ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ»

Виконав: студент 7 курсу, групи БСЗМ-71
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Якубенко С.В.
(прізвище та ініціали)
Керівник Савченко В.А.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібенетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
“___” _____ 2022 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Якубенко Сергій Вячеславович
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія застосування методів криптографічного захисту інформації в системах електронних міжбанківських платежів»
керівник магістерської роботи Савченко В.А. , д.т.н., професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від « 12» жовтня 2022 року № ____.

2. Строк подання студентом магістерської роботи 15.05.2022р.

3. Вихідні дані до магістерської роботи
Методи та засоби захисту інформації в системах електронних міжбанківських платежів.
Науково-технічна література. Стандарти. Рекомендації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Система електронних міжбанківських платежів як об’єкт інформаційної безпеки.

2. Методи та засоби забезпечення безпеки в системах електронних міжбанківських платежів.
3. Способи і засоби забезпечення інформаційної безпеки.

5. Перелік графічного матеріалу

1. Тема.
2. Система електронних платежів в Україні
3. Аналіз загроз та ризиків СЕП
4. Стандарти електронних розрахунків
5. Вибір системи шифрування
6. Технологія накладання/перевірки ЕЦП у СЕМП
7. Висновки

6. Дата видачі завдання 20.03.2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Аналіз науково-технічної літератури	26.10.2022р.	
2.	Аналіз системи електронних міжбанківських платежів як об'єкту інформаційної безпеки	01.11.2022р.	
3.	Методи забезпечення криптографічного захисту в системах електронних міжбанківських платежів	06.11.2022р.	
4.	Вибір та застосування методів криптографічного захисту інформації в системах електронних міжбанківських платежів	16.112022р.	
5.	Реферат, вступ, висновки.	21.11.2022р.	
6.	Підготовка презентації до захисту.	15.12.2022р.	

Студент _____ Владіміров В.О.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ Власенко В.О.
(підпис) (прізвище та ініціали)

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента **Якубенко Сергій Вячеславович**

на тему: **«Технологія застосування методів криптографічного захисту інформації в системах електронних міжбанківських платежів»**

Актуальність: Стрімкий розвиток популярності глобальний мережі Інтернет привів до виникнення потужного імпульсу розвитку нових підходів і рішень в найрізноманітніших областях світової економіки.

Система електронних платежів являє собою сукупність правил, організаційних заходів, програмно-технічних засобів, які використовуються банком для забезпечення здійснення розрахунків у межах України між банками як за дорученнями клієнтів банків, так і за зобов'язаннями банків. СЕП виконує міжбанківський переказ у файловому режимі та в режимі реального часу. Дана система належить до багаторівневих критичних систем, тому що її відмова, відступ від обмежень, що задаються, або зміни в роботі підсистеми можуть викликати серйозні наслідки або привести до краху всієї системи в цілому.

Позитивні сторони:

1. Зміст роботи відповідає завданню. Студент показав високий рівень знань і ступінь підготовленості її до майбутньої роботи за фахом.
2. Обґрунтовано необхідність розвитку вибору та налаштування криптографічних механізмів захисту інформації в системах електронних міжбанківських платежів .
3. Текст викладено грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. Не достатньо розкрито вимоги до автоматизованої банківської системи.
2. Доцільно було б провести порівняння між криптографічними методами.

Вищезгадані зауваження не впливають на загальну позитивну оцінку магістерської роботи.

Висновок: робота заслуговує оцінку "*добре*", а студент – Владіміров Андрій Олександрович гідний присвоєння кваліфікації 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Якість магістерської роботи	
Виконано на замовлення підприємств	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ МПТ	*
Має практичну цінність	*
Проект-частина комплексної теми	

Підпис рецензента _____

_____
(П.І.Б.)

_____
(посада, науковий ступінь, вчене звання)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Якубенко С.В. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія застосування методів криптографічного захисту інформації в системах електронних міжбанківських платежів».
Магістерська робота і рецензія додаються.
Директор інституту _____ _____В.А. Савченко
(підпис)

Довідка про успішність

Якубенко С.В. ____ за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року до 2023 року повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ ___ _____
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Якубенко С.В.*** обрав тему роботи, метою якої було дослідити здійснення аналізу чинних в Україні методів та засобів захисту інформації в системах електронних міжбанківських платежів; визначення уразливостей, загроз та ризиків; формулювання основних вимог безпеки в системах електронних міжбанківських платежів. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Якубенко С.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студента Владімірова Андрія Олександровича на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Савченко В.А
(підпис)
“___”_____2023 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Якубенко С.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____”_____2023 рік

РЕФЕРАТ

Текстова частина магістерської роботи:87 сторінки, 5 рисунків, 1 таблиця, 30 джерел.

Об'єкт дослідження – процес побудови захищеної СЕМП.

Предмет дослідження – види криптографічних алгоритмів та їх ефективніть.

Мета роботи – дослідити підвищення ефективності виявлення, аналізу та реагування на шахраїв, а також забезпечення конфіденційності, цілісності, захищеності та правового режиму доступу до інформації, яка циркулює в міжбанківській інформаційній системі.

Методи дослідження – теорія криптографії та шифрування, теорія інформаційної безпеки.

В роботі проведено аналіз можливих загроз інформаційним ресурсам СЕМП, особливості їх реалізації та заходи щодо послаблення їх деструктивного впливу.

Зроблено огляд основних методів захисту комерційної інформації В СЕМП.

Виявлено основні проблеми криптографічного захисту електронної платіжної системи.

Запропоновано рекомендації щодо реалізації криптографічних механізмів захисту для забезпечення внутрішньої та зовнішньої безпеки СЕМП на основі розмежування доступу, контролю цілісності, застосування технології ЕЦП, аналізу захищеності, криптографічного захисту та використання системи захищеної електронної пошти.

Галузь використання – побудова систем моніторингу і аналізу подій та загроз в будь-яких системах електронних міжбанківських платежів.

СИСТЕМА ЕЛЕКТРОННИХ ПЛАТЕЖІВ, ПЛАТІЖНА СИСТЕМА, СИСТЕМА МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, АВТОМАТИЗОВАНА БАНКІВСЬКА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВПС	– внутрішньодержавна платіжна система
МПС	– міжнародна платіжна система
НБУ	– Національний банк України
СЕП	– система електронних платежів
СЕМП	– система електронних міжбанківських платежів
НСМЕП	– Національна система масових електронних платежів
АРМ	– автоматизоване робоче місце
БПЦ	– банківський прицесинговий центр
ГПЦ	– головний процесинговий центр
ЗПЦ	– зовнішній процесинговий центр
РПЦ	– регіональний процесинговий центр
СА	– сервер авторизації
СБД	– сервер баз даних
СЗ	– сервер застосувань
ПЦ	– процесинговий центр
РУ	– регіональне управління
РП	– розрахункова палата
ЗЗІ	– засоби захисту інформації
ЦРП	– центральна розрахункова палата
СП	– системне проектування
ОДБ	– програмний комплекс «Операційний день банку»
ЕП	– електронна пошта
ЕЦП	– електронний цифровий підпис
ЕК	– електронна комерція
ЕІС	– економічна інформаційна система
АІС	– автоматизована інформаційна система
АБС	– автоматизована банківська система
АКЗІ	– апаратура криптографічного захисту інформації
СТП	– система термінових платежів
АЗБД	– апаратура захисту банківських даних

ВСТУП

Актуальність теми. Стрімкий розвиток популярності глобальний мережі Інтернет привів до виникнення потужного імпульсу розвитку нових підходів і рішень в найрізноманітніших областях світової економіки. Новим течіям піддалися навіть такі консервативні системи, як системи платежів у банках. Це виразилося в появі і розвитку нових систем платежів – систем електронних платежів, головна перевага яких полягає в тому, що клієнти можуть здійснювати платежі (фінансові транзакції), минувши виснажливий і іноді технічно важкоздійсненний етап фізичного транспортування платіжного доручення у банк.

У системах електронних платежів циркулює інформація, в тому числі і конфіденційна, яка вимагає захисту від перегляду та модифікації. Розробка відповідних технологій захисту, орієнтованих на Інтернет, викликає серйозні ускладнення. Причина цього в тому, що архітектура, основні ресурси і технології мережі Internet орієнтовані на організацію доступу або збору відкритої інформації. Проте, останнім часом з'явилися підходи і рішення, що свідчать про можливість застосування стандартних технологій Інтернет в побудові систем захищеної передачі інформації.

Система електронних платежів являє собою сукупність правил, організаційних заходів, програмно-технічних засобів, які використовуються банком для забезпечення здійснення розрахунків у межах України між банками як за дорученнями клієнтів банків, так і за зобов’язаннями банків. СЕП виконує міжбанківський переказ у файловому режимі та в режимі реального часу. Дана система належить до багаторівневих критичних систем, тому що її відмова, відступ від обмежень, що задаються, або зміни в роботі підсистеми можуть викликати серйозні наслідки або привести до краху всієї системи в цілому.

У зв’язку з цим можна зробити висновок, що тема магістерської роботи, присвячена розробці рекомендацій щодо вибору та налаштування криптографічних механізмів захисту інформації в системах електронних міжбанківських платежів, є

актуальною.

Мета роботи – здійснення аналізу чинних в Україні методів та засобів захисту інформації в системах електронних міжбанківських платежів; визначення уразливостей, загроз та ризиків; формулювання основних вимог безпеки в системах електронних міжбанківських платежів, формулювання рекомендацій щодо вибору та налаштування криптографічних механізмів захисту інформації в системах електронних міжбанківських платежів.

Для досягнення поставленої мети в роботі вирішуються такі *завдання:*

- досліджено системи електронних міжбанківських платежів як об'єкта інформаційної безпеки;
- досліджено методи та засоби забезпечення криптографічного захисту електронних документів в системах електронних міжбанківських платежів;
- обґрунтовано рекомендації щодо застосування методів криптографічного захисту для забезпечення безпеки в СЕМП.

Виходячи з такого *об'єктом дослідження в дипломній роботі є* процес побудови криптографічного захисту інформації в системах електронних міжбанківських платежів. *Предметом дослідження* є загальні підходи та методики щодо вибору методів та засобів для побудови системи інформаційної безпеки в системах електронних міжбанківських платежів.

Для вирішення вищезазначеного завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки, а також прикладної криптології та організаційно-технічного захисту інформації, використання нормативно-правової бази держави.

Новизна одержаних результатів полягає в пропозиціях покращення системи захисту інформації СЕМП, які випливають із зробленого аналізу

Практичне значення одержаних результатів. Нові наукові результати, отримані в роботі складають у сукупності фундамент для більш ефективного та якісного застосування методів криптографічного захисту інформації в СЕМП.

1 СИСТЕМА ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ ЯК ОБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Система електронних платежів в Україні

1.1.1. Принципи організації та функціонування СЕП в Україні. Основні функції та учасники 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 [1].

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 файлу 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 понад 90% міжбанківських переказів у національній валюті в межах України.

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).

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).

Задачі та функції СЕП.

Нормальне функціонування економіки важко уявити без системи розрахунків між суб'єктами господарської діяльності, забезпечення надійності та своєчасності платежів. У розрахунках і платежах, що здійснюються установами банків, відображаються практично всі види економічних відносин у суспільстві і

все це неможливо без розрахунків між банками. Для забезпечення міжбанківських розрахунків створюються спеціальні платіжні системи. Платіжні системи міжбанківських розрахунків різних країн організовані по-різному, і в світі не існує єдиної платіжної моделі, однак є загальні принципи і характеристики, які визначають функціонування національних платіжних систем [3].

Розлад у платіжній системі тієї чи іншої країни часто є одним з перших і безпосередніх проявів зародження фінансової кризи. В Україні в 1992-1993 рр. Розрахунки між банківськими установами проводилися за допомогою паперових платіжних документів протягом трьох тижнів, а в деяких випадках - місяці і більше. Кожен день відстрочки створення системи обертався значними збитками для підприємців через зростання темпів інфляції і фінансових втрат від розкрадань за підробленими платіжними документами. Розуміючи важливість цієї проблеми, НБУ в 1992 р .. Розробив Концепцію електронного грошового обігу в Україні, яка була розглянута банками і затверджена Правлінням НБУ.

Програмне забезпечення та засоби захисту інформації були розроблені фахівцями НБУ і вперше передані учасникам системи міжбанківських розрахунків в липні-вересні 1993 року. 5 серпня 1993 почалася пробна експлуатація системи, учасниками якої були три комерційні банки Києва, а з жовтня 1993 року в усіх регіонах України почалося впровадження СЕП в промислову експлуатацію.

Впровадження СЕП дозволило з 1 січня 1994 повністю відмовитися від використання поштових і телеграфних авізо та значно підвищити швидкість, якість і надійність проведення платежів, безпеку і конфіденційність банківської інформації. Система електронних платежів дозволила значно підвищити швидкість обігу грошей.

«Систему високо оцінили її користувачі, а також зарубіжні фахівці, провідні міжнародні інститути. Аналогів СЕП немає не тільки в одній країні колишнього СРСР, а й в більшості країн світу. Показово, що консультанти, які допомагали Україні впроваджувати СЕП, визнають: учні перевершили вчителя»

Впровадження системи електронних платежів України дозволило досягти

таких принципових результатів:

- Прискорення виконання розрахунків та обігу коштів;
- Зменшення документообігу;
- Зменшення ймовірності фальсифікації міжбанківських розрахункових документів, завдяки чому знизилася прихована емісія, пов'язана з надходженням в обіг коштів, отриманих за підробленими документами;
- Вивільнення грошової маси;
- Посилення контролю за станом грошової маси в державі, поява нових можливостей впливу з боку Національного банку на цей стан;
- Підвищення можливостей НБУ контролювати здійснення платежів;
- Значне зниження збитків держави і підприємців, які виникали раніше внаслідок високих темпів інфляції, низької швидкості виконання розрахунків та використання підроблених платіжних документів.

Можна без перебільшення зробити висновок, що впровадження СЕП підняло банківську індустрію України на якісно новий рівень.

Система електронних платежів Національного банку України (СЕП НБУ) – загальнодержавна платіжна система, яка забезпечує здійснення розрахунків між банківськими установами, органами державного казначейства на території України із застосуванням електронних засобів приймання, обробки, передачі та захисту інформації.

У розрахунках між банками України використовуються лише електронні платіжні документи.

