N6) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК КОДІВ СХЕМ  
НАДАННЯ ДАНИХ» (KOD\_A011)**

#### Таблиця 10.5

|  |  |  |
| --- | --- | --- |
| Назва поля | Ідентифікатор | Формат |
| Код схеми надання | A011 | С(2) |
| Тип файла передачі | A017 | С(1) |
| Код схеми відповіді | F\_FROM | С(1) |
| Назва | NAME\_S | С(48) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК РОЗРІЗІВ  
РЕЗИДЕНТНОСТІ» (KOD\_A012)**

#### Таблиця 10.6

|  |  |  |
| --- | --- | --- |
| Назва поля | Ідентифікатор | Формат |
| Код розрізу резидентності | A012 | С(1) |
| Назва | NAME | С(48) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК КОДІВ  
ОДИНИЦЬ ВИМІРУ» (KOD\_A015)**

#### Таблиця 10.7

|  |  |  |
| --- | --- | --- |
| Назва поля | Ідентифікатор | Формат |
| Код одиниці виміру | A015 | С(2) |
| Назва одиниці виміру | NAME\_OD | С(30) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК БАНКІВ» (BANK)**

#### Таблиця 10.8

| Назва поля | Ідентифікатор | Формат |
| --- | --- | --- |
| Код МФО | MFO | N(6) |
| Код банку | KB | N(4) |
| Код області | KU | N(3) |
| Тип банку | PRB | N(1) |
| Коротка назва банку | KNB | С(27) |
| Ідентифікатор банку | NCKS | С(4) |
| Електронна адреса банку | HCKS | С(4) |
| Дата відкриття банку | DATA\_O | D(8) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК РАХУНКІВ» (KL\_R020)**

#### Таблиця 10.9

|  |  |  |
| --- | --- | --- |
| Назва поля | Ідентифікатор | Формат |
| Тип банку | TIP\_BANK | С(3) |
| Клас рахунків | KL | N(1) |
| Розділ | RAZD | N(2) |
| Група балансових рахунків | GR | N(3) |
| Ознака (класу, розділу, групи) | PR | С(1) |
| Номер балансового рахунку 4-го порядку | R020 | N(4) |
| Тип балансового рахунку | T020 | N(1) |
| Характеристика балансового рахунку | R050 | С(2) |
| Код резидентності | K030 | N(1) |
| Код групи валют | R031 | N(1) |
| Строковість кредиту | S181 | N(1) |
| Галузь економіки 2-го рівня | K0N1 | N(1) |
| Перелік балансових рахунків для файла «#01» | F\_01 | N(1) |
| Назва балансового рахунку | NAME\_BR | С(1N2) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК ВАЛЮТ» ( KL\_R030)**

#### Таблиця 10.10

| Назва поля | Ідентифікатор | Формат |
| --- | --- | --- |
| Код валюти | R030 | N(3) |
| Код країни | K040 | N(3) |
| Літерний код валюти | A3 | С(3) |
| Код групи валют | R031 | N(1) |
| Код групи валют за групою країн | R032 | N(1) |
| Група конвертації | GR | N(1) |
| Літерний код країни(старий) | KOD\_LIT | С(3) |
| Код валюти (старий) | KOD\_NUM | С(3) |
| Назва показника | TXT | С(27) |
| Номінал валюти | NOMIN | N(5) |
| Назва валюти | NAIM | С(27) |

##### СТРУКТУРА ФАЙЛА «ДОВІДНИК РЕЗИДЕНТНОСТІ» KL\_K030

#### Таблиця 10.11

|  |  |  |
| --- | --- | --- |
| Назва поля | Ідентифікатор | Формат |
| Код резидентності | K030 | N(1) |
| Назва | NAME | С(48) |

**СТРУКТУРА ФАЙЛА «ДОВІДНИК ГРУП КРАЇН» (KL\_K041)**

#### Таблиця 10.12

|  |  |  |
| --- | --- | --- |
| Назва поля | Ідентифікатор | Формат |
| Код групи країн | K041 | N(1) |
| Код групи валют за групою країн | R032 | N(1) |
| Місце емісії | S120 | N(1) |
| Код резидентності | K030 | N(1) |
| Назва групи країн | NAME\_GR\_K | С(48) |

**СТРУКТУРА ФАЙЛА «СТАН РАХУНКУ» ( SOST\_CHET)**

#### Таблиця 10.13

| Назва поля | Ідентифікатор | Формат |
| --- | --- | --- |
| Номер аналітичного рахунку | N\_R | N(14) |
| Код резидентності | K030 | N(1) |
| Код групи валют | R\_031 | N(3) |
| Вхідний залишок по дебету | VH\_D | N(17).N(2) |
| Вхідний залишок по кредиту | VH\_K | N(17).N(2) |
| Обороти по дебету | O\_D | N(17).N(2) |
| Обороти по кредиту | O\_K | N(17).N(2) |
| Вихідний залишок по дебету | V\_D | N(17).N(2) |
| Вихідний залишок по кредиту | V\_K | N(17).N(2) |

### 

**Лекція 11. ТЕХНОЛОГІЯ ЗАХИСТУ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ**

## 11.1. Файли інтерфейсу між ОДБ та АРМ-3

Всі файли, якими обмінюється комерційний банк з СЕП, умов­но можна поділити на такі групи:

 пакети платіжних документів:

vA — файл початкових платежів від банку в РРП;

vB — файл зворотних платежів на банк від банку-отри­мувача;

 повідомлення між АРМ про завершення етапів обробки:

vK — кінець сеансу АРМ-2, звіт для АРМ-3 про зміну його   коррахунку;

vZ — звіт про кінець дня АРМ-3;

vV — кінець дня АРМ-2, зведений документ для АРМ-3 про змінення його коррахунку;

 файли-квитанції на пакети платіжних документів та інші файли:

vT — квитанція на vA;

vS — квитанція на vB. Всі перераховані квитанції видаються системою, тобто відповідним АРМ-ом;

 технологічні файли:

vU — завдання на коректуру списку учасників;

M — файл бізнес -правил.

 Файли нормативно-довідкової інформації:

 S\_VAL — довідник валют;

 S\_ER — довідник кодів помилок;

 S\_UCH — довідник банків учасників СЕП;

 S\_NR — довідник призначень платежу;

 M.UCH — файл інвалютних коррахунків;

 U\_SNG — довідник субкорреспондентів шлюзових банків.

Схему обміну даними між банком та СЕП наведено на рис. 11.1.

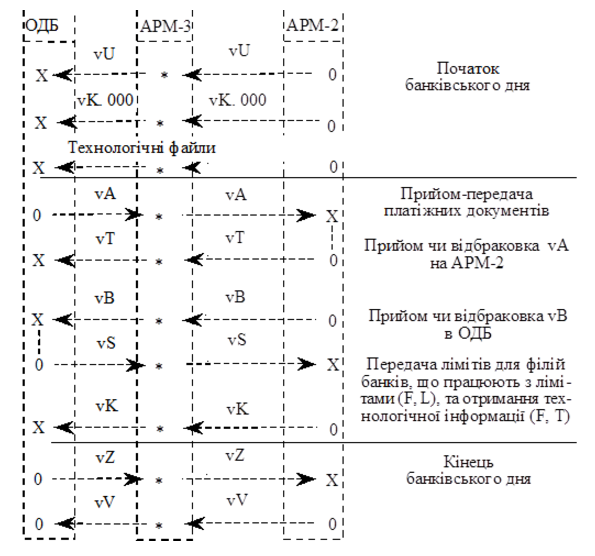


Рис. 11.1. Схема обміну інформацією між ОДБ банку та СЕП

*Умовні позначення:* 0 — місце породження файла;

x — місце обробки файла;

\* — місце перевірки і передачі файла.

Для роботи з бізнес-правилами ОДБ банку повинно мати допоміжний блок, який називається АРМ-М. Він виконує ряд функцій:

для головного банку:

 ведення бази даних бізнес-правил для філій;

 зміна бізнес-правил для філій, формування і відправка в СЕП файлів M.A ;

 формування завдань філіям на коригування їх бізнес-правил;

 отримання технологічної інформації з СЕП (файлів M.T) про проходження пакетів бізнес-правил до філії-адресата;

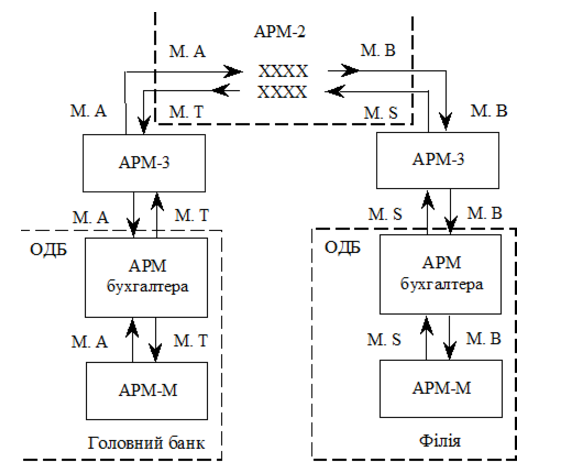
для філії:

 ведення бази даних бізнес-правил, що встановлюються для філії;

 прийом з СЕП файлів M.B — завдань на коректування бізнес-правил, виконання відповідної модифікації бази даних, відправка в СЕП технологічної інформації (файлів M.S) про обробку пакета бізнес-правил;

 перевірка початкових платежів філії на відповідність бізнес-правилам і заборону виконання платежів, не відповідних встанов­леним бізнес-правилам.

Можлива реалізація АРМ-М як однієї з підзадач АРМ-бух­галтера СЕП. Схему інформаційного обміну файлами під час роботи з бізнес-правилами подано на рис. 11.2.



**Рис. 11.2 Схема інформаційного обміну під час роботи  
з бізнес-правилами**

Під час роботи за сьомою моделлю управління роботою філій за допомогою бізнес-правил формуються такі файли:

М.А — файл бізнес-правил, що формується та відправляється головним банком на АРМ-2;

М.Т — файл-квитанція на відправлений файл бізнес-правил головному банку від АРМ-2;

М.В — файл бізнес-правил, які отримує філія від АРМ-2;

М.S — файл-квитанція на файл бізнес-правил , що відправляється з філії на АРМ-2.

Файли бізнес-правил та квитанції на них мають структуру, аналогічну відповідним файлам СЕП.

## 11.2. Технологія міжбанківських платежів у комерційному банку

Робота протягом одного робочого дня виконується за таким режимом:

1. Відкриття нового дня.

2. Початок дня.

3. Передача та прийом пакетів платіжних документів протягом дня.

4. Кінець дня.

5. Сервіс.

При відкритті нового дня встановлюється дата для даного банківського дня. Для неї формується каталог поточного банківського дня для відображення роботи системи протягом дня.

### 11.2.1. Робота в режимі «початок дня»

В режимі «початок дня» від АРМ-2 приймається ціла низка файлів, що забезпечують роботу СЕП. Це такі файли:

 vK.000, що вміщує інформацію про розмір коштів на коррахунку банку на початок робочого дня. Цей файл є обов’язковим, без нього не можна виконувати прийом та передачу платіжних документів.

 vU завдання на корегування списку учасників СЕП. Цей файл є необов’язковим. Він передається лише у випадках появи нових учасників СЕП.

Для банків, що працюють за сьомою моделлю, надходить файл типу vM, що вміщує бізнес-правила.

### 11.2.2. Робота в основному режимі

Режим «Передача та прийом пакетів платіжних документів» є основним режимом функціонування СЕП.

В режимі «Передача та прийом пакетів платіжних документів» виконується така робота: передача початкових платіжних документів, прийом та обробка документів, що надійшли електронною поштою.

Підготовка платіжних документів виконується в комерційних банках за допомогою власного пакета «Операційний день банку». При цьому ОДБ має забезпечувати:

 формування всіх реквізитів платіжного документа;

 формування з окремих платіжних документів пакета початкових платежів;

 розміщення сформованого пакета в каталозі обміну ОДБ та АРМ-3.

Документи, сформовані програмою ОДБ, передаються в АРМ-3 у вигляді текстових файлів.

Прийом та передача платіжних документів може виконуватись одноразовим запуском режиму «Передача та прийом пакетів платіжних документів» чи автоматично через певні інтервали часу (цей порядок задається в параметрах налагодження АРМ-3).

АРМ-3 через певний інтервал часу запускає електронну пош­ту. При цьому він обробляє файли, що знаходяться у вхідних каталогах від ОДБ і АРМ-2, розкладає файли-результати у вихідні каталоги для ОДБ та для електронної пошти.

З кожним файлом, що надійшов до АРМ-3, виконуються такі дії:

1. Перевірка на унікальність імені файла протягом банківського дня.

2. Перевірка файла в цілому (правильність формування імені файла, відповідність його поточній даті роботи, відповідність структурі, обчислення та перевірка контрольних сум).

3. Подокументальна перевірка файла.

Файл, що перевіряється незалежно від результатів, записується в каталог поточного робочого дня.