Електронний платіжний документ – це банківське повідомлення визначеного формату, яке містить інформацію про переказ коштів, має вигляд файлу при передачі по банківській мережі та при зберіганні на магнітних носіях.

Банківські повідомлення у формі електронних документів повинні, відповідати певним вимогам:

1. Бути підготовлені, передані і прийняті з використанням програмно-технічних засобів, які сертифіковані і затверджені НБУ.

2. Банківські електронні документи повинні бути захищені спеціальними

засобами, які надаються централізовано національним банком України, відповідно до положення про систему захисту електронних банківських документів в обчислювальній мережі національного банку України та положення про арбітражні послуги служби захисту електронних банківських документів в обчислювальній мережі НБУ. їх захист ґрунтується на використанні методів ідентифікації вузлів відправника та одержувача повідомлення, його шифрування і дешифрування на основі використання методів криптографії в вузлах-адресатів, а також при передачі по каналах ЕП, накладання електронного підпису та авторизації відправника та одержувача електронного банківського документа.

Основні завдання системи:

- задоволення потреб економіки, що реформується і розвивається;
- вдосконалення кредитно-монетарної політики, яку проводить НБУ, завдяки отриманню оперативної та точної інформації про переміщення грошових коштів і стан кореспондентських рахунків;
- виконання міжбанківського етапу всіх видів безготівкових розрахунків;
- мінімізація часу на виконання міжбанківських розрахунків та на обіг грошових коштів;
- високий рівень безпеки міжбанківських розрахунків;
- надання широкого спектру послуг для користувачів;
- високий рівень внутрішнього бухгалтерського обліку та контролю;
- мінімізація вартості банківського посередництва шляхом оптимізації платіжних засобів і раціоналізації систем.

Основними функціями СЕП є:

- проведення розрахунків між банками України в національній валюті країни;
- ефективне використання тимчасово вільних ресурсів банків;
- контрольні функції Національного банку про стан кореспондентських рахунків банків;
- надання інформаційних послуг учасникам розрахунків;

- обмін екстреної інформацією про проведення розрахунків;
- забезпечення надійності розрахунків;
- багатоступінчастий контроль за достовірністю даних на всіх стадіях розрахунків;
- багаторівневий захист інформації від несанкціонованого доступу, використання, викривлення і фальсифікації на всіх стадіях обробки;
- надання НБУ механізму впливу на порушників чинного законодавства та норм банківської діяльності методом обмеження їх обслуговування в СЕП.

Основні фактори, що визначають вимоги до кількісних і якісних показників системи:

- поточна завантаженість СЕП;
- перспективи економічного розвитку України;
- можливість інфляції;
- тенденція переходу від готівки форм розрахунків до безготівкових;
- оцінка досвіду інших країн, що розвиваються, по динаміці розвитку міжбанківських розрахунків.

НБУ як центральний банк країни, бере безпосередню участь в міжбанківських розрахунках і організовує їх реалізацію. Саме НБУ є гарантом платіжної системи в цілому і системи міжбанківських електронних платежів зокрема. Інші банки України, як учасники міжбанківських розрахунків, несуть солідарну відповідальність за їх стан і діють відповідно до нормативних актів НБУ і договорів учасників міжбанківських розрахунків.

Розрахунки між банками ведуться на підставі кореспондентських рахунків банків, які відкриваються в регіональних управліннях НБУ.

Регіональне управління НБУ (РУ) – це установа НБУ, уповноважена виконувати в певному регіоні визначені чинним законодавством функції та операції від імені головної установи НБУ. Головною вважається установа НБУ, обслуговує рахунки регіональних управлінь НБУ при здійсненні міжбанківських розрахунків.

Система електронних платежів організаційно представлена мережею

розрахункових палат НБУ, яка була створена відповідно до Постанови Правління НБУ від 16.07.93 за № 57. Вона складається з регіональних розрахункових палат (РРП) і Центральної розрахункової палати ЦРП

Регіональна розрахункова палата – це підрозділ РУ НБУ, у функції якого входить обслуговування системи електронних платежів і впровадження нових платіжних технологій в межах відповідного регіону.

Розрахункова палата (РП) – структурний підрозділ територіального управління Національного банку України, який обслуговує в СЕП банки відповідного банківського регіону.

Центральна розрахункова палата – установа Національного банку України, яка забезпечує функціонування СЕП у цілому, ведення бази даних для ЩС по електронних міжбанківських розрахунків, виконаних через СЕП, а також здійснює функції РП для банківських установ Києва і Київської області, обслуговує інші банківські регіони.

Принципи СЕП:

1. СЕП забезпечує розрахунки між банками в національній валюті України та в найбільш уживаних іноземних валютах.

2. СЕП функціонує за схемою типу "Брутто", оскільки кожна наступна оплата проводиться окремо з урахуванням підсумкового сальдо, отриманого на попередній операції, зменшує ризик недостатньої ліквідності банків-учасників.

3. Угоди відображаються в режимі реального часу на рахунках банків. Це дає можливість блокувати угоди, що призводять до овердрафту, (стан, коли на рахунку банку виникає дебетове сальдо), і мати необхідну інформацію для прогнозування стану ліквідності та своїх дій.

4. Ініційована банківською установою транзакція не підлягає скасуванню.

5. Відсутні пріоритети обробки транзакцій за ознаками, крім черговості надходження в систему.

6. Головним режимом роботи системи є передача електронних платіжних документів та підтвердження їх отримання. СЕП виключає необхідність використання паперової технології.

7. Обмін платіжними документами організовано у вигляді технологічних циклів прийому-передачі, тривалість яких коливається в залежності від поточних потреб.

8. Граничні суми транзакцій в системі не обумовлені.

9. СЕП є власністю НБУ і обслуговує комерційні банки на договірній основі. Учасники електронних платежів діють на підставі договору з регіональним управлінням НБУ на проведення міжбанківських розрахунків і "Положення про міжбанківські розрахунки в Україні" відповідно до "Регламенту функціонування мережі розрахункових палат України".

Права і обов’язки учасників СЕП регулюються двосторонніми договорами банків-учасників з регіональними управліннями НБУ - на ведення кореспондентських рахунків та проведення розрахунків в мережі розрахункових палат.

Основні обов'язки регіонального управління НБУ (розрахункової палати) по відношенню до банку-учасника СЕП:

- забезпечувати своєчасне і якісне здійснення міжбанківських розрахунків на регіональному та міжрегіональному рівнях;
- дотримуватися банківської таємниці та дотримуватися вимог банківської безпеки згідно "положення про захист системи електронних міжбанківських документів в обчислювальній мережі НБУ";
- відображати підсумки розрахунків банку на відповідному кореспондуючому рахунку;
- щодня видавати банку інформацію про результати міжбанківських розрахунків, виконаних в мережі розрахункових палат за попередній день;
- забезпечувати банк програмними засобами зв'язку з РРП, в тому числі по електронній пошті;
- забезпечувати необхідними консультаціями в підготовці персоналу банку для роботи в мережі розрахункової палати протягом місяця після підписання договору і подальші консультації протягом договору.
- регіональне управління НБУ має право відмовити банку в обслуговуванні

або тимчасово припинити надані послуги при порушеннях банком регламенту роботи в мережі СП України.

Основні обов'язки банку-учасника СЕП:

- подавати в розрахункову палату інформацію у вигляді електронних документів, підготовлених програмними засобами відповідно до вимог «регламенту функціонування мережі РРП»;
- використовувати при роботі в обчислювальній мережі НБУ лише офіційно придбані та зареєстровані програмні засоби;
- своєчасно оплачувати послуги, які надаються розрахунковою палатою;
- виконувати вимоги банківської безпеки, включаючи наявність технічних і програмних засобів банківської безпеки, а також умов зберігання, обліку та використання цих коштів.

Банк-учасник СЕП має право:

- передавати інформацію іншим абонентам засобами електронної пошти національного банку;
- вибирати будь-яку визнану НБУ систему для проведення своїх розрахунків, не обмежуючись рамками мереж розрахункових палат.

Виняток комерційного банку з СЕП здійснюється НБУ в разі:

- ліквідації комерційного банку за рішенням національного банку України;
- оголошення комерційного банку банкрутом за рішенням арбітражного суду;
- ліквідації комерційного банку за рішенням арбітражного суду;
- реорганізації або ліквідації комерційного банку за рішенням загальних зборів акціонерів.

Виняток комерційного банку з СЕП здійснюється Національним банком за рішенням самого вищого органу управління комерційним банком, який має право реорганізації і ліквідації банку.

Загальну структуру СЕП НБУ можна представити у вигляді схеми, яка зображена на рис. 1.1.

Серверна структура СЕП Національного банку України складається з

наступних компонентів:

- програмно-технічні комплекси СЕП;
- електронна пошта національного банку;
- способи захисту інформації.

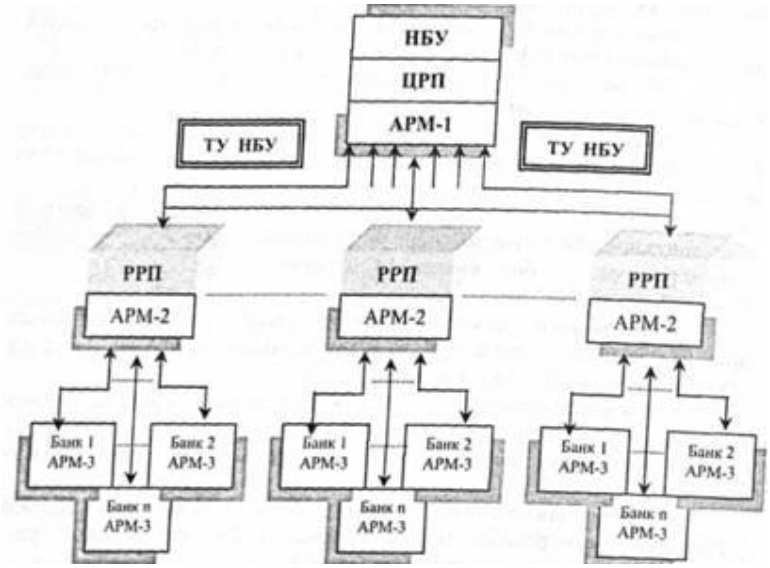

Рис. 1.1. Загальна структура СЕП

Система міжбанківських електронних платежів має трирівневу ієрархічну структуру.

На 1-му, верхньому рівні СЕП міститься Центральна розрахункова палата. Вона обслуговується програмно-технічним комплексом АРМ-1, виконує наступні основні функції:

1."Пересилання" міжрегіональних електронних документів засобами електронної пошти національного банку України.

2. Перевірку правильності формування електронних документів.

3. Формування та підтримка в робочому стані основних довідників НБУ.

Основним довідником, з яким працює СЕП, є довідник банків - учасників розрахунків. Він містить повний список банків, які є учасниками розрахунків через СЕП за станом на поточний банківський день. Зрозуміло, що цей список повинен бути однаковим на всіх АРМ СЕП і у всіх ОДБ банків-учасників і містити актуальну інформацію як щодо кількісного складу банків-учасників, так і

за їх реквізитами (найменування, підпорядкованості та т.і.).

Зміни в довіднику відбуваються:

- при відкритті нової банківської установи;
- при зміні назви або адреси електронної пошти установи;
- при переході філії банку у власність іншої юридичної особи("купівлі"філії);
- при перекладі банківської установи на обслуговування в інший РРП;
- при закритті банківської установи.

Синхронні зміни в довідниках усіх АРМ СЕП і в ОДБ банків відбуваються за допомогою спеціального файлу і - завдання на коректування довідника учасників розрахунків. Він створюється в Центральній розрахунковій палаті і розсилається з АРМ-1 на всі АРМ-2 СЕП. Кожен АРМ-2 потім передає його всім АРМ-НБУ банків, які він обслуговує. АРМ-НБУ банку передає цей файл в ОДБ. У момент проходження файлу і через кожен з АРМ СЕП виконуються зміни в довіднику учасників цього АРМ,

4) Захист електронних документів і системи в цілому від несанкціонованого доступу.

5) Диспетчеризація (бухгалтерський технологічний контроль) проходження міжрегіональних платежів і синхронізація закриття дня банку.

На 2-му рівні мережі розташовуються регіональні розрахункові палати, які обслуговуються своїми програмно-технічними комплексами АРМ-2.

АРМ-2 - це програмно-технічний комплекс, встановлений в РРП і призначений для обслуговування певної кількості банків цього регіону і організації взаємодії з іншими АРМ-2.

АРМ-2 забезпечує виконання наступних основних операцій:

1)обмін електронними документами між самою РРП і банками учасниками міжбанківських розрахунків;

2)формування і відправлення міжрегіональних платежів в ЦРП;

3)отримання міжрегіональних платежів від ЦРП і їх аналіз;

4)обмін електронними документами з іншими АРМ-2 своєї РРП;

5) захист електронних документів і їх обробка від несанкціонованого доступу.

На 3-му, нижньому рівні СЕП перебувають учасники міжбанківських електронних розрахунків, що діють на підставі угод з РРП на проведення розрахунків та Положення про міжбанківські розрахунки в Україні відповідно до Регламенту функціонування мережі розрахункових палат України. Учасниками електронних платежів можуть бути і здійснювати за допомогою СЕП міжбанківські розрахунки, будь-які кредитно-фінансові підприємства і організації, які мають відкриті КР у відповідних РУ НБУ і задовольняють вимоги, що висуваються НБУ до учасників СЕП.

У розпорядження кожного з учасників платежів надається єдина копія програмно-технічного комплексу з умовною назвою АРМ-3 (або інакше АРМ НБУ), через банк обмінюється інформацією з СЕП за допомогою файлів, структура і функціональне призначення яких визначені в документі "Інтерфейс між САБ і АРМ -3 системи електронних платежів (СЕП) ".

АРМ-3 на рівні банку-учасника розрахунків забезпечує виконання наступних основних операцій.

1) перевірку пакетів платіжних документів, підготовлених банком, що експлуатує даний АРМ-3;

2) обмін електронними документами з відповідною РРП;

3) захист системи від несанкціонованого доступу.

Оскільки для передачі пакетів використовується система електронної пошти (ЕП) НБУ, то банк одночасно є і абонентським вузлом цієї пошти, а АРМ-3 - одним з основних кінцевих користувачів цього вузла. Згідно АРМ-2 є кінцевим користувачем вузла 2-го рівня ЕП НБУ, а АРМ-1 - один з основних користувачів Центрального вузла ЕП НБУ.