Якщо перевірений файл не приймається АРМ-3, то формується і надсилається відправнику файла (в ОДБ для файла vA чи в РРП для файла vB) квитанція, що вказує на причини відмови прийняти файл.

Для отримання довідки про відправлені та прийняті файли необхідно користуватись режимом «Сервіс».

На кожний відправлений в РРП файл vA обов’язково має прийти квитанція, по якій можна визначити, пройшли чи ні файли в СЕП. Якщо протягом деякого інтервалу (1-2 годин) довідка не отримана, то це свідчить, що файл взагалі не надійшов у СЕП. В такому разі необхідно його шукати в статистиці роботи електронної пошти чи зв’язуватись по телефону з РРП.

РРП обслуговується комплексом АРМ-2, що працює циклічно в автоматичному режимі. За сеанс електронної обробки вважаєтьсяодин цикл обробки файлів, прийнятих в момент початку циклу.  
В сеансі обробляються файли платіжних документів типу vA і vB, а також файли квитанцій типу vT і vS. Після закінчення сеансу РРП надсилає тим комерційним банкам, від яких в даному сеансі були отримані файли типу vA та vS, файл з інформацією про динамічний стан технічного кореспондентського рахунку — файл типу vK. Ця інформація дає змогу формувати пакети платіжних документів для передачі у СЕП таким чином, щоб не допустити овердрафт.

АРМ-3 приймає від ОДБ тільки файли поточного банківського дня.

АРМ-3 передає в ОДБ всі файли незалежно від їх банківської дати, крім файлів vB.

ОДБ повинен обробляти незалежно від дати файли V і U. При надходженні в ОДБ більше одного файла U вони повинні бути оброблені в хронологічному порядку.

Єдиний тип файлів СЕП, який може прийматись і оброблятися за різні банківські дні — це файл B. У день формування пакета «функціональний підтип файла СЕП» формується рівним «0». Якщо в день формування пакета платежу файл не був проведений по технічному коррахунку банку, то він переночує на спеціальному рахунку в РРП, який дістав умовну назву «нічного», і на наступний банківський день АРМ-2 привласнює даному пакету нове ім’я і знову відправляє його банку.

При цьому:

 склад і вміст платіжних документів пакета (тобто інформаційних рядків пакета) не змінюється,

 день і місяць в імені файла (і в заголовному рядку) змінюється — заноситься дата нового банківського дня,

 до «функціонального підтипу» імені файла додається одиниця.

Таким чином, непідтверджені файли B відправляються одержувачу протягом 9 банківських днів (в день формування vB «функціональний підтип» рівний 0, в подальші дні змінюється відповідно на «1», «2», ..., «9»). СЕП не зберігає файли vB більше 10 днів. Файли, не підтверджені протягом цього терміну, підлягають примусовій квітовці в РРП.

### 11.2.3. Робота в режимі «Кінець дня»

Режим «Кінець дня» складається з кількох етапів. Необхідними умовами завершення дня є:

 отримання квитанції від РРП на всі відправлені банком файли початкових платежів;

 отримання квитанцій від ОДБ на всі отримані банком від РРП і надіслані до ОДБ файли зворотних платежів.

АРМ-3 виконує перевірку, чи на всі відправлені в РРП файли vA отримано з РРП файли-квитанції vT. Якщо в РРП відправлені файли типу vA і виконано закриття банківського дня раніше, ніж прийшли квитанції на них, то це вважається порушенням технології роботи в СЕП. АРМ-3 контролює цю ситуацію й видає повідомлення про те, що закривати день ще не можна з тієї причини, що в системі залишились несквітовані файли vA.

Формується й відправляється в АРМ-2 файл vZ, що містить звіт про роботу системи за даний банківський день.

Протокольний звіт використовується для архівування в РРП, обліку, звітності та для вирішення спірних питань. Відправка цього файла обов’язкова. Відправити файл vZ наступного дня неможливо.

Виконується архівування журналу програми криптографування. Після закриття дня створюється архів закритого дня. При спробі заархівувати незакритий день буде видано відповідне повідомлення.

## 11.3. Інформаційне забезпечення СЕП

Усі файли СЕП є текстовими файлами. Їхня структура має такий вигляд:

— службовий рядок;

— заголовковий рядок;

— інформаційні рядки.

Заголовковий рядок несе інформацію про файл у цілому. Зокрема, він вміщує інформацію про кількість інформаційних рядків у файлі. Усі інформаційні рядки файла конкретного типу мають однакову довжину (крім файла vM). У деяких типів файлів інформаційні рядки відсутні. В такому разі склад файла СЕП обмежується службовими та заголовковими рядками. Усі рядки (службовий, заголовковий і всі інформаційні) закінчуються символами повернення каретки (переведення рядка CHR(13)+CHR(10)), які будуть позначатись як CRLF. Під час аналізу файла відсутність CRLF повинна розцінюватись як порушення структури файла. Розподілювачі кінця файла не використовуються. Службовий рядок використовується для підвищення безпеки та надійності СЕП.

### 11.3.1. Правила задання імен файлів

Усі імена файлів інтерфейса АРМ-3 — ОДБ мають таку структуру:

vtАRxxmd. f nn,

де v — однобайтний ідентифікатор валюти у СЕП. Для української національної валюти введене позначення «v». Для інших валют 1-й символ імені файла містить однобайтний ідентифікатор валют згідно з довідником валют СЕП, який може приймати значення (A ... Z, 0 ... 9).

t — тип файла у СЕП (нині використовуються такі типи файлів: A, T, B, S, K, Z, V, F, M, U, O). В міру розвитку системи список може розширюватись.

АRxx—ідентифікатор банка у СЕП,

де А — однобайтний ідентифікатор АРМ-2 СЕП, якому підпорядкований банк. Згідно з діючою нині системою це — друга літера електронної адреси АРМ-2. Якщо банк не працює у СЕП у національній валюті, то ставиться цифра 0 ;

R — ідентифікатор адміністративного регіону України, де розташована банківська установа;

хх — унікальний ідентифікатор банку в межах даного регіону.

Слід зазначити, що Rxx збігається з останніми трьома байтами електронної адреси банку в електронній пошті НБУ.

m — місяць банківського дня у системі числення за основою 36;

d*—*день місяцябанківського дня у системі числення за основою 36 (1,2, . . .,9, А,В,С, . . .,U,V);

f— функціональний підтип файла СЕП:

— для типу F,M — підтип файла,

— для типу В — ознака повторної передачі,

— для всіх інших типів — 0.

nn — технологічний номер файла за 36-річною системою обчислення (00 ... ZZ). У ньому допускаються цифри від 0 до 9 і латинські літери.

Ім’я файла квитанції формується з імені файла, що квітується шляхом заміни символу «тип файла» на відповідний тип квитанції (наприклад, A —>T, B — >S) .

АРМ-1, АРМ-2, АРМ-3 СЕП обмінюються інформацією у вигляді текстових файлів.

Кожен пакет платіжних документів повинен вміщувати документи в одній валюті.

Файли, імена яких побудовані не за заданим стандартом СЕП, не розглядаються.

### 11.3.2. Структура файлів

**Файл А** містить інформацію про початкові платежі банку — відправника платежів у СЕП. Кожний інформаційний рядок несе інформацію про один платіжний документ, всі документи файла повинні бути представленими у одній валюті.

Заголовковий рядок файла А має таку структуру:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Назва файла | С | 12 |
| 2 | Дата+час створення файла | D | 10 |
| 3 | Кількість інформаційних рядків у файлі | N | 6 |
| 4 | Сума дебету по файлу | N | 16 |
| 5 | Сума кредиту по файлу | N | 16 |
| 6 | Електронний цифровий підпис (ЕЦП) | B | 64 |
| 7 | Ідентифікатор ключа ЕЦП | С | 6 |
| 8 | ЕЦП заголовкового рядка | B | 64 |
| 9 | CRLF | B | 2 |

Інформаційний рядок файла А має таку структуру:

| № п/п | Назва реквізиту | Тип | Довжина |
| --- | --- | --- | --- |
| 1 | МФО банку А | N | 9 |
| 2 | Особовий рахунок клієнта банку А | N | 14 |
| 3 | МФО банку Б | N | 9 |
| 4 | Особовий рахунок клієнта банку Б | N | 14 |
| 5 | Ознака «дебет/кредит» платежу | C | 1 |
| 6 | Сума платежу | N | 16 |
| 7 | Вид платежу | N | 2 |
| 8 | Номер операційний платежу | C | 10 |
| 9 | Валюта платежу | N | 3 |
| 10 | Дата платіжного документа | D | 6 |
| 11 | Дата надходження платіжного документа в банк А | D | 6 |
| 12 | Назва платника (клієнта А) | C | 38 |
| 13 | Назва отримувача (клієнта Б) | C | 38 |
| 14 | Призначення платежу | C | 160 |
| 15 | Допоміжні реквізити | C | 60 |
| 16 | Код призначення платежу | C | 3 |
| 17 | Спосіб заповнення реквізитів 14-16 | C | 2 |
| 18 | Ідентифікатор клієнта А | N | 14 |
| 19 | Резерв | C | 14 |
| 20 | Ідентифікатор документа | N | 9 |
| 21 | Ідентифікатор операціоніста банку А | C | 6 |
| 22 | Номер рядка БІР | N | 2 |
| 23 | Резерв | C | 8 |
| 24 | ЕЦП основних реквізитів платежу | B | 64 |
| 25 | Ім’я файла А | C | 12 |
| 26 | Порядковий номер інформаційного рядка у файлі А | N | 6 |
| 27 | Час проходження через АРМ-3 А | T | 4 |
| 28 | Час отримання в АРМ-2 А | T | 4 |
| 29 | Ім’я файла С | C | 12 |
| 30 | Порядковий номер інформаційного рядка у файлі С | N | 6 |
| 31 | Час формування в АРМ-2 С | T | 4 |
| 32 | Час отримання в АРМ-2 С | T | 4 |
| 33 | Ім’я файла В | C | 12 |
| 34 | Порядковий номер інформаційного рядка у файлі В | N | 6 |
| 35 | Час формування в АРМ-2 В | T | 4 |
| 36 | Час отримання в АРМ-3 В | T | 4 |
| 37 | Дата отримання в АРМ-3 В | D | 6 |
| 38 | CLRF | B | 2 |

Реквізит «Номер (операційний) платежу» відповідає номеру, який поставив клієнт-відправник на платіжному документі. Реквізит «Ідентифікатор операціоніста банку А» містить ідентифікатор того операціоніста банку А, який сформував електронний платіжний документ і завірив його ЕЦП. На файл А завжди формується файл-квитанція T.

**Файл vT** — це файл-квитанція на відповідний файл vA. Він містить інформацію про те, прийнятий чи ні відправлений на АРМ-2 пакет платіжних документів, якщо ні, то з якої причини.

Файл vA у СЕП завжди приймається або ж не приймається у цілому, тобто якщо відбраковано хоча б один платіж з файла, то інші платежі з цього ж файла також не приймаються до обробки.

Якщо vA містить помилки в одному або кількох платежах, то відповідний файл vT містить інформаційні рядки у кількості, що дорівнює кількості виявлених помилкових документів. Кожний рядок однозначно ідентифікує помилковий документ з відповідними кодами помилок для кожного з документів.

Структура заголовкового рядка файла Т має такий вигляд:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Назва файла | С | 12 |
| 2 | Дата+час створення файла | D | 10 |
| 3 | Кількість інформаційних рядків у файлі | N | 6 |
| 4 | Сума дебета по файлу | N | 16 |
| 5 | Сума кредиту по файлу | N | 16 |
| 6 | Електронний цифровий підпис (ЕЦП) | B | 64 |
| 7 | Ідентифікатор ключа ЕЦП | С | 6 |
| 8 | Назва квітуємого (КВ) файла | С | 12 |
| 9 | Дата+час створення КВ файла | D | 10 |
| 10 | Кількість інформаційних рядків у КВ файлі | N | 6 |
| 11 | Сума дебета по КВ файла | N | 16 |
| 12 | Сума кредиту по КВ файлу | N | 16 |
| 13 | ЕЦП КВ файла | B | 64 |
| 14 | Ідентифікатор ключа ЕЦП КВ файла | С | 6 |
| 15 | Код помилки по КВ файлу | С | 4 |
| 16 | ЕП заголовкового рядка файла | В | 64 |
| 17 | CRLF | B | 2 |

Якщо файл vA вміщує помилку не в платіжних документах, а в заголовковому рядку, то відповідний файл vT не утримує інформаційних рядків, а містить лише код помилки в інформаційному рядку.

Структура інформаційного рядка файла Т:

|  |  |  |  |
| --- | --- | --- | --- |
| п/п | Назва реквізиту | Тип | Довжина |
| 1 | Порядковий номер інформаційного рядка (ІР) у файлі А | N | 6 |
| 2 | Код помилки | С | 4 |
| 3 | СRLF |  |  |

Файл T формується лише АРМ-2. Реквізити «Сума дебета по файлу» і «Сума кредиту по файлу» дорівнюють відповідним сумам файла vA, що квітується, якщо файл прийнятий без помилок. Ці суми дорівнюють 0, якщо файл бракується з будь-якої причини.