Система електронної пошти Національного банку України (система ЕП) – система програмно-технічних засобів і організаційно-технологічних заходів забезпечення інформаційної взаємодії між банківськими та іншими установами в електронній формі.

З метою підвищення надійності та ефективності роботи СЕП Національний банк може змінювати технологічну структуру системи та шляхи програмно-технічної реалізації її компонентів і вимагати від учасників відповідної адаптації їх програмно-технічних засобів. Терміни інформування учасників розрахунків про необхідність внесення змін до програмно-технічного забезпечення мережі визначається Національним банком. Заміна програмно-технічних засобів і технологій електронних розрахунків здійснюється за розпорядженням ЦРП у разі потреби після експериментальної експлуатації системи в нових технологічних умовах.

Паралельно з розвитком економіки України СЕП постійно розвивається з метою підвищення надійності її функціонування, розширення спектру послуг банкам-учасникам СЕП, розвитку бухгалтерської моделі.

Одночасно зі створенням СЕП банки активно розробляли і впроваджували системи автоматизації внутрішньобанківської діяльності (так звані програмні комплекси "Операційний день банку" (ОДБ)). Це - програмне забезпечення, яке обслуговує поточну внутрішньобанківську діяльність (бухгалтерський облік, обслуговування рахунків клієнтів тощо).

Оскільки СЕП дозволила практично уникнути затримання платежів на міжбанківському рівні, для банків і їх клієнтів стало доцільним використання систем "клієнт-банк" для розрахунків в електронній формі між клієнтом банку та банком.

Деякі банки, що мають розгалужену систему філій, для здійснення розрахунків в електронній формі між своїми філіями створювали власні платіжні системи, так звані внутрішньобанківські платіжні системи (ВПС).

Створення ОДБ та ВПС відбувалося паралельно зі створенням і розвитком СЕП. Національний банк України практично не обмежував діяльності комерційних банків зі створення таких систем, контролюючи лише узгодження їх функціонування з СЕП.

Ще одним способом виконання міжбанківських розрахунків в Україні є встановлення між банками прямих кореспондентських відносин, яке здійснюється з метою прискорення розрахунків. З огляду на, що на території України діє

система електронних міжбанківських розрахунків НБУ, учасниками якої є всі банки і яка практично задовольняє потреби банків у цій сфері, прямі кореспондентські відносини між банками України встановлюються, як виняток. Це виняток може бути пов'язаний зі специфікою проведення банківських операцій, що мають постійний характер. Наприклад:

- при здійсненні операцій з продажу та купівлі валютних коштів на міжбанківській валютній біржі;
- при розрахунках між банками за операціями, які мають постійний характер і великі обсяги.

Щоразу дозвіл на встановлення прямих кореспондентських відносин надає Національний банк України, за наявності обґрунтування банками доцільності цього [2].

Система міжбанківських розрахунків України перебуває на поточний момент з таких компонентів:

- система електронних міжбанківських розрахунків національного банку України;
- системи термінових платежів;
- системи автоматизації роботи банків;
- внутрішньобанківські платіжні системи;
- системи "клієнт-банк";
- система масових платежів з використанням карток.

1.2. Міжбанківські інформаційні системи

1.2.1. Поняття автоматизованої банківської системи

Створення і функціонування автоматизованих банківських технологій базується на системотехнічних принципах, які відображають найважливіші положення теоретичної бази, яка включає ряд суміжних наукових дисциплін і напрямів. До них відносяться економічна кібернетика, загальна теорія систем,

теорія інформації, економіко-математичне моделювання банківських ситуацій і процесів, аналіз і прийняття рішень.

Історично розвиток АБС пройшов ряд етапів.

Перші серійні АБС працювали на автономних персональних комп'ютерах, що не були об'єднаними в локальну мережу. Операціоністи виконували проводки безпосередньо за особовими рахунками клієнтів. В кінці операційного дня дані з усіх комп'ютерів переносили на дискетах на один - головний комп'ютер, на якому розраховувався баланс.

I. Початковий етап автоматизації був заснований на використанні *автономних робочих місць банківських фахівців*; етап характеризується відносною простотою реалізації, можливістю швидкого впровадження, нечисленністю команди розробників, практичною незалежністю від комунікацій.

II. Перехід *до єдиного операційного дня* – природний крок на шляху до формування єдиної банківської бухгалтерії, орієнтований на звітності.

У 1992р. у багатьох банках впроваджувалося в другому поколінні АБС на основі локальних мереж з розміщенням всіх робочих файлів на її сервері. Коли кілька користувачів з кількох робочих станцій одночасно зверталися до даних, в локальній мережі виникали «конфлікти». Мережа досить скоро перевантажувалася, і було потрібно збільшувати потужність сервера і пропускну здатність активного мережевого обладнання. Системи, зроблені на технологічній базі «персональних» СУБД, перестали задовольняти багато банків і, перш за все, великі: для них важлива була ефективна робота в локальній мережі.

III. Потреби в розширенні можливостей з аналізу діяльності банку і його клієнтів призвели до створення *інтегрованих систем банківського обліку*, націлених на розширення аналітичних можливостей в багатофіліальному банку, в тому числі, і можливості аналізу клієнтської бази.

IV. Розвиток АБС, спрямованих на інтегрованість щодо можливостей аналізу звітності та на *багатофункціональність системи управління банківською діяльністю*.

V. Створення інтегрованих АБС (ІАБС), орієнтованих на використання

розподілених, комплексних, *адаптивних систем управління банківською діяльністю*. Характерними рисами такого виду систем є формування єдиного інформаційного простору, адаптованість в залежності від змінення вимог і зовнішніх умов (включаючи зміни законодавства і нормативів, розширення номенклатури послуг), комплексність рішень, заснованих на системах проектування інформаційних систем [4].

Автоматизована банківська система (базовий комплекс) дозволяє організувати швидке і якісне обслуговування клієнтів по широкому спектру послуг. Основні функціональні модулі системи реалізують:

- розрахунково-касове обслуговування юридичних осіб;
- обслуговування рахунків банків-кореспондентів;
- кредитні, депозитні, валютні операції;
- будь-які види вкладів приватних осіб та операції з ним;
- фондові операції;
- розрахунки за допомогою пластикових карт;
- бухгалтерські функції;
- аналіз, прийняття рішень, менеджмент, маркетинг та ін.

1.2.2. Вимоги до автоматизованої банківської системи

Першою і основною вимогою, яка ставиться до АБС, є вимога щодо її функціональної повноти. Повнофункціональною можна вважати систему, якщо набір її функцій дає змогу виконувати всі операції конкретного банку. Звичайно, система, яка відповідає сьогоднішнім потребам, може не задовольняти їх завтра, якщо у банку з’являться нові функції. Тому наступною вимогою, що ставиться до АБС, є її гнучкість.

Гнучкість — це один з ключових факторів, який полягає у тому, що будь-яка банківська система повинна мати можливість розширюватись та розвиватись і не лише фірмою-розробником, а й силами спеціалістів банку. Розвиток системи може відбуватися у двох напрямах: кількісному — при збільшенні кількості філій

чи клієнтів та якісному — при розширенні спектра банківських операцій і послуг. Зміни кількісного характеру приводять до необхідності нарощування системи, яке може виконуватись двома способами:

за рахунок встановлення у головній конторі більш потужної ЕОМ чи шляхом розпаралелення процесу обробки на кілька ЕОМ;

за рахунок збільшення продуктивності обчислювальних комплексів у філіях банку і переходу на розподілену обробку даних, зберігши за центральним обчислювальним комплексом лише функції консолідації балансу та обслуговування поточних інформаційних потреб.

Вибір способу нарощування АБС залежить від стратегії розвитку банку, особливостей взаємодії головної контори та її філій, а також від прийнятого розподілу функцій та відповідальності за них. Але в будь-якому разі розробник АБС повинен вказати конкретні шляхи вирішення проблеми нарощення системи для того чи іншого банку.

В цілому система повинна мати можливість розширення як по горизонталі (збільшення кількості клієнтів, каналів зв’язку і т.п.), так і по вертикалі (перехід на більш потужну техніку).

При цьому мають бути зведені до мінімуму можливі зміни:

інтерфейса користувача;

технології роботи з системою;

структури файлів бази даних.

Також має бути виключена або зведена до мінімуму необхідність модифікації прикладного програмного забезпечення і перепідготовки персоналу.

Надійність полягає в тому, що АБС повинна забезпечувати роботу великої кількості користувачів, які одночасно можуть вводити, коригувати документи (рахунки чи угоди), формувати звітність без будь-яких конфліктів, пов’язаних з одночасним доступом до даних.

Реальний масштаб часу після введення документа АБС повинен забезпечувати його бухгалтерське проведення. Новий стан рахунків відразу стає доступним для всіх користувачів й відоб-ражається у балансі, а також може бути

використаний при обчисленні нормативів. Система, побудована з урахуванням цієї вимоги, має такі переваги:

дозволяє в будь-який момент часу мати повну картину фінансового стану банка;

надає можливість оперативно відстежувати інформацію, що надходить у систему;

надає можливість отримання додаткових кредитних ресурсів.

Інтегрованість системи означає, що система повинна складатися з інформаційно та функціонально пов'язаних між собою модулів. Інформаційний зв'язок полягає у тому, що всі складові системи працюють із спільною базою даних, що дає змогу уникнути дублювання та забезпечує цілісність й узгодженість даних. Функціональний зв'язок дозволяє функціональним задачам, які характеризуються однаковою прикладною логікою, але розв'язуються на різних АРМах, використовувати спільні процедури, що зберігаються у відповідних бібліотеках (наприклад, нарахування процентних ставок та ін.).

Забезпечення багатофіліальної роботи банку полягає в тому, що для банків, які мають багато філій, і особливо для тих, структура яких є трирівневою, важливим моментом є забезпечення єдності й цілісності технології. Виконання цієї вимоги в ідеальному варіанті — це забезпечення розподіленої обробки даних в режимі On-line. Забезпечення розподіленої обробки даних в такому режимі коштує поки що досить дорого і під силу не всім банкам. Тому більш реальним з точки зору забезпечення цієї вимоги є єдність технологій, тобто як мінімум системи всіх рівнів повинні мати однакову структуру даних, однакові інтерфейси і інструментальні засоби розробки програмного забезпечення [5].

Безпека та захищеність системи — це одна із життєво необхідних вимог, що ставиться до АБС. За оцінками західних спеціалістів, навіть великий і стабільний банк збанкрутує, якщо він відкриє всю свою документацію. Тому АБС має бути захищена як всередині від можливих зловживань співробітниками банку, так і зовні від різного роду спроб розкриття банківської таємниці та махінацій з його коштами.

1.2.3. Структура системи автоматизованої обробки банківської інформації

Створення або вибір автоматизованих банківських систем (АБС) пов'язані з плануванням всієї системної інфраструктури інформаційної технології банку. Під інфраструктурою АБС розуміється сукупність, співвідношення і змістовне наповнення окремих складових процесу автоматизації банківських технологій. В інфраструктурі крім концептуальних підходів виділяються забезпечуючі і функціональні підсистеми [6].

Структурна схема комплексної автоматизації банку включає наступні модулі:

– активно-пасивних операцій;

– автоматизації облікових операцій;

– аналізу та формування звітності;

– надання інтерактивних послуг.

Перелічимо основні функції АБС (зазвичай вони реалізуються у вигляді незалежних модулів єдиної системи):

– Автоматизація всіх щоденних внутрішньобанківських операцій, ведення бухгалтерії та складання зведених звітів.

– Система комунікації з філіями і іногородніми відділеннями.

– Система автоматизованого взаємодії з клієнтами («банк-клієнт »).

– Аналітичні системи, включаючи аналіз всієї діяльності банку і вибір оптимальних в даній ситуації рішень.

– Автоматизація роздрібних операцій, в тому числі застосування банкоматів і кредитних карток.

– Системи міжбанківських розрахунків.

– Системи автоматизації роботи банку на ринку цінних паперів.

– Інформаційні системи. Можливість швидкого отримання необхідної інформації, що впливає на фінансову ситуацію.

1.2.4. Характеристика сучасних банківських технологій

Сучасні банківські технології як інструмент підтримки та розвитку банківського бізнесу створюються на базі ряду основоположних принципів: комплексний підхід в охопленні широкого спектру банківських функцій з їх повною інтеграцією; модульний принцип побудови, що дозволяє легко конфігурувати системи під конкретне замовлення з наступним нарощуванням; відкритість технологій, здатних взаємодіяти з різними зовнішніми системами (системи телекомунікації, фінансового аналізу та ін.), забезпечувати вибір програмно-технічної платформи і можливість перенесення її на інші апаратні засоби; гнучкість настройки модулів банківської системи і адаптація їх до потреб і умов конкретного банку; масштабованість, яка передбачає розширення і ускладнення функціональних модулів системи в міру розвитку бізнес-процесів (наприклад, підтримка роботи філій і відділень банку, поглиблення аналізу і т.і.); розрахований на багато користувачів доступ до даних в реальному часі і реалізація функцій в єдиному інформаційному просторі; моделювання банку і його бізнес-процесів, можливість алгоритмічних налаштувань бізнес-процесів; безперервний розвиток і вдосконалення системи на основі її реінжинірингу бізнес-процесів.

Представляється важливим вирішення таких проблем:

– проведення аналізу зарубіжних АБС, виведення позитивних і негативних властивостей цих систем;

– визначення функціональних і забезпечують підсистем АБС;

– виявлення приблизної вартості АБС перед її впровадженням з метою визначення оптимальної банківської системи «щоб все могла і була по кишені»;

– розкриття ситуації, що склалася на російському і міжнародному ринку АБС;

– інформаційна безпека АБС.

АБС створюються відповідно до сучасних уявлень про архітектуру банківських додатків, яка передбачає поділ функціональних можливостей на три рівні.

Верхній рівень (Front-office) утворюють модулі, що забезпечують швидке і зручне введення інформації, її первинну обробку і будь-яку зовнішню взаємодію банку з клієнтами, іншими банками, ЦБ, інформаційними та торговими агенствами і т.д.

Середній рівень (Back-office) являє собою додатки з різних напрямків внутрішньобанківської діяльності та внутрішніми розрахунками (роботу з кредитами, депозитами, цінними паперами, пластиковими картками тощо).