Файл Т підтверджує нормальний прийом файла у тому випадку, якщо: реквізит «Кількість інформаційних рядків» дорівнює нулеві, самі інформаційні рядки взагалі відсутні, код помилки по КВ файла = «0000» і виконуються такі рівності:

«Сума дебета по файлу А» = «Сумі дебета по КВ файла»

«Сума кредиту по файлу А»= «Сумі кредиту по КВ файла»

Якщо файл vA містить помилку не в платіжних документах, а в заголовковому рядку, то відповідний файл vT не утримує інформаційних рядків, а вміщує лише код помилки в інформаційному рядку.

**Файл vB** містить інформацію про зворотні платежі банку отримувачу платежів у СЕП. Кожний інформаційний рядок несе інформацію про один платіжний документ. На файл vВ завжди формується файл-квитанція vS.

Структура заголовкового рядка файла vВ збігається з структурою заголовкового рядка файла vА. Структура інформаційного рядка файла vВ збігається із структурою інформаційного рядка файла vА. В полі «ЕЦП основних реквізитів платежу» знаходиться ЕЦП, яка накладає АРМ-3 банку-відправника.

**Файл vS** — це файл-квитанція на зворотний файл vB. Він містить інформацію про те, прийнятий чи ні відправлений пакет пла­тіжних документів, якщо ні, то з якої причини.

У випадку, якщо сам АРМ-3 провів відбраковку vB і навіть не передає його в ОДБ, квитанція S генерується в АРМ-3 й автоматично надсилається до АРМ-2 .

Файл vB у СЕП завжди приймається або ж ні у цілому, тобто, якщо з файла відбраковано хоча б один платіж, то інші платежі з цього файла до обробки також не приймаються.

Якщо vB містить помилки в одному або кількох платежах, то відповідний файл vS містить інформаційні рядки, кількість яких дорівнює кількості виявлених помилкових документів. Кожний рядок однозначно ідентифікує помилковий документ з відповідними кодами помилок для кожного з документів.

Якщо файл vB містить помилку не в платіжних документах, а в заголовковому рядку, то відповідний файл vS не утримує інформаційних рядків, а містить лише код помилки в інформаційному рядку.

Зарахування грошей по файлу vB на коррахунок здійснюється тільки після отримання АРМ-2 квитанції S з нульовими кодами завершень на цей файл.

Структура заголовкового та інформаційного рядків файла vS збігається із структурою відповідних рядків файла vT.

**Файл vК** містить технологічну інформацію про сеанс роботи АРМ-2 з АРМ-3:

 список файлів vА, що надійшли від АРМ-3;

 список файлів vВ, на які надійшли файли vS від АРМ-3;

 інформацію про величину технічного коррахунку, поточні ліміти коррахунку і т.ін.

Розширення у назві файла відповідає номеру технологічного сеансу. Для відстеження правильності у послідовності файлів vК номер попереднього vК зазначається у заголовковому рядку поточного vК.

Файл з розширенням 000 містить інформацію станом на початок банківського дня РРП.

Кожний інформаційний рядок утримує інформацію про один файл vA чи vB, на які надійшли файли типу vS. Якщо значення реквізиту «Коди помилок» дорівнює «0000», то сума по даному файлу була проведена по коррахунку.

**Файл vZ** формується у банку і є сигналом для АРМ-2 про те, що АРМ-3 цього банку завершив роботу після прийняття/передачі файлів платіжних документів. Файл містить таку інформацію про роботу АРМ-3 з АРМ-2 протягом банківського дня:

 список файлів vA, відправлених з АРМ-3 у СЕП;

 список файлів vВ, отриманих у банку, на які сформовані і відправлені у СЕП квитанції vS.

Файл vZ може не утримувати інформаційних рядків. Розширення файла Z повинно бути «000». Якщо банк працює одночасно з кількома валютами, то на кожний тип валюти формується окремий файл vZ.

Кожний інформаційний рядок утримує інформацію про один відправлений файл vA чи надісланий файл vB. Якщо значення реквізиту «Коди помилок» дорівнює «0000», то:

 для відправленого vA одержаний vТ без помилок;

 для отриманого vВ прийнятий з ОДБ та переданий у АРМ-2 vS з нульовими кодами помилок.

В усіх інших випадках треба аналізувати конкретні коди помилок.

За технологією банк може відправляти протокольний звіт тільки тоді, коли на всі відправлені у РРП vA отримані квитанції vT та на всі прийняті vB отримані з ОДБ й передані у РРП квитан­ції vS. Якщо банк посилає vZ у момент, коли який-небудь файл не дочекався квитанції, то цей стан файла відображається відповідним кодом помилки на цей файл.

**Файл vV** містить інформацію про значення технічного коррахунку та про платіжні документи банку:

 початкові платежі, прийняті АРМ-2 від банку;

 всі зворотні платежі, сформовані АРМ-2 для банку.

Кожний інформаційний рядок несе інформацію про один платіжний документ. Файл vV може не утримувати інформаційних рядків.

Файл U необхідний для автоматизованого корегування списку учасників електронних платежів в усіх АРМ СЕП.

Структура заголовкового рядка файла U

| № п/п | Назва реквізиту | Тип | Довжина |
| --- | --- | --- | --- |
| 1 | Назва файла | С | 12 |
| 2 | Дата+час створення файла | D | 10 |
| 3 | Кількість інформаційних рядків у файлі | N | 6 |
| 4 | Кількість банків—учасників СЕП до коригування | N | 16 |
| 5 | Кількість банків—учасників СЕП після коригування | N | 16 |
| 6 | ЕЦП файла | B | 64 |
| 7 | Ідентифікатор ключа ЕЦП | С | 6 |
| 8 | Кількість інвалютних коррахунків до коригування | N | 6 |
| 9 | Кількість інвалютних коррахунків після коригування | N | 6 |
| 10 | Резерв | С | 32 |
| 11 | ЕП заголовкового рядка файла | В | 64 |
| 12 | CRLF | B | 2 |

Інформаційний рядок файла U має таку структуру:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Назва реквізиту | Тип | Довжина |
| 1 | Ознака операції | С | 1 |
| 2 | МФО банку | N | 9 |
| 3 | Назва банку | С | 38 |
| 4 | Коррахунок банку | N | 14 |
| 5 | Ідентифікатор банку у СЕП | С | 4 |
| 6 | Електронна адреса банку в NBUMAIL | C | 4 |
| 7 | Модель роботи з єдиним коррахунком | С | 1 |
| 8 | Номер моделі роботи з єдиним коррахунком | С | 1 |
| 9 | МФО головного банку чи 0 | N | 9 |
| 10 | Ідентифікатор валюти | N | 3 |
| 11 | Тип платіжної системи шлюзового банку | С | 1 |
| 12 | Ознака блокування банку | С | 1 |
| 13 | АРМ-2, який обслуговує валютний рахунок | C | 1 |
| 14 | Резерв | С | 32 |
| 15 | CLRF | B | 2 |

**Лекція 12. Безпека електронних банківських документів та платежів.**

## 12.1. Загрози безпеки АБС

Основні загрози безпеки АБС можна розподілити на такі групи: інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові (див. рис. 11.1). Дамо пояснення основних видів загроз.