Нижній рівень (Accounting) – це базові функції бухгалтерського обліку, або бухгалтерське ядро. Саме тут зосереджені модулі, що забезпечують ведення бухгалтерського обліку за всіма п'ятьма главами нового плану рахунків.

Поділ банку на front-office і back-office ґрунтується не стільки на функціональній специфіці обробки банківських операцій (угод) і прийняття рішень (узагальнення і аналізу), скільки на самій природі банку як системи, з одного боку, фіксуючої, а, з іншого, активно впливає на економічну взаємодію в фінансово-кредитній сфері [7].

При роботі банку зі своїми філіями можна виділити наступні напрямки автоматизації взаємодії:

– забезпечення міжфілійного і міжрегіонального документообігу;

– отримання консолідованої щоденної і аналітичної звітності;

– надання філіями інформації про всіх клієнтів банку і залишках на їх рахунках;

– функції, що контролюють та регламентують діяльність філії.

У системах інтерактивного обслуговування клієнтів активно використовуються такі пристрої:

– автоматичні телефонні довідкові системи;

– інформаційні інтелектуальні принтери;

– мультимедіа-кіоски;

– Web-сервери мережі Інтернет.

АБС засновані на мережевої технології в архітектурі "клієнт-сервер", спираються на єдині принципи побудови і функціонування. Слабкою стороною багатьох вітчизняних систем є недостатня підтримка специфіки банківської

справи та його моделювання, недостатнє відображення предметної області. Останнім часом стало приділятися більше уваги питанням фінансового аналізу і цілям управління бізнесом.

Сучасна банківська система - це сфера різноманітних послуг, наданих своїм клієнтам - від традиційних грошово позичкових і розрахунково касових операцій, що визначають основу банківської справи, до новітніх форм грошово кредитних і фінансових інструментів, використовуваних банківськими структурами (Лізинг, факторинг тощо).

В умовах посиленої міжбанківської конкуренції успіх підприємницької діяльності буде супроводжувати тим банкірам, які краще оволодіють сучасними методами управління банківськими процесами. сьогодні все більше банків роблять ставку на професійність своїх співробітників і нові інформаційні технології.

Інтерес до розвитку комп'ютеризованих банківських систем визначається не бажанням витягти миттєву вигоду, а, головним чином, стратегічними інтересами. Як показує практика, інвестиції в такі проекти починають приносити прибуток лише через певний період часу, необхідний для навчання персоналу і адаптації системи до конкурентних умов. Вкладаючи кошти в програмне забезпечення, комп'ютерне і телекомунікаційне обладнання та створення бази для переходу до нових обчислювальних платформ, банки, в першу чергу, прагнуть до здешевлення і прискорення своєї рутинної роботи та перемоги в конкурентній боротьбі.

1.3. СЕМП НБУ як об’єкт інформаційної безпеки

1.3.1. Загальні засади функціонування СЕМП НБУ

В Україні відповідно до Закону України "Про платіжні системи та переказ грошей в Україні"(2346-14) можуть створюватися системи міжбанківських розрахунків, що призначені для переказу грошей у межах України між банківськими установами для виконання зобов'язань їх клієнтів, а також власних

зобов'язань цих банківських установ.

Порядок діяльності системи міжбанківських розрахунків визначається її правилами, установленими платіжною організацією цієї системи та узгодженими з Національним банком. Для їх узгодження платіжна організація подає до Національного банку (на ім'я заступника Голови, до функціональних обов'язків якого належить загальне керівництво з питань функціонування платіжних систем в Україні) викладені державною мовою три прошиті та засвідчені на звороті відбитком печатки копії Правил діяльності системи міжбанківських розрахунків. Правила мають встановлювати:

– правову базу, на підставі якої платіжна організація має забезпечувати діяльність платіжної системи;

– організаційну структуру системи міжбанківських розрахунків;

– умови членства, порядок вступу та виходу із системи;

– порядок урегулювання неплатоспроможності та інших випадків нездатності виконання членами системи своїх зобов'язань;

– порядок вирішення спорів;

– управління ризиками в системі та систему страхування;

– перелік платіжних інструментів, що використовуються в системі для ініціювання переказу грошей, їх форми та порядок застосування;

– принцип виконання документів на переказ грошей та їх відкликання;

– порядок завершення міжбанківського переказу;

– порядок, технологію та регламент проведення розрахунків;

– порядок проведення реконсиляції;

– порядок використання програмно-технічних засобів, систем захисту інформації та телекомунікаційних каналів зв'язку;

– технологію формування, порядок та строки зберігання архівів електронних банківських документів і баз даних, а також процедуру знищення інформації щодо проведення переказу грошей, строки зберігання якої закінчилися;

– порядок резервування та відновлення функціонування системи в разі

порушення її роботи або виникнення надзвичайних ситуацій;

– інші положення, визначені платіжною організацією.

Визначений платіжною організацією порядок функціонування системи міжбанківських розрахунків, засоби формування і оброблення документів на переказ, що використовуються в системі, мають забезпечувати цілісність та конфіденційність інформації, своєчасне завершення щоденного оброблення платежів, високий рівень безпеки й операційної надійності системи, відновлення роботи системи в разі порушення її роботи або виникнення надзвичайних ситуацій.

Банківські установи здійснюють міжбанківський переказ за міжбанківськими електронними розрахунковими документами, що формуються ними на підставі:

– паперових розрахункових документів клієнтів;

– паперових розрахункових документів банківської установи;

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

– електронних розрахункових документів, отриманих засобами ВПС від філії банку;

– електронних розрахункових документів, автоматично сформованих САБ за умовами договорів або згідно з потребою банківської установи;

– електронних розрахункових документів, отриманих засобами інших платіжних систем, телекомунікаційних систем, інших засобів зв'язку за умови забезпечення цілісності та конфіденційності інформації тощо [8].

1.3.2. Структурна схема СЕМП НБУ

Загальна структура НСМЕП включає в себе такі основні елементи:

1. Центр системної ініціалізації та системної персоналізації (установа НБУ).

2. Розрахунковий банк (РБ) системи на базі Головного управління НБУ. Схема розрахунків – клірингова.

3. Головний та регіональні процесінгові центри (ГПЦ та РПЦ) в обласних управліннях НБУ або комерційних установах (до 25 РПЦ на всю Україну). Вони виконують обробку міжбанківських транзакцій, розрахунок клірингу, керування системою.

4. Банки-емітенти і банки-еквайєри НСМЕП із своїми банківськими системами, торгівельною інфраструктурою та інфраструктурою сфери послуг.

5. Користувачі карток – фізичні та юридичні особи.

6. Картки на інтегрованих схемах (або смарт-картки). Для забезпечення захисту банківської інформації в ВПБС на різних рівнях використовуються криптографічні механізми, однак, бурхливе зростання обчислювальної техніки, створення систем і технологій кібертерроризму призводить до появи нових загроз (активних і пасивних атак) і злому підсистеми захисту ВПБС [9].

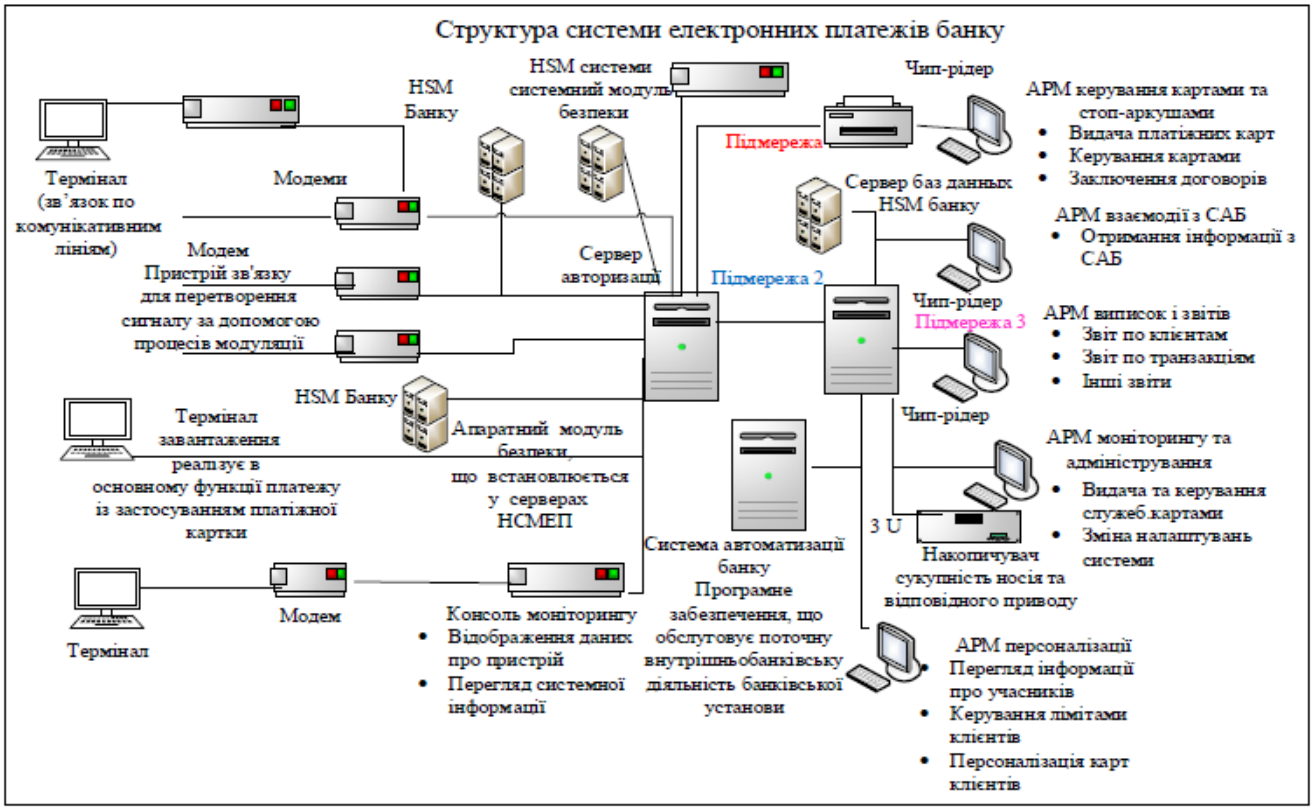

Рис. 1.2. Структура системи електронних платежів

1.3.3. Загальна структура та основні елементи НСМЕП НБУ

Згідно ПОЛОЖЕННЯ про захист інформації в Національній системі масових електронних платежів (№119 від 02.06.2008):

ПЦ та АКС членів та учасників НСМЕП мають той чи інший комплект серверів залежно від функцій, які виконує член/учасник НСМЕП. Режимні вимоги до приміщень, у яких розташовані сервери програмно-технічних комплексів залежать від розташування цих серверів.

До початку проведення інсталяції програмно-апаратного комплексу АКС/БПЦ наказом члена/учасника НСМЕП призначається відповідальна за засоби захисту НСМЕП особа – офіцер безпеки АКС/БПЦ члена/учасника НСМЕП. Копія цього наказу передається в управління захисту інформації Департаменту інформатизації.

До складу АКС банків - учасників НСМЕП та/або БПЦ входять робочі АРМ та такі сервери: СА, СБД, СЗ і БЦГКІ.

Залежно від своїх потреб член/учасник НСМЕП вибирає ту чи іншу конфігурацію для виконання функцій НСМЕП:

– Перша конфігурація - СА, СБД суміщений з СЗ та БЦГКІ, робочі АРМ. СА та СБД повинні розміщуватися в приміщенні з обмеженим доступом в екранованих шафах, обладнаних відповідно до вимог нормативно-правових актів Національного банку. СБД, суміщений з СЗ та БЦГКІ, повинен розміщуватися в приміщенні з обмеженим доступом, яке додатково обладнане сейфами (металеві міцні шафи) для зберігання резервних МБ, службових карток та відповідної документації. Доступ до цього приміщення має лише офіцер безпеки АКС члена/учасника НСМЕП.

– Друга конфігурація - СА, СБД, СЗ, суміщений з БЦГКІ, робочі АРМ. СА та СБД повинні розміщуватися в серверному приміщенні, яке обладнане відповідно до вимог нормативно-правових актів Національного банку. СЗ повинен розміщуватися в приміщенні з обмеженим доступом, яке додатково обладнане сейфами (металеві міцні шафи) для зберігання резервних МБ,

службових карток та відповідної документації. Доступ до цього приміщення має лише офіцер безпеки АКС члена/учасника НСМЕП.

– Третя конфігурація - основний та резервні СА, СБД, основний, суміщений з БЦГКІ, та резервні СЗ, робочі АРМ. Основні та резервні СА, СБД та резервні СЗ повинні розміщуватися в серверному приміщенні, яке обладнане відповідно до вимог нормативно-правових актів Національного банку. Основні та резервні сервери рекомендується розміщувати в різних серверних приміщеннях за наявності кількох обладнаних приміщень. Якщо немає іншого серверного приміщення, то рекомендується резервні сервери розміщувати в іншому приміщенні з обмеженим доступом в екранованих шафах, які відповідають вимогам нормативно-правових актів Національного банку. Основний СЗ повинен розміщуватися в приміщенні з обмеженим доступом, яке додатково обладнане сейфами (металеві міцні шафи) для зберігання резервних МБ, службових карток та відповідної документації. Доступ до цього приміщення має лише офіцер безпеки АКС члена/учасника НСМЕП.

– Четверта конфігурація - СА, СБД, СЗ, БЦГКІ, робочі АРМ. СА, СБД та СЗ повинні розміщуватися в серверному приміщенні, яке обладнане відповідно до вимог нормативно-правових актів Національного банку. БЦГКІ повинен розміщуватися в приміщенні з обмеженим доступом, яке додатково обладнане сейфами (металеві міцні шафи) для зберігання резервних МБ, службових карток та відповідної документації. Доступ до цього приміщення має лише офіцер безпеки АКС члена/учасника НСМЕП [10].

Висновки до першого розділу

Проведено дослідження системи електронних платежів як об’єкта інформаційної безпеки, а саме: 1. Проаналізовано поняття платіжних систем, класифікації та вимоги до них, структуру систем електронних платежів. 2. Розглянуто поняття міжбанківських інформаційних систем, вимоги та їх структура. 3. Досліджено СЕМП НБУ як об’єкт інформаційної безпеки, засади функціонування, структура та основні елементи.