*Несанкціонований доступ* — вид комп’ютерних порушень, який полягає в отриманні користувачем доступу до об'єкта, на який у нього немає санкціонованого дозволу адміністратора системи.

*Маніпулювання даними***—**це свідома фальсифікація, дезінформації чи приховування даних.

*Установка програмних закладок***—**цеспеціально розроблена і приховано впроваджена в захищену систему програма, яка дає змогу зловмиснику дістати доступ до захищених ресурсів системи.

*Неправильне розмежування прав доступу***—**це надання певних повноважень особам, які не є відповідальними за ту чи іншу технологічну операцію. Будь-яка захищена система містить засоби, що використовуються в надзвичайних ситуаціях, коли користувач повинен мати можливість доступу до всіх наборів системи. Звичайно ці засоби використовуються адміністраторами, операторами, системними програмістами та іншими користувачами, що виконують спеціальні функції. Надання цих повноважень більш широкому колу спеціалістів є серйозною загрозою безпеки системи.

Кожний з користувачів системи повинен мати чіткі і обмежені його посадовими функціями права доступу до ресурсів системи. Набори прав доступу повинні охоронятися системою захисту від несанкціонованого (незаконного) їх захоплення.

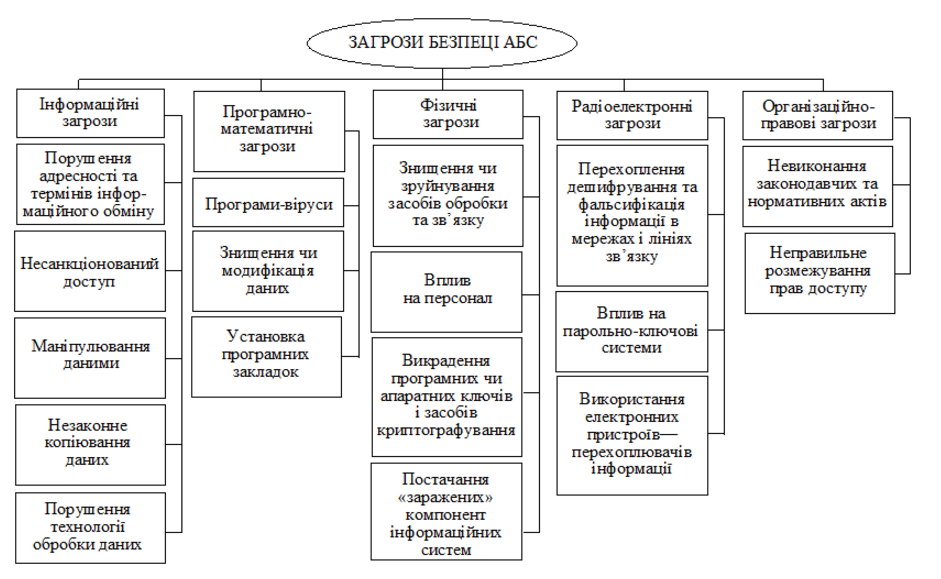


Рис. 12.1. Загрози безпеці АБС

## 12.2. Основні засоби захисту

До основних засобів захисту інформації можна віднести такі: фізичні засоби, апаратні засоби, програмні засоби, апаратно-прог­рамні засоби, криптографічні та адміністративні методи.

*Фізичні засоби захисту —*це засоби, необхідні для зовнішнього захисту ЕОМ, території та об’єктів на базі обчислювальної техніки, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та ін­формації, що захищаються. Спектр сучасних фізичних засобів захисту дуже широкий. Це різного роду замки, які можуть встановлюватись на вході в приміщення та на блоках системи, це системи пожежної сигналізації і т.п. До цієї групи засобів захисту також належать різні засоби екранування робочих приміщень та каналів передачі даних.

*Апаратні засоби захисту* — це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв’язку та ін.

Основні функції апаратних засобів захисту:

 заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача;

 заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних в результаті випадкових чи зумисних дій персоналу;

 захист цілісності програмного забезпечення.

Ці функції реалізуються шляхом:

 ідентифікації суб’єктів (користувачів, обслуговуючого персоналу) і об’єктів (ресурсів) системи;

 аутентифікації суб’єкта по наданому ним ідентифікатору;

 перевірки повноважень, яка полягає в перевірці дозволу на певні види робіт;

 реєстрації (протоколювання) при звертаннях до заборонених ресурсів;

 реєстрації спроб несанкціонованого доступу.

*Програмні засоби захисту* необхідні для виконання логічних і інтелектуальних функцій захисту, які вмонтовані до складу програмного забезпечення системи.

За допомогою програмних засобів захисту реалізуються наступні задачі забезпечення безпеки:

 контроль завантаження та входу в систему за допомогою сис­теми паролів;

 розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних і т.п.;

 захист файлів від вірусів;

 автоматичний контроль за роботою користувачів шляхом протоколювання їх дій.

*Апаратно-програмні засоби захисту* — це засоби, які основані на синтезі програмних та апаратних засобів. Ці засоби широко використовуються при аутентифікації користувачів АБС. Аутентифікація — це перевірка ідентифікатора користувача перед допуском його до ресурсів системи.

Апаратно-програмні засоби захисту використовуються також при накладанні електронно-цифрових підписів відповідальних користувачів. Найбільш поширеним в АБС є вико-  
ристання смарт-карт, які вміщують паролі та ключі користу-  
вачів.

*Криптографічні методи захисту* — це методи, основані на криптографічних перетвореннях даних, тобто на їх шифруванні.

Основні криптографічні методи захисту:

 шифрування з допомогою датчика псевдовипадкових чисел, яке полягає в тому, що генерується гамма шифра за допомогою датчика псевдовипадкових чисел і накладається на відкриті дані з врахуванням зворотності процесу;

 шифрування за допомогою криптографічних стандартів шиф­рування даних (з симетричною схемою шифрування), в основі якого використовуються перевірені і випробовані алгоритми шиф­рування даних з великою криптостійкістю, наприклад амери-  
канський стандарт DES;

 шифрування за допомогою пари ключів (з асиметричною сис­темою шифрування), в яких один ключ є відкритим і використовується для шифрування інформації, другий ключ — закритим і використовується для розшифрування інформації. Прикладом може служити метод RSA.

Криптографічні методи захисту інформації дуже широко використовуються в АБС і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту.

В таблиці наведено характеристики алгоритмів криптозахисту.

|  |  |  |
| --- | --- | --- |
| Характеристика | DES | RSA |
| Вид алгоритму | Одноключовий | Двоключовий |
| Швидкість роботи | Швидко | Повільно |
| Функція, що використовується | Перестановка і підстановка | Піднесення до степеня |
| Довжина ключа | 56 біт | 300-600 біт |
| Найменш затратний криптоаналіз | Перебір по всьому клю­човому простору | Розкладання модуля |
| Стійкість | Теоретична | Практична |
| Часові витрати на розкриття | Століття | Залежать від довжини ключа |
| Час генерації ключів | Мілі-секунди | Десятки секунд |
| Тип ключа | Симетричний | Асиметричний |

Порівняльний аналіз алгоритмів криптозахисту дає можливість відмітити такі їх особливості. Алгоритм RSA працює приблизно в тисячу разів повільніше за алгоритм DES і потребує в десять раз довших ключів, його стійкість теоретично не доведена. Але велика перевага RSA полягає у відсутності необхідності організації строго засекреченої процедури обміну ключами.

Тому в АБС потрібно застосовувати гібридні системи, засновані на двох і більше алгоритмах, використовувати їх переваги.

*Адміністративні засоби захисту —*це заходи організаційного характеру, регламентуючі процеси функціонування АБС, використання її ресурсів, діяльність персоналу і т. д. Мета цих заходів в найбільшій мірі перешкодити та виключити можливість реалізації загроз безпеки. Адміністративно-організаційних заходів багато. Наведемо лише деякі:

 розробка чіткої технології обробки інформації в АБС та конт­роль за її дотриманням**;**

 організація захисту від встановлення прослуховуючої апаратури в приміщеннях інформаційних служб;

 ретельний відбір персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки).

**12.3. Основні задачі та вимоги до захисту банківської інформації в СЕП**

В міжбанківських платежах використовується нова для України форма платіжних інструментів — електронний платіжний документ. Такий документ має встановлену форму і відповідні засоби захисту, що надаються НБУ кожному учаснику СЕП. Крім того, кожний банк—учасник СЕП може мати власну систему захисту внутрібанківських розрахунків.

Система безпеки СЕП розроблена з урахуванням таких вимог:

 система захисту охоплює всі етапи розробки, впровадження та експлуатації програмно-технічного комплексу СЕП;

 система безпеки включає організаційні, технічні, апаратні і програмні засоби захисту;

 в системі чітко розподілена відповідальність за різні етапи обробки та виконання платежів.

В системі виділені такі основні задачі захисту СЕП:

 захист від зловживань (несанкціоноване розшифрування повідомлень, поява фальсифікованих повідомлень);

 автоматичне протоколювання використання банківської мережі з метою локалізації порушників технології роботи в СЕП;

 захист від технічних пошкоджень та збоїв в роботі обладнання (вихід з ладу апаратних та програмних засобів, поява перешкод в каналах зв’язку).

Система безпеки СЕП є багатоступеневою. Вона не тільки включає засоби шифрування інформації на різних її рівнях, а й вміщує цілий комплекс технологічних та бухгалтерських засобів контролю за проходженням платежів у СЕП. Технологічний та бухгалтерський контроль забезпечується програмно на всіх рівнях, що дає змогу персоналу РРП і учасникам СЕП слідкувати за порядком проходження платежів як на протязі дня, так і за підсумками його завершення.

### 12.3.1. Технологічні засоби контролю

*Технологічні засоби контролю* включають:

 механізм обміну квитанціями, що дозволяє однозначно ідентифікувати отримання адресатом конкретного пакета документів і достовірність отриманої в ньому інформації;

 механізм інформування банків-учасників про поточний стан його кореспондентського рахунку за підсумками кожного технологічного сеансу, що дозволяє банку простежити відповідність змін коррахунку після сеансу прийому/передачі пакетів платіжних документів;

 обмін банку та РРП підсумковими документами в кінці дня, програмне зведення підсумкових документів як в РРП, так і в банку;

 програмний комплекс самодіагностики, що дозволяє виявити порушення цілісності та узгодженості баз даних АРМ-2, що мо­жуть виникнути в результаті збою функціонування системи, спроб несанкціонованого доступу (НДС) до баз даних АРМ-2 чи їх фізичного пошкодження;

 обмін АРМ-2 та АРМ-1 звітними повідомленнями про функціонування РРП в цілому;

 механізм контролю програмних засобів на предмет несанкціонованої модифікації виконавчих модулей.

Всі технологічні засоби контролю вмонтовані в програмне забезпечення. У випадках виникнення нестандартної ситуації чи підозри на НДС оператору АРМ-2 видається відповідне повідомлення з наданням йому можливості оперативного втручання, а та­кож автоматично дублюється повідомлення про виникнення нестандартної ситуації на АРМ-1.

### 12.3.2. Бухгалтерські засоби контролю

*Бухгалтерські засоби контролю* включають:

 низку звітних документів, отриманих як від АРМ-2, так і від АРМ-3, що вміщують повну технологічну та бухгалтерську інформацію, перехресні посилання та аналіз балансу;

 низку звітних форм АРМ-1, що вміщують інформацію про стан СЕП в Україні;

 засоби вивірення взаємодій РРП в АРМ-1, що дозволяють виявити неузгодженість в звітній інформації, що надана в РРП;

 засоби аналізу причин відсутності балансу в масштабах України.

Використання тільки технологічних та бухгалтерських методів контролю є недостатнім для забезпечення захисту від зловживань при передачі платіжних документів в СЕП. Тому необхідне автоматичне ведення протоколу виконуваних дій в системі платежів, що має також забезпечувати захист цього протоколу від підробки та модифікацій. Всі ці вимоги можуть бути виконані тільки за допомогою програмних та апаратних засобів захисту.

### 12.3.3. Програмні та апаратні засоби захисту інформації

Захист банківської інформації в СЕП включає комплекс дій, пов’язаних з шифруванням інформації, що циркулює в платіжній системі. Шифруванню підлягають усі файли СЕП: початкові і зворотні платіжні файли, файли квитанцій, файли звітів, файли лімітів, файли стану коррахунку, файли нормативно-довідкової інформації.