2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ В СИСТЕМАХ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ

2.1. Аналіз загроз та ризиків СЕП

2.1.1. Найхарактерніші загрози інформації в платіжній системі

Інформація є ресурсом, який подібно іншим важливим бізнес-ресурсам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це важливо у все більш взаємопов’язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов’язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та вразливостей [11].

Під загрозою розуміється сукупність умов чинників, що створюють небезпеку несанкціонованого, в тому числі випадкового, доступу до інформації, результатом якого може стати знищення, зміна, блокування, копіювання, поширення інформації, загальна класифікація загроз наведена на рис. 2.1.

2.1.2. Проблеми криптографічного захисту платіжної системи

В умовах конкурентної боротьби збереження провідних позицій і залучення нових клієнтів можливо тільки за умови надання більшої кількості послуг і скорочення часу обслуговування. Цього можна досягти лише при забезпеченні необхідного рівня автоматизації всіх банківських операцій. У той же час застосування обчислювальної техніки не тільки вирішує виникнені проблеми, а й призводить до появи нових, нетрадиційних для банку загроз, пов'язаних з схильністю інформації до фізичного перекручення чи знищення, можливістю випадкової або умисної модифікації і небезпекою несанкціонованого отримання інформації особами, для яких вона не призначена.

Рис 2.1. Загальна класифікація загроз

У цих умовах на перший план виходять завдання захисту банківської інформації та, в тому числі, впровадження криптографічних засобів. Однак аналіз існуючого стану показує, що рівень заходів щодо захисту інформації, як правило, відстає від темпів автоматизації. Таке відставання може обернутися надзвичайно серйозними наслідками [12].

На підставі проведеного аналізу даних про застосовувані засобів криптографічного захисту можна сформулювати такі концептуальні положення з проблеми криптографічного захисту платіжної системи:

1. Система міжбанківських розрахунків в даний час практично не оснащена сертифікованими засобами криптографічного захисту та підтвердження справжності. Безпека банківської інформації багато в чому здійснюється охоронними і режимними заходами.

2. Існуючі організаційні і технічні заходи не забезпечують повноцінний захист від несанкціонованого підключення до мереж внутрішньобанківського і міжбанківського обміну.

3. Не вирішені до кінця питання захисту від навмисного або ненавмисного порушення цілісності банківської інформації, що зберігається в ЕОМ (внесення змін, знищення інформації і ряд інших).

4. Створення системи безпеки необхідно проводити одночасно з впровадженням телекомунікаційних систем і систем автоматизованої обробки банківської інформації.

5. Система криптографічного захисту інформації не повинна істотно впливати на технологію обробки банківських документів, повинна допускати їх автоматизовану обробку спільно з ЕЦП і не вносити значних часових затримок у процес обробки платежів.

6. Для криптографічної співпраці різних систем міжбанківських розрахунків криптографічний захист повинен будуватися на єдиних принципах і алгоритмах криптографічного перетворення і ЕЦП.

7. Засоби криптографічного захисту повинні мати різну реалізацію (програмну, програмно-апаратну, апаратну) і давати можливість користувачам

вибирати найбільш прийнятну для конкретних умов.

8. Засоби криптографічного захисту повинні бути максимально прості в експлуатації, з огляду на невисоку професійну підготовку операторського складу.

2.1.3. Модель можливих руйнівних дій зловмисника

Головним об'єктом нападу зловмисника є фінансові кошти, точніше платіжні доручення, що циркулюють в платіжній системі. По відношенню до даних засобів зловмисник може переслідувати наступні цілі:

1. Викрадення фінансових коштів.

2. Впровадження фальшивих фінансових коштів (порушення фінансового балансу системи).

3. Порушення працездатності системи (технічна загроза).

Зазначені об'єкти і цілі нападу носять абстрактний характер і не дозволяють провести аналіз і розробку необхідних заходів захисту інформації, тому в таблиці 1 наводиться конкретизація об'єктів і цілей руйнуючих дій зловмисника.

Таблиця 2.1.

Модель руйнівних дій зловмисника

Об'єкт впливу	Мета впливу	Можливі механізми реалізації впливу.
HTML-сторінки на web-сервері банку	Підміна з метою отримання інформації, що вноситься в платіжне доручення клієнтом.	Атака на сервер і підміна сторінок на сервері. Підміна сторінок в трафіку. Атака на комп'ютер клієнта і підміна сторінок у клієнта
Клієнтські інформаційні сторінки на сервері	Отримання інформації про платежі клієнта (ів)	Атака на сервер. Атака на трафік. Атака на комп'ютер клієнта.
Дані платіжного доручення, що вносяться клієнтом в форму	Отримання інформації, що вноситься в платіжне доручення клієнтом.	Атака на комп'ютер клієнта (віруси і т.д.). Атака на дані доручення при його пересиланні по трафіку. Атака на сервер.

Продовження таблиці 2.1.

Модель руйнівних дій зловмисника

Приватна інформація клієнта, розташована на комп'ютері клієнта і не відноситься до системи електронних платежів	Отримання конфіденційної інформації клієнта. Модифікація інформації клієнта. Виведення з ладу комп'ютера клієнта.	Весь комплекс відомих атак на комп'ютер, підключений до мережі Інтернет. Додаткові атаки, які з'являються в результаті використання механізмів платіжної системи.
Інформація процесингового центру банку.	Розкриття і модифікація інформації процесингового центру та локальної мережі банку.	Атака на локальну мережу, підключену до Інтернет.

З даної таблиці випливають базові вимоги, яким повинна задовольняти будь-яка система електронних платежів через Інтернет:

1.Система повинна забезпечувати захист даних платіжних доручень від несанкціонованого зміни і модифікації.

2. Система не повинна збільшувати можливості зловмисника по організації атак на комп'ютер клієнта.

3. Система повинна забезпечувати захист даних, розташованих на сервері від несанкціонованого читання і модифікації.

4. Система повинна забезпечувати або підтримувати систему захисту локальної мережі банку від впливу з глобальної мережі [13].

2.2. Основні методи захисту комерційної інформації

З початку впровадження електронної комерції стало очевидно, що методи ідентифікації власника карти, що застосовуються в звичайних транзакціях, є незадовільними для транзакцій ЕК.

Дійсно, при здійсненні операції купівлі у фізичному магазині продавець має можливість розглянути пропоновану для розрахунків пластикову карту на

предмет її відповідності вимогам платіжних систем (зокрема, перевірити наявність голограми, спеціальних секретних символів, звірити підпис на панелі підпису і торговому чеку і т. П.). Крім того, продавець може зажадати від покупця документ, що засвідчує його особу. Все це робить шахрайство з підробленою карткою досить дорогим заходом.

У разі транзакції ЕК все, що потрібно від шахрая - знання реквізитів картки. Витрати, пов'язані з виготовленням підробленої фізичної карти, в цьому випадку не потрібні. Безумовно, це не може не привернути увагу криміналу до цього типу комерції, свідками чого ми стаємо вже сьогодні.

У світі пластикових карт із магнітною смугою найнадійнішим способом захисту транзакції від шахрайства є використання PIN-коду для ідентифікації власника картки його банком-емітентом. Секретною інформацією, якою володіє власник карти, є PIN-код. Він являє собою послідовність, що складається з 4-12 цифр, відому тільки власнику картки і його банку-емітенту. PIN-код застосовується завжди при проведенні транзакцій підвищеного ризику, наприклад при видачі власнику карти готівки в банкоматах. Видача готівки в банкоматах відбувається без присутності представника обслуговуючого банку (ситуація схожа на транзакцію ЕК). Тому звичайних реквізитів картки для захисту операції «зняття готівки в банкоматі» недостатньо і використовується секретна додаткова інформація - PIN-код [14].

Більш того, загальна тенденція розвитку платіжних систем - більш активне використання PIN-коду для операцій «покупка» за дебетовими картками. Здавалося б, використання подібного ідентифікатора могло б допомогти вирішити проблему безпеки в ЕК, проте це не так. На жаль, в додатку до ЕК цей метод в класичному вигляді непридатний.

Дійсно, використання PIN-коду має проводитися таким чином, щоб цей секретний параметр на всіх етапах обробки транзакції залишався зашифрованим (PIN-код повинен бути відомий тільки власнику картки і її емітенту). У реальному світі це вимога реалізується за рахунок використання в пристроях введення транзакції спеціальних фізичних пристроїв, званих PIN-PAD і містять Hardware

Security Module - апаратно-програмні пристрої, що дозволяють зберігати і перетворювати деяку інформацію вельми надійним способом. Ці пристрої зберігають спеціальним способом захищений секретний комунікаційний ключ, згенерований обслуговуючим банком даного ТП. Коли власник карти вводить значення PIN-коду, воно негайно закривається (шифрується) комунікаційним ключем і відправляється всередині авторизаційного запиту на хост обслуговуючого банку. Точніше кажучи, шифрується не саме PIN-код, а деякий електронний «конверт», в який код поміщається. На хості обслуговуючого банку зашифрований ідентифікаційний код перекодується всередині Hardware Security Module хоста (хост обслуговуючого банку також має свій пристрій шифрування) в блок, зашифрований на комунікаційному ключі платіжної системи, і передається в мережу для подальшого пред'явлення емітенту. По дорозі до емітента PIN-код буде перетворюватися ще кілька разів, але для наших міркувань це не важливо. Важливо інше – для того, щоб слідувати класичною схемою обробки PIN-коду, кожен власник картки повинен зберігати криптограми комунікаційних ключів всіх обслуговуючих банків, що на практиці неможливо.

Класичну схему можна бито б реалізувати за допомогою застосування асиметричних алгоритмів шифрування PIN-коду власника карти відкритим ключем ТП. Однак для подання PIN-коду в платіжну мережу його необхідно зашифрувати, як це прийнято у всіх платіжних системах, симетричним ключем. Автор не знає жодного стандартного Hardware Security Module, здатного виконати трансляцію PIN-коду, зашифрованого за допомогою асиметричного криптоалгоритму, в PIN-код, зашифрований на симетричному алгоритмі шифрування.

Існує інше, некласична рішення по використанню PIN-коду. Наприклад, можна на комп'ютері власника карти шифрувати PIN-код плюс деякі динамічно мінливі від транзакції до транзакції дані на ключі, відомому тільки емітенту і власнику карти. Такий підхід вимагає рішення задачі розподілу секретних ключів. Це завдання є досить непростим (очевидно, що у кожного власника карти повинен бути свій індивідуальний ключ), і якщо вже вона вирішується, то

використовувати її рішення має сенс для інших, більш ефективний у порівнянні з перевіркою PIN-коду методів аутентифікації власника карти [15].

У той же час ідея перевірки PIN-коду побуту реалізована для підвищення безпеки транзакцій ЕК по картах, БД яких зберігається на хості процесора STB CARD. У загальних рисах STB CARD реалізує наступну схему. Власники карт, емітенти який тримають свою БД карток на хості STB CARD, можуть отримати додатковий PIN-код, званий ПІН2. Цей код є послідовністю з 16 шістнадцяткових цифр, яка роздруковується в PIN-конверті, переданому власнику карти (спеціальний паперовий конверт, який використовується банком-емітентом для зберігання в ньому секретної інформації, що відноситься до емітованої карті), і вираховується емітентом за допомогою симетричного алгоритму шифрування, застосованого до номера карти і використовує секретний ключ, відомий тільки емітенту карти.

Далі під час проведення транзакції ЕК на одному з ТП, яку обслуговує банком STB CARD, у власника карти в процесі отримання даний про клієнта запитується інформація за ПІН2. Клієнт вводить значення коду ПІН2 в яку заповнюють форму і повертає її ТП.

Тут потрібно зробити важливе зауваження щодо сказаного раніше. Власник карти в дійсності веде діалог в захищеній SSL-сесії не з ТП, а з віртуальним POS-сервером, через який працює ТП (система STB CARD в даний час використовує сервер Assist).

Повертаючись до схеми STB CARD, відзначимо, що, звичайно ж, в заповненій клієнтом формі ПИН2 не міститься, а в дійсності все виглядає наступним чином: ТП (точніше, сервер Assist), визначивши, що має справу з картою банку STB CARD, передає власнику карти форму, яка містить підписаний Java-аплет, який реалізує деякий симетричний алгоритм шифрування. При цьому ПИН2 грає роль секретного ключа цього алгоритму шифрування, а шифровані дані виходять в результаті застосування хеш-функції до номера карти, суму та дату транзакції, а також випадковим числа £, що генерується ТП. Таким чином, в заповненій власником карти формі присутній тільки результат шифрування

перерахованих вище даних про транзакції на ключі ПІН2.

Далі ТП формує авторизаційне повідомлення, передане на хост обслуговуючого банку, що містить крім «стандартних» даних про транзакції ще результат шифрування і випадкове число £.

Емітент карти, отримавши повідомлення ТП, за номером картки обчислює значення ПИН2, і далі за номером картки, суму та дату транзакції, а також за випадковим числу %, обчислює результат шифрування цих даних на ключі ПІН2. Якщо отримана величина збігається з аналогічною величиною з повідомлення ТП, верифікація PIN-коду вважається виконаним успішно. В іншому випадку транзакція відкидається.

Таким чином, технологія перевірки PIN-коду, прийнята в системі STB CARD, в дійсності забезпечує не тільки динамічну аутентифікацію клієнта, але ще і гарантує «наскрізну» цілісність деяких даних про транзакції (сума транзакції, номер карти). Під «наскрізний» цілісністю тут розуміється захист від модифікації даних на всьому протязі їх передачі від клієнта до банку-емітента.

Мінуси даного підходу полягають у наступному:

• Для реалізації схеми перевірки значення PIN-коду необхідно, щоб ТП «вміло» формувати відповідну форму з Java-ann-влітку, що відразу звужує сферу застосування схеми у відносно невеликому безлічі ТП.

• Використання довгого (шістнадцять шістнадцяткових цифр) ключа робить його застосування на практиці вкрай незручним для власника карти.

• Захист від підстановки (форма, яка запитує ПІН2, надається власнику картки не ТП, а шахраєм, бажаючим дізнатися значення ПИН2) заснована на надійності аутентифікації клієнтом сервера ТП, а також на підписуванні аплету секретним ключом сервера ТП. Оскільки порушення обох захистів призводить тільки до появи на екрані монітора власника карти відповідного попередження, супроводжуваного питанням - продовжити сесію чи ні, то особливо довіряти цим формам захисту не варто.

Забезпечити надійний захист від підставки можна за допомогою електронного гаманця клієнта (спеціального програмного забезпечення, яке

клієнт може «скачати» на свій комп'ютер з деякого сайту), що заміняє за своєю функціональністю Java-аплет в формі ТП. Такий електронний гаманець може використовувати як завгодно потужні засоби шифрування даних. Секретні ключі власника карти можуть триматися в порядку підвищення надійності їх зберігання на диску комп'ютера, дискеті або мікропроцесорної карті. Доступ до електронного гаманця повинен проводитися за паролем його власника.

В результаті проведеного аналізу платіжні системи сформували основні вимоги до схем проведення транзакції ЕК, що забезпечує необхідний рівень її безпеки. Ці вимоги зводяться до наступного:

• Аутентифікація учасників покупки (покупця, торгового підприємства і його обслуговуючого банку). Під аутентифікацією покупця (продавця) розуміється процедура, яка доводить (на рівні надійності відомих криптоалгоритмів) факт того, що даний власник карти дійсно є клієнтом деякого емітента-учасника (обслуговуючого банку-учасника) даної платіжної системи. Аутентифікація обслуговуючого банку доводить факт того, що банк є учасником цієї платіжної системи.

• Реквізити платіжної картки (номер картки, термін її дії, CVC2/CVV2 і т.п.), Що використовується при проведенні транзакції ЕК, повинні бути конфіденційними для ТП.

• Неможливість відмови від транзакції для всіх учасників транзакції ЕК, тобто наявність у всіх учасників незаперечного доказу факту здійснення покупки (замовлення або оплати).

• Гарантування магазину платежу за електронну покупку - наявність у ТП докази того, що замовлення було ТП виконаний.

Усюди далі під протоколом ЕК розуміється алгоритм, який визначає порядок взаємодії учасників ЕК (власника карти, торгового підприємства, обслуговуючого банку, банку-емітента та центру сертифікації) і формати повідомлень, якими учасники ЕК обмінюються один з одним з метою забезпечення процесів авторизації і розрахунків [16].

2.3. Стандарти електронних розрахунків

2.3.1. Протокол IPSec

IPSec (Internet Protocol Security) - система стандартів, спрямована на встановлення і підтримання захищеного каналу для передачі даних.

IPSec передбачає аутентифікацію при встановленні каналу, шифрування переданих даних і поширення секретних ключів, необхідних для роботи протоколів аутентифікації і шифрування. Засоби IPSec реалізують захист вмісту пакетів IP, а також захист від мережевих атак шляхом фільтрації пакетів і використання тільки надійних з'єднань.

Протоколи IPSec забезпечують захист мереж, використовуючи для цього криптографічні протоколи безпеки і динамічне управління ключами. Стек протоколів IPsec діє на мережевому рівні, захищаючи і аутентіфікуючи IP-пакети між пристроями, які беруть участь в з'єднанні. Він не прив'язаний до конкретних алгоритмам шифрування, аутентифікації і безпеки та технологій генерації ключів.

Служби безпеки IPsec:

Конфіденційність - шифрування даних, що передаються з метою їх захисту від несанкціонованого перегляду.

Цілісність даних - гарантує, що дані в процесі передачі через Інтернет не були змінені. IPsec гарантує цілісність даних за допомогою контрольних сум, простій перевірки по надмірності.

Аутентифікація - гарантує, що з'єднання встановлено з потрібним партнером. Одержувач може аутентифікувати джерело пакета, гарантуючи і сертифікуючи справжність джерела інформації.

Захист від повторення пакетів - гарантує, що кожен пакет унікальний і не дублюється. Захист пакетів IPsec забезпечується за рахунок порівняння номерів послідовності отриманих пакетів. Пакет з номером послідовності нижче ковзного вікна вважається запізнілими або дубльованим. Запізнілі або дубльовані пакети відкидаються

Протокол IPSec забезпечує стандартний спосіб шифрування трафіку на мережевому (третьому) рівні IP і захищає інформацію на основі наскрізного шифрування: незалежно від працюючого програми, шифрується кожен пакет даних, що проходить по каналу. Це дозволяє організаціям створювати в Інтернеті віртуальні приватні мережі. IPSec працює поверх звичайних протоколів зв'язку, підтримуючи DES, MD5 і ряд інших криптографічних алгоритмів [17].

Забезпечення інформаційної безпеки на мережевому рівні за допомогою IPSec включає:

1. Підтримку немодифікованих кінцевих систем;

2. Підтримку транспортних протоколів, відмінних від TCP;

3. Підтримку віртуальних мереж в незахищених мережах;

4. Захист заголовка транспортного рівня від перехоплення (запобігання несанкціонованого аналізу трафіку);

5. Захист від атак типу "відмова в обслуговуванні".

Крім того, IPSec має дві важливі переваги:

1. Його застосування не вимагає змін в проміжних пристроях мережі;

2. Робочі місця і сервери не обов'язково повинні підтримувати IPSec.

2.3.2. Протокол SSL

Сьогодні найбільш поширеним протоколом, використовуваним при побудові систем ЕК є протокол SSL.

Протоколи ЕК, засновані на використанні SSL, не підтримують аутентифікації клієнта Інтернет-магазином, оскільки сертифікати клієнта в таких протоколах майже не використовуються. Використання «класичних» сертифікатів клієнтами в схемах SSL є справою практично марні. Такий «класичний» сертифікат, отриманий клієнтом в одному з відомих центрів сертифікації, містить тільки ім'я клієнта і, що, вкрай рідко, його мережеву адресу (більшість клієнтів не має виділеної IP-адреси). У такому вигляді сертифікат мало чим корисний ТП при проведенні транзакції ЕК, оскільки може бути без великих труднощів отриманим і

шахраєм. Для того, щоб сертифікат клієнта що-небудь значив для ТП, необхідно, щоб він встановлював зв'язок між номером картки клієнта і його банком-емітентом. Причому будь-який Інтернет-магазин, в який звертається за покупкою власник карти з сертифікатом, повинен мати можливість перевірити цей зв'язок (можливо, за допомогою свого обслуговуючого банку).

Іншими словами, такий сертифікат повинен бути отриманий клієнтом в своєму банку-емітенті. Формат сертифіката, спеціальні процедури маскування номера карти в сертифікаті (очевидно, номер карти не повинен бути присутнім в сертифікаті у відкритому вигляді), процедури поширення і відкликання сертифікатів, а також багато іншого в цьому випадку має бути обумовлено між усіма учасниками транзакції ЕК. Інакше кажучи, потрібно створення ієрархічної інфраструктури центрів сертифікації . Без створення такої інфраструктури всі розмови про забезпечення взаємної аутентифікації учасників транзакції ЕК - нерозуміння суті питання.

Відсутність аутентифікації клієнта в схемах SSL є найсерйознішим недоліком протоколу, який дозволяє шахраєві успішно провести транзакцію, знаючи тільки реквізити карти. Тим більше, протокол SSL не дозволяє аутентифікувати клієнта обслуговуючим банком (аутентифікація клієнта обслуговуючим банком є важливим елементом захисту останнього від недобросовісних дій ТП і забезпечується протоколом SET).

При використанні протоколу SSL ТП аутентифікується тільки на свою адресу в Інтернеті (URL). Це означає, що клієнт, який здійснює транзакцію ЕК, не аутентифікує ТП (не отримує доказів існування договірних відносин між ТП і його обслуговуючим банком-учасником платіжної системи). Аутентифікація ТП тільки за URL полегшує шахрайським ТП доступ до різних систем ЕК. Зокрема, торговельні підприємства, що займаються збором інформації про картки клієнтів, можуть отримати сертифікат в будь-якому відомому центрі сертифікації загального користування (наприклад, Verisign, GTE, Thawte і т. П.) На підставі тільки своїх установчих документів, після чого дорога до шахрайства для них стає відкритою.

Справедливості заради треба сказати, що перевірка сертифіката сервера ТП проводиться тільки по URL сервера через те, що так влаштовані всі відомі браузери на робочих місцях клієнтів. Протокол SSL дозволяє передавати додатки, які працюють через браузер, інформацію, яка може аналізуватися цими додатками (наприклад ім'я власника сертифіката, час і дату початку встановлення сесії і т. П.). На основі аналізу отриманих даних додаток може втручатися в процес роботи протоколу (наприклад визнати аутентифікацію одного з учасників SSL-сесії неуспішною і перервати сесію). Щоб такий додатковий аналіз був можливий, потрібен спеціальний додаток, що використовує функціональність браузера. Такий додаток реалізується в рамках, так званого, електронного гаманця або гаманця клієнта - спеціального програмного забезпечення, призначеного для реалізації клієнтом електронної покупки.

Використання електронного гаманця крім того, що має на увазі деякі зусилля з боку клієнта (гаманець потрібно завантажити), а також наявність центру, що розподіляє такі гаманці, не вирішують проблему. Для вирішення проблеми потрібно ієрархічна інфраструктура центрів сертифікації. Легальність ТП повинна встановлюватися тільки перевіркою того факту, що сертифікат відкритого ключа ТП, який відповідає його закритому ключу, виданий обслуговуючим банком, що має всім відомий сертифікат платіжної системи.

Протокол SSL не підтримує цифрового підпису, що ускладнює процес розв'язання конфліктних ситуацій, які виникають в роботі платіжної системи . Для доказу проведення транзакції потрібно або зберігати в електронному вигляді весь діалог клієнта і ТП (включаючи процес встановлення сесії), що дорого з точки зору витрат ресурсів пам'яті і на практиці не використовується, або зберігати паперові копії, що підтверджують отримання клієнтом товару.

При використанні SSL не забезпечується конфіденційність даних про реквізити карти для ТП (як це, втім, відбувається і в транзакціях «купівля» в звичайних неелектронних ТП).

За правилами міжнародних платіжних систем Europay / MasterCard при використанні протоколу SSL транзакції по дебетових картках заборонені (VISA

прийняла рішення дозволити транзакції ЕК за дебетовими картками VISA / Electron).

Введемо таке визначення. Протокол ЕК називається стійким, якщо він забезпечує на рівні криптостійкості визнаних алгоритмів цифрового підпису та шифрування:

– аутентифікацію обслуговуючого банку торговим підприємством;

– конфіденційність повідомлень, якими обмінюються учасники ЕК через Інтернет;

– конфіденційність інформації про реквізити карти для ТП;

– цілісність даних, якими обмінюються учасники ЕК;

– неможливість відмови від транзакції (non-repudiation) - наявність для кожного учасника транзакції електронного практично незаперечного доказу факту здійснення транзакції.

Отже, протокол SSL не є стійким [18].

2.3.3. Авторизація, ідентифікація, аутентифікація

До засобів інформаційної безпеки, що використовуються банками, відносяться, авторизація, аутентифікація , ідентифікація, перевірка цілісності і призначені для захисту законних користувачів інформаційної системи від неправомірних дій зловмисників. Об'єктами і суб'єктами ідентифікації і аутентифікації можуть бути люди (абоненти кінцевих терміналів, оператори), технічні засоби, носії інформації, документи та ін.

Авторизація - операція перевірки дозволів та прав, наданих користувачеві. В ЕК в процесі авторизації може встановлюватися кредитоспроможність клієнта. До подальших операцій після авторизації клієнт допускається лише при наявності у нього необхідної для покупки товару або послуги суми грошей. Таку авторизацію здійснюють електронні платіжні системи.

Ідентифікація - це присвоєння будь-якого об'єкта чи суб'єкту унікального імені (Login, LoginName, UserName) або образу. З цього імені здійснюється

ототожнення істинного користувача при зверненні користувача до певного сервісу.

Аутентифікація - це підтвердження (встановлення) дійсності об'єкта або суб'єкта взаємодії в інформаційній мережі по висунутій ідентифікатором. Ідентифікатор - ім'я, під яким зареєстрований користувач в перевіряє його інформаційній системі. У процесі аутентифікації встановлюється правомірність користувача з'єднуватися з сервером, проводиться перевірка справжності абонента. Встановлюється, що повідомлення належить законному абоненту, а не зловмисникові. Для аутентифікації використовуються як програмні, так і апаратні засоби [19].

2.4. Основні механізми, методи та засоби КЗІ в СЕМП

2.4.1. Політики безпеки

Одним з найбільш вразливих місць в системі електронних платежів є пересилання платіжних та інших повідомлень між банками, між банком і банкоматом, між банком і клієнтом.

У відповідності до Стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010 керівництву банків пропонується процесний підхід до управління інформаційною безпекою, заохочує його користувачів робити наголос наважливості:

a) розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей інформаційної безпеки;

b) впровадження заходів безпеки та забезпечення їх функціонування для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків організації;

c) моніторингу та перегляді продуктивності та ефективності СУІБ (система управління інформаційної безпеки);

d) постійному вдосконаленні, основаному на об’єктивному вимірюванні.

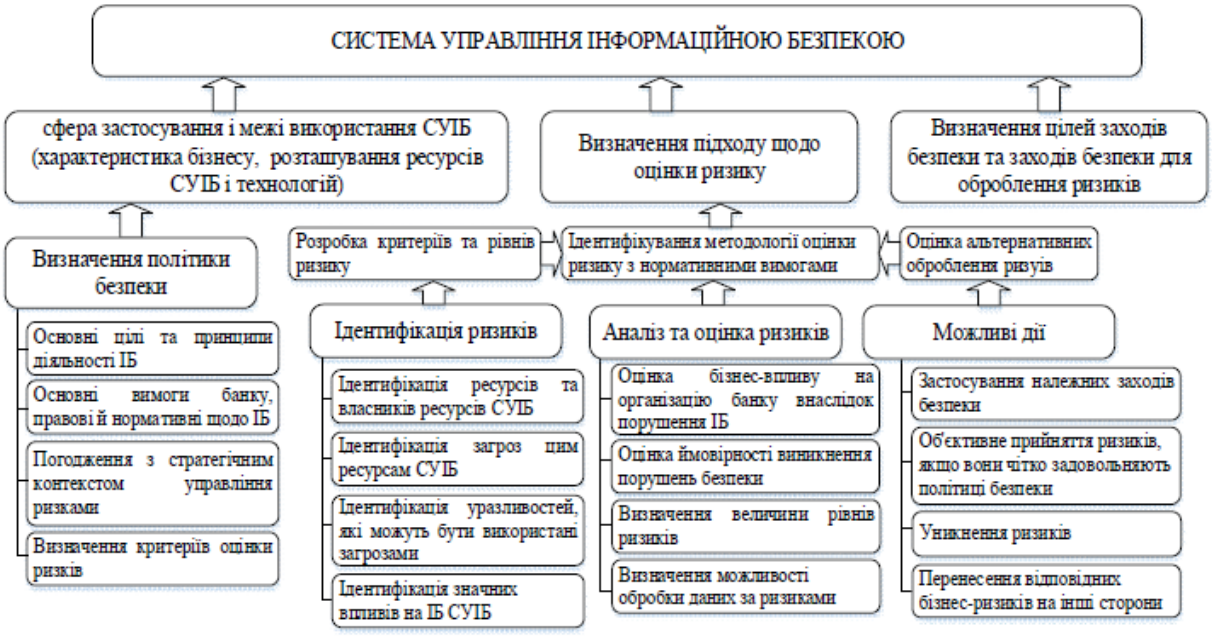

Рис.2.2. Етапи побудови СУІБ банку

Цей стандарт приймає модель “Плануй-Виконуй-Перевіряй-Дій” («Plan-Do-Check-Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ. СУІБ забезпечує вибір адекватних і взаємопов’язаних заходів безпеки, які убезпечують інформаційні ресурси СУІБ та гарантують конфіденційність зацікавленим сторонам [20].

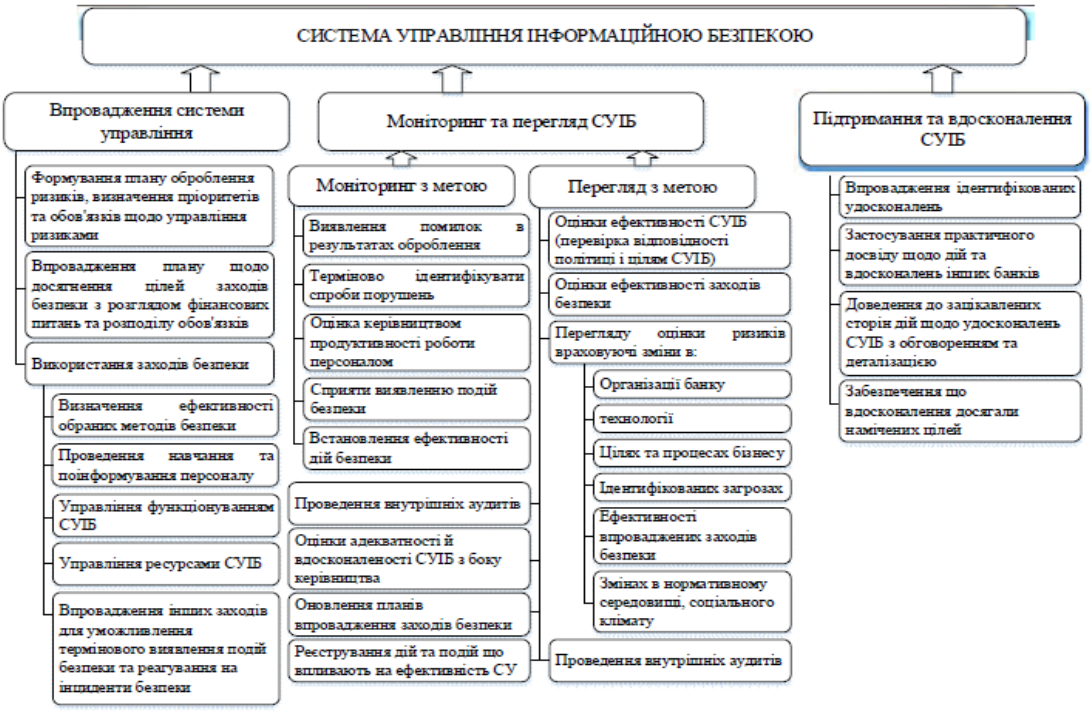

Рис.2.3. Основні функції СУІБ банку

Основні етапи побудови СУІБ банку наведені на рис. 2.2. Проведений аналіз основних вимог стандарту визначає основні функції системи управління ІБ, які наведені на рис. 2.3.

2.4.2. Основні механізми КЗІ

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

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

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

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

При роботі засобів криптування банківської інформації ведеться шифрований архів банківських платежів, де зберігаються всі зашифровані та відправлені, а також одержані та дешифровані платежі. Дешифрування повідомлень архіву можливе лише за наявності ключа, який знаходиться в Службі

захисту електронних банківських документів Національного банку. Наприкінці робочого дня цей шифрований архів треба обов'язково переписати на гнучкі магнітні носії. Він використовується для надання інформаційно-арбітражних послуг, які надає Служба захисту електронних банківських документів Національного банку відповідно до «Положення про інформаційно-арбітражні послуги служби захисту електронних банківських документів у СЕП».

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

- ім'я абонента, який відправив (зашифрував) електронний платіжний документ;

- ім'я абонента, якому адресовано електронний платіжний документ;

- дату, годину та хвилину, коли виконувалося шифрування електронного платіжного документа;

- дату, годину та хвилину, коли та ким виконувалося дешифрування електронного платіжного документа.

При використанні апаратних засобів захисту додатково визначається:

- номер апаратури захисту, на якій виконувалось шифрування (дешифрування) електронного платіжного документа;

- номер електронної картки, якою користувались під час шифрування (дешифрування) електронного платіжного документа.

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

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

технологічних запобіжних заходів.

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

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

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

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

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

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

При генерації ключів таємний ключ записується на дискету або на touch-memory. Відкриті ключі, які використовуються всередині банку (наприклад, ключі

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

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

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

регламентують порядок роботи фахівців банківських установ із засобами захисту, використання та зберігання криптографічних ключів, розподіл повноважень щодо питань захисту інформації в банківській установі.

У головних вузлах збору, обробки та зберігання інформації в системі (Центральнарозрахункова палата, регіональні розрахункові палати тощо) повинні вживатися заходи для захисту інформації від витоку технічними каналами. В усіх приміщеннях, де розташовані сервери системи, включаючи телекомунікаційні, постійно ведеться контроль за дотриманням визначеного комплексу організаційно-технічних заходів щодо порядку обстеження цих приміщень для контролю за витіканням інформації технічними каналами (лінії живлення, заземлення, допоміжні технічні засоби, електромагнітне випромінювання обчислювальних машин). Спеціальні вимоги щодо дотримання режимних умов у приміщеннях банківських установ -учасників СЕП, де обробляються, працюють та зберігаються засоби захисту, зазначені у «Положенні проміж банківські розрахунки в Україні» і обов'язкові для усіх банківських установ. Усі службові особи, які виконують електронні розрахунки, зобов'язані суворо дотримуватися цих вимог. Відповідальність за виконання вищезгаданих вимог покладено на керівників банківських установ [21].

2.4.3. Вибір системи шифрування

Криптографічні методи захисту інформації – це методи захисту даних із використанням шифрування

Головна мета шифрування (кодування) інформації - її захист від несанкціонованого читання. Системи криптографічного захисту (системи шифрування інформації) для банківських on-line -сисгем можна поділити за різними ознаками:

– за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);

– за способом реалізації (апаратний, програмний, програмно-апаратний);

– за криптографічними алгоритмами, які використовуються (загальні, спеціальні);

– за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувача);

– за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо.

Вбудовані механізми криптографічного захисту входять до складу системи, їх створюють одночасно з розробленням банківської on-line-системи. Такі механізми можуть бути окремими компонентами системи або бути розподіленими між іншими компонентами системи.

Додаткові механізми криптозахисту - це додаткові програмні або апаратні засоби, які не входять до складу системи. Така реалізація механізмів криптозахисту має значну гнучкість і можливість швидкої заміни. Для більшої ефективності доцільно використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту.

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним. Апаратна реалізація криптографічного захисту - найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передачі в апаратуру може бути виконана за допомогою спеціально розроблених програм типу "вірус".

Програмна реалізація криптографічного захисту значно дешевша та гнучкіша в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від "вірусних" атак, потрібно вжити заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, що використовувались під час роботи програм "збирання сміття".

Крім того, можна використовувати комбінацію апаратних і програмних механізмів криптографічного захисту. Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, вибираючи апаратні засоби для зберігання криптографічних ключів, треба пам'ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм - це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв’язаного (шифрованого) тексту.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптоалгоритми мають таємний алгоритм шифрування, а загальні криптоалгоритми характерні повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхня висока криптостійкість доведена. Ці алгоритми оприлюднюють для обговорення, при цьому навіть визначається премію за успішну спробу його "злому". Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою відповідно до збільшення довжини ключа.

Є дві великі групи загальних криптоалгоритмів: симетричні і асиметричні. До симетричних криптографічних алгоритмів належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник, і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість обробки як для апаратної, так і

для програмної реалізації. Основним їх недоліком є труднощі, пов'язані з дотриманням безпечного розподілу ключів між абонентами системи. Для асиметричних криптоалгоритмів шифрування і розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостій-кості алгоритму і не дає можливості відновлення парного йому ключа.

Усі криптографічні алгоритми можна використовувати з різними цілями, зокрема:

• для шифрування інформації, тобто приховування змісту повідомлень і даних;

• для забезпечення захисту даних і повідомлень від модифікації.

З найпоширеніших методів шифрування можна виділити американський алгоритм шифрування DES (Data Encryption Standart, розроблений фахівцями фірми IBM і затверджений урядом США 1977 року) із довжиною ключа, що може змінюватися, та алгоритм ГОСТ 28147-89, який був розроблений та набув широкого застосування в колишньому СРСР і має ключ постійної довжини. Ці алгоритми належать до симетричних алгоритмів шифрування.

Алгоритм Потрійний DES був запропонований як альтернатива DES і призначений для триразового шифрування даних трьома різними закритими ключами для підвищення ступеня захисту.

RC2, RC4, RC5 - шифри зі змінною довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Здатні підвищувати ступінь захисту через вибір довшого ключа.

IDEA (International Data Encryption Algoritm) призначений для швидкої роботи в програмній реалізації.

Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується.

Алгоритм RSA дозволяє виконувати шифрування в різних режимах:

• за допомогою таємного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;

• за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;

• за допомогою таємного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Але не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Другою метою використання криптографічних методів є захист інформації від модифікації, викривлення або підробки. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена. Для симетричних алгоритмів шифрування така додаткова інформація - це код автентифікації, який формується за наявності ключа шифрування за допомогою криптографічних алгоритмів.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву електронний цифровий підпис. Формуючи електронний цифровий підпис, виконують такі операції:

• за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;

• отримане значення хеш-функції шифрується: а) таємним або відкритим; б) таємним і відкритим ключами відправника і отримувача повідомлення - для алгоритму RSA

• використовуючи значення хеш-функції і таємного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису, - наприклад, для російського стандарту Р.31-10.

Для того, щоб перевірити цифровий підпис, потрібно:

• виходячи із значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;

• обчислити хеш-функцію з тексту повідомлення;

• порівняти ці значення. Якщо вони збігаються, то повідомлення не було модифікованим і відправлене саме цим відправником [22].

2.4.4. Механізм розподілу ключів

Останнім часом використання електронного цифрового підпису значно поширюється, у тому числі для регулювання доступу до конфіденційної банківської інформації та ресурсів системи, особливо для on-line -систем реального часу.

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

1. Метод базових/сеансових ключів. Такий метод описаний у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключів потребує значного часу і значних затрат.

2. Метод відкритих ключів. Такий метод описаний у стандарті ISO 11166 і може бути використаний для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих

ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує "абсолютного" захисту інформації, але гарантує, що вартість "злому" у кілька разів перевищує вартість зашифрованої інформації [23].

Щоб використовувати систему криптографії з відкритим ключем, потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. (Респондент – особа або сукупність осіб, які підлягають статистичному спостереженню у встановленому законодавством порядку).

Найнадійніший спосіб розповсюдження відкритих ключів - через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат – це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності.

2.4.5. Технологія накладання/перевірки ЕЦП у СЕМП

Для забезпечення захисту інформації від модифікації з одночасною суворою автентифікацією та безперервного захисту платіжної інформації та інших інформаційних задач з часу її формування система захисту СЕМП включає механізми формування перевірки ЕЦП на базі несиметричного алгоритму RSA. Для забезпечення конфіденційності інформація СЕМП, що циркулює в інформаційній мережі, має пройти обробку АРМ-НБУ або АРМ-СТП. Програмно-апаратний комплекс АРМ-НБУ є єдиним шлюзом до всіх задач файлового обміну

інформацією Національного банку. Генерація ключової інформації для апаратури захисту, Її транспортування, контроль за Її обліком і використанням, контроль за використанням апаратури захисту, техніко-експлуатаційне обслуговування та ремонт апаратури захисту, а також сертифікація відкритих ключів покладаються лише на службу захисту інформації Національного банку.

Технологія накладання/перевірки ЕЦП у СЕМП створена таким чином, щоб одна службова особа не мала змоги відіслати міжбанківський електронний розрахунковий документ. Під час формування міжбанківського електронного розрахункового документа на робочому місці операціоніста службова особа, яка формує цей документ, має накладати ЕЦП на документ за допомогою свого таємного ключа. Під час формування файла міжбанківських електронних розрахункових документів на робочому місці бухгалтера накладається ЕЦП на цей файл, що забезпечує захист від модифікації файла в цілому. Сформований таким чином платіжний файл обробляється АРМ-НБУ, де виконується перевірка ЕЦП операціоніста на кожному міжбанківському електронному розрахунковому документі та накладається ЕЦП АРМ-НБУ, який можуть перевірити всі банківські установи - учасники СЕП. Під час оброблення платіжних файлів на АРМ-2 виконується перевірка підписів на файлі в цілому та після формування файлів відповідних платежів накладається ЕЦП на файл у цілому за допомогою таємного ключа АРМ-2. Під час отримання відповідних платіжних файлів виконується аналогічна перевірка/накладання ЕЦП до часу остаточного оброблення документів операціоністом. Така технологія оброблення міжбанківських електронних розрахункових документів використовується також і в СТП [24].

Ця технологія обробки платежів у банківській установі забезпечує надійний розподіл доступу під час обробки міжбанківських електронних розрахункових документів та захист цих документів від модифікації в локальній мережі банку. Виконання технології використання ЕЦП на всіх етапах оброблення міжбанківських електронних розрахункових документів є обов'язковою вимогою для всіх типів САБ, які працюють у банківських установах, незалежно від моделі обслуговування консолідованого кореспондентського рахунку.

2.4.6. Засоби створення захищених каналів передачі інформації

Дуже широке поширення за останні роки отримали локальні і глобальні комп'ютерні мережі на основі комунікаційної архітектури TCP / IP. Одна з причин популярності TCP / IP - добре розроблена система функцій захисту інформації, закріплена рекомендаціями серії RFC, які публікуються міжнародною організацією IETF (Intemet Engineering Task Force). У зв'язку з цим вони є основною нормативно-технічної базою реалізації інформаційних систем, призначених для цілей електронної комерції.

У мережах, заснованих на архітектурі TCP/IP, найбільшого поширення набули два методи реалізації захищених каналів передачі інформації. Один з них - застосування стандартних механізмів і протоколів захисту інформації, що визначаються архітектурою безпеки IPSec. Це рамкова модель (frame-work) включає чотири компоненти:

1) протокол AH - Authentication Header;

2) протокол ESP - Encapsulating Security Payload;

3) протокол IPcomp -IP payload compression;

4) рамкову модель IKE- Intemet Key Exchange.

Для кожного з них (що займають своє місце серед протоколів комунікаційної архітектури TCP / IP) описуються формати, заголовки, специфічні криптографічні механізми і режими їх застосування. Архітектура IPSec додає до IP-пакетів перевірку цілісності, дійсності (автентичності), шифрування і захист від повтору пакетів. Вона використовується для забезпечення безпеки з'єднань між кінцевими користувачами і для створення захищених тунелів між шлюзами [25].

Архітектура IPSec була створена для забезпечення здатності до взаємодії. При коректній реалізації вона не робить ніякого впливу на мережі і хости, які не підтримують її. Модель не залежить від використовуваних криптографічних алгоритмів і допускає включення нових алгоритмів у міру їх появи.

Висновки до другого розділу

1. Проведено аналіз загроз та ризиків в СЕП;

2. Встановлено, що безпека платіжної системи може бути досягнута за рахунок застосування захищених протоколів, які представляють набір сервісів для шифрування і автентифікації. Кожен протокол розміщується на певному рівні (мережному, транспортному, прикладному). Було виділено наступні великі захищені протоколи IPsec, SSL.

3. Визначено, щоб виключити роботу в рамках інформаційної системи незаконних користувачів, необхідні процедури авторизації, ідентифікації, автентифікації.

4. Досліджено, що ефективний захист комерційної інформації повинен передбачати цілу систему напрямків діяльності, кожному з яких відповідає свій метод захисту.

5. Використання різних криптографічних алгоритмів на різних етапах обробки електронних банківських документів дає змогу забезпечити безперервний захист інформації в інформаційній мережі (під час передавання за допомогою телекомунікаційних каналів зв’язку), а також відокремлену обробку інформації стосовно різних задач інформатизації Національного банку.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННИХ МІЖБАНКІВСЬКИХ ПЛАТЕЖІВ

3.1. Аналіз законодавчої бази до системи захисту інформації СЕП

3.1.1. ISO/IEC 27002:2005, MOD): СОУ Н НБУ 65.1 СУІБ 1.0:2010

Стандарт ISO/IEC 27002:2005, є модифікацією стандарту ISO/IEC 17799:2005, та являє собою частину стандарту НБУ: СОУ Н НБУ 65.1 СУІБ 1.0:2010.

Цей стандарт створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою. Прийняття СУІБ повинне бути стратегічним рішенням для організації. На проектування та впровадження СУІБ організації впливають потреби та цілі організації, вимоги безпеки, застосовувані процеси, розмір і структура організації. З часом очікуються зміни цих факторів і систем, які їх підтримують. Передбачається, що впровадження СУІБ буде масштабуватися відповідно до потреб організації, наприклад, проста ситуація потребує простого рішення для СУІБ.

Доповнення Цей стандарт розроблений для банків України і має використовуватися усіма банками України та їх підрозділами Рекомендується створювати єдину систему управління інформаційною безпекою для банку в цілому.

Цей стандарт приймає процесний підхід до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ організації [26].

Для ефективної діяльності організації необхідно ідентифікувати та управляти багатьма видами діяльності. Будь-яку діяльність, що використовує ресурси та підлягає управлінню з метою забезпечення перетворення вхідних

даних у вихідні, можна розглядати як процес. Часто вихідні дані одного процесу є безпосередньо вхідними даними для наступного.

Застосування системи процесів у межах організації разом з ідентифікацією цих процесів та їх взаємодіями, а також управління ними можна розглядати як «процесний підхід».

Процесний підхід до управління інформаційною безпекою, запропонований цим стандартом, заохочує його користувачів робити наголос на важливості:

a) розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей інформаційної безпеки;

b) впровадження заходів безпеки та забезпечення їх функціонування для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків організації;

c) моніторингу та перегляді продуктивності та ефективності СУІБ; і

d) постійному вдосконаленні, основаному на об’єктивному вимірюванні.

Цей стандарт приймає модель «Плануй-Виконуй-Перевіряй-Дій» («PlanDo-Check-Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ.

Плануй (розробляй Розробити політику СУІБ, цілі, процеси та процедури, СУІБ) суттєві для управління ризиком та вдосконалення інформаційної безпеки для отримання результатів, які відповідають загальним політикам та цілям організації.

Виконуй (впроваджуй Впровадити та забезпечити функціонування політики та забезпечуй інформаційної безпеки, заходів безпеки, процесів та функціонування СУІБ) процедур СУІБ.

Перевіряй (здійснюй Оцінювати і, за можливості, вимірювати продуктивність моніторинг та процесів згідно з політикою, цілями СУІБ і практичним перегляд СУІБ) досвідом та звітувати про результати керівництву для перегляду.

Дій (підтримуй та Вживати коригувальні та запобіжні дії на підставі ревдосконалюй СУІБ) зультатів внутрішнього аудиту і перегляду СУІБ з боку

керівництва або іншої важливої інформації для досягнення постійного вдосконалення СУІБ.

Цей стандарт узгоджено із стандартами ISO 9001:2000 та ISO 14001:2004 з метою підтримки послідовного та комплексного впровадження і функціонування разом з іншими пов’язаними стандартами управління. Таким чином, одна відповідним чином запроектована система управління може задовольняти вимоги всіх цих стандартів.

Цей стандарт розроблено для надання змоги організації узгодити свою СУІБ з відповідними вимогами системи управління або інтегрувати її в них.

Національний банк України не вимагає від банків отримання сертифіката відповідності міжнародному стандарту ISO/IEC 27001. Такий сертифікат банк може отримати за власним бажанням [27].

3.2. Принципи побудови системи захисту інформації банківських організацій згідно Положення «Про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України»

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 асиметричних алгоритмів RSA та Національного стандарту України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих", затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої

політики.

Організація для забезпечення захисту інформації зобов'язана мати трибайтний унікальний ідентифікатор.

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 асиметричних алгоритмів RSA та ДСТУ 4145-2002 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 безпеки для сертифікації (крім ВК для робочих місць операціоністів, що використовуються лише в САБ) [28].

Департамент 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 безпеки надає криптобібліотеки безкоштовно всім організаціям, які використовують ЗЗІ, для вбудовування в програмне забезпечення САБ або інше відповідне програмне забезпечення [30].

3.3. Рекомендації щодо використання заходів інформаційної безпеки в СЕП згідно чинних стандартів

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.

Рекомендації щодо організації внутрішнього контролю за станом інформаційної безпеки:

Організація для забезпечення захисту інформації 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 [29].

Для мінімізації втрат від помилок в роботі з інформаційною системою зазвичай робляться такі заходи.

По-перше, проводиться продумана і задокументована політика контролю за інформаційними ресурсами в банку, яка повинна визначати типи основних документів, умови та види контролю за їх проходженням. Можна виділити наступні принципи, що визначають політику контролю:

– Додатковий візуальний контроль документів на великі суми (понад деякого заздалегідь встановленого рівня);

– Угруповання документів у пачки не більше ніж по 30-40 штук;

– Паралельне незалежне введення ключових реквізитів всіх (або хоча б зовнішніх) платіжних документів.

По-друге, система налаштовується відповідно до прав користувача, тобто його доступ до проведення операцій повинен бути обмежений певними умовами та контрольованими параметрами.

По-третє, вводиться чітка регламентація дій співробітників у разі помилкових операцій.

По-четверте, регулярно проводиться підвищення кваліфікації співробітників, що використовують комп'ютерну техніку.

Однак, в повному обсязі ці заходи рідко застосовуються, незважаючи на те, що втілення їх в життя необхідно. Основні причини – висока трудомісткість і відсутність відповідних процедур в програмному забезпеченні інформаційної системи банку. Подібними процедурами при побудові системи захисту зазвичай нехтують, особливо в невеликих банках, де витрати на автоматизацію невисокі.

Вимоги щодо захисту інформації від несанкціонованого доступу спрямовані на досягнення (в певному поєднанні) трьох основних властивостей інформації, що захищається:

- конфіденційність (засекречена інформація повинна бути доступна тільки тому, кому вона призначена);

- цілісність (інформація, на основі якої приймаються важливі рішення, повинна бути достовірною і точною і повинна бути захищена від можливих

ненавмисних і злочинних спотворень);

- готовність (інформація і відповідні інформаційні служби повинні бути доступні, готові до обслуговування завжди, коли в них виникає необхідність).

В основі контролю доступу до даних лежить система розмежування доступу між користувачами АБС і інформацією, що обробляється системою. Для успішного функціонування будь-якої системи розмежування доступу необхідне рішення двох завдань.

1. Зробити неможливим обхід системи розмежування доступу діями, які перебувають в рамках обраної моделі:

2. Гарантувати ідентифікацію користувача, що здійснює доступ до даних (автентифікація користувача).

Одним з ефективних методів збільшення безпеки АБС є реєстрація. Система реєстрації і обліку, відповідальна за ведення реєстраційного журналу, дозволяє простежити за тим, що відбувалося в минулому, і відповідно перекрити канали витоку інформації. У реєстраційному журналі фіксуються всі здійснені або нездійснені спроби доступу до даних або програм. Зміст реєстраційного журналу може аналізуватися як періодично, так і безперервно.

У реєстраційному журналі ведеться список всіх контрольованих запитів, здійснюваних користувачами системи.

Система реєстрації і обліку здійснює:

- реєстрацію входу (виходу) суб'єктів доступу в систему (з системи) або реєстрацію завантаження і ініціалізації операційної системи і її програмного зупину (реєстрація виходу з системи або зупинки не проводиться в моменти апаратного відключення), причому в параметрах реєстрації зазначаються: час і дата входу (виходу) суб'єкта доступу в систему (з системи) або завантаження (зупинки) системи; результат спроби входу - успішний або неуспішна (при спробі несанкціонованого доступу), ідентифікатор (код або прізвище) суб'єкта, який пред'являється при спробі доступу;

- реєстрацію та облік видачі друкованих (графічних) документів на тверду копію;

- реєстрацію запуску (завершення) програм і процесів (завдань, задач), призначених для обробки захищаються файлів;

- реєстрацію спроб доступу програмних засобів (програм, процесів, завдань, завдань) до захищених файлів;

- облік всіх носіїв інформації, що захищаються, за допомогою їх будь-якого маркування (облік носіїв, що захищаються, повинен проводитися в журналі (картотеці) з реєстрацією їх видачі / прийому, має проводитися кілька видів обліку (дублюючих) носіїв інформації, які захищаються).

Висновки до третього розділу

1. Відзначено, що кожну систему обробки інформації захисту слід розробляти індивідуально з огляду на такі особливості:

– організаційну структуру банку;

– обсяг і характер інформаційних потоків (всередині банку в цілому, всередині відділів, між відділами, зовнішніх);

– кількість і характер виконуваних операцій: аналітичних та повсякденних;

– кількість і функціональні обов'язки персоналу;

– кількість і характер клієнтів;

– графік добового навантаження.

2. Досліджено, що захист АБС повинен розроблятися для кожної системи індивідуально, але відповідно до загальних правил. Побудова захисту передбачає наступні етапи:

– аналіз ризику, який закінчується розробкою проекту системи захисту і планів захисту, безперервної роботи і відновлення;

– реалізація системи захисту на основі результатів аналізу ризику;

– постійний контроль за роботою системи захисту і АБС в цілому (програмний, системний і адміністративний).

3. Встановлено, що на кожному етапі реалізуються певні вимоги до захисту; їх точне дотримання призводить до створення безпечної системи.

ВИСНОВКИ

Проведені в роботі дослідження направлені на підвищення стану захищеності систем електронних міжбанківських платежів шляхом використання криптографічних методів та засобів захисту інформації.

У ході вирішення поставлених задач отримано наступні результати:

– Сформульовано особливості СЕМП як об’єкта інформаційної безпеки, проведено аналіз основних загроз, уразливостей та ризиків СЕП;

– Визначено основані принципи розробки рекомендацій щодо побудови та реалізації захисту СЕМП на основі використання захищених протоколів електронних розрахунків SSL, IPSec, механізму ЕЦП, засобів ідентифікації, автентифікації і авторизації;

– Запропоновано рекомендації щодо реалізації криптографічних механізмів захисту для забезпечення внутрішньої та зовнішньої безпеки СЕМП на основі розмежування доступу, контролю цілісності, використання технології ЕЦП, аналізу захищеності, криптографічного захисту, адміністрування СЕМП та використання системи захищеної електронної пошти.

Отримані результати доцільно до використання при розробці, впровадженні та експлуатації систем захисту інформації у СЕМП.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вимоги до технічних засобів, що входять до складу автоматизованої карткової системи (АКС) НСМЕП НБУ

2. Гайкович Ю.В., Першин А.С. Безопасность электронных банковских систем./ Ю.В. Гайкович, А.С. Першин — М.: Единая Европа, 1994. – 354 с.

3. Голдовский И.В. Безопасность платежей в Интернете – С-П.: Москва-Харьков-Минск, 2001

4. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

5. Деднев М.А., Дыльнов Д.В., Иванов М.А. Защита информации в банковском деле и электронном бизнесе./ М.А. Деднев, Д.В. Дыльнов, М.А. Иванов – М.: НОУ «ОЦ КУДИЦ-ОБРАЗ», 2004. – 512 с.

6. Демин В.С. и др. Автоматизированные банковские системы./ В.С. Демин и др. — М.: Менатеп-Информ, 1997. – 325 с.

7. Диффи У. Защищенность и имитостойкость / У. Диффи, М. Хеллман // Введение в криптографию. - 1979. - № 3. - С. 