Усі платіжні документи СЕП перед відправленням з банку обробляються апаратно-програмними засобами захисту інформації, що забезпечують виконання таких вимог з точки зору безпеки інформації:

 інформація, що передається, має бути закритою, тобто повідомлення може бути прочитане лише тим, кому воно адресоване;

 цілісність — випадкове чи навмисне пошкодження повідомлення на етапі його передачі буде виявлене під час його прийому;

 аутентичність відправника (під час прийому повідомлення можна однозначно визначити, хто його відправив).

Крім перерахованих основних вимог, необхідно виконувати низку допоміжних, що дає змогу більш детально аналізувати мож­ливі нестандартні ситуації:

 засобами захисту інформації ведеться шифрований арбітраж­ний журнал, в якому зберігається протокол обробки інформації, а також вміст файлів, що обробляються;

 у шифроване повідомлення включені поля дати та часу обробки.

В основу роботи засобів захисту інформації в СЕП покладено алгоритм шифрування із закритими ключами відповідно до ДСТ 28147-89. Цей метод характеризується високою надійністю з точки зору його дешифрування, але ставить дуже високі вимоги до процедури транспортування та зберігання закритих ключів, секретність яких забезпечує на практиці стійкість системи шифрування.

Основними засобами захисту інформації в СЕП є апаратні засоби. Секретність ключів у них забезпечується технологічно:

 ключі зберігаються в спеціальній електронній картці, прочитати їх можна тільки за допомогою спеціального блоку, що виконує процес шифрування інформації. Прочитати ключі іншими засобами неможливо;

 електронна картка видається банку з попередньою прив’яз­кою її до конкретного блоку шифрування цього ж банку; втрачена чи викрадена картка не буде працювати в іншому шифро-блоці (наприклад, в апаратурі іншого банку);

 у випадку крадіжки одночасно блоку і картки у конкретного банку передбачено режим виключення цієї апаратури зі списку користувачів СЕП; банк може продовжити роботу в СЕП після вирішення юридичних та фінансових питань, пов’язаних з втратою апаратури та отриманням нового комплексу.

Найбільш слабким місцем з точки зору безпеки є ділянка підготовки платежів персоналом банку—учасника СЕП. Всі зареєстровані більш-менш успішні спроби НДС були з боку представників банків, що призводило до крадіжки коштів у власного банку, а не в держави чи в інших банках. В усіх цих випадках особи, які робили спроби НДС, мали легальний доступ до системи підготовки та захисту платіжної інформації, причому їх повноваження були перевищені (доступ до багатьох чи навіть до всіх банківських ресурсів системи).

З метою гарантування безпеки інформації на цій ділянці від учасників СЕП вимагається виконання низки організаційних вимог:

 допуск тільки довірених осіб до ключових операцій підготовки платіжних документів;

 виконання відповідальними особами банку постійного, реального та достатнього контролю за станом бухгалтерського балансу та кореспондентського рахунку банку;

Всі повноваження щодо доступу до програмно-апаратних засобів банку недоцільно зосереджувати в особі одного співробітника банку: за кожну ділянку обробки платежів має відповідати окремо уповноважений (адміністратор локальної мережі, адміністратор електронної пошти, відповідальний за роботу АРМ-3 СЕП і т.ін.).

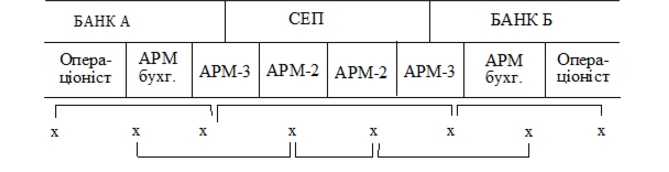
Для гарантування безпеки інформації на рівні банків—учасників СЕП пропонується впровадження перехресного накладення електронного підпису на платіжні документи.

Банкам пропонується використання програмних засобів, що реалізують цифровий підпис, реалізований на основі алгоритму RSA.

Алгоритм RSA належить до асиметричних алгоритмів шифрування. Кожний учасник обміну електронними документами має два ключі: секретний, що повинен ретельно оберігатися від сторонніх осіб і бути відомим тільки його власнику, та відкритий, що розповсюджений в системі і може бути відомим кожному учаснику системи.

Суть алгоритму RSA зводиться до того, що в основу електронного цифрового підпису покладено оброблене спеціальним ал­горитмом саме повідомлення, яке підписується, причому шифрування цього прототипу електронного цифрового підпису виконується за допомогою секретного ключа відправника і відкритого ключа отримувача повідомлення. При цьому саме повідомлення може не шифруватись (цей варіант реалізовано в програмному комплексі НБУ), але спробу модифікувати підписане повідомлення (навіть один біт) буде відразу виявлено при перевірці підпису отриманого повідомлення. Під час перевірки електронного цифрового підпису програмним комплексом отримувача формується прототип електронного підпису отриманого повідомлення. Отриманий цифровий підпис дешифрується відкритим ключем від­правника і секретним ключем отримувача повідомлення і вираховується прототип електронного цифрового підпису. Отриманий прототип порівнюється з обрахованим прототипом електрон­ного цифрового підпису. Збіг цих двох прототипів підпису (отри­маного та обчисленого) показує, що повідомлення було підписане зазначеним відправником інформації та отримане у тому ж вигляді, в якому воно було підписане.

Схему використання електронного цифрового підпису представлено на рис.10.2.



Виходячи з технології обробки платежів для СЕП, ОДБ має забезпечувати чітке виконання двох операцій для різних робочих місць.

1.***На робочому місці операціоніста*** має виконуватись накладення електронного цифрового підпису на адресу АРМ-3, яке в подальшому буде включатися до файлу початкових платежів банку (тип А). При цьому треба використовувати секретний ключ операціоніста та відкритий ключ АРМ-3 банку.

2.***На робочому місці АРМ-бухгалтера*** після формування файла початкових платежів має виконуватись операція накладення електронного цифрового підпису на адресу АРМ-2 на файл типу A*.*При цьому використовується секретний ключ бухгалтера і відкритий ключ АРМ-2.

При отриманні зворотного файла типу B на АРМ-бухгалтера виконується перевірка електронного цифрового підпису АРМ-2 на адресу АРМ-бухгалтера. При цьому використовується відкритий ключ оператора АРМ-2 та секретний ключ бухгалтера.

Секретні ключі кожного учасника локальної мережі ОДБ мають бути записані на дискету чи інший апаратний засіб зберігання ключів і ретельно зберігатися господарем секретного ключа від крадіжок та втрат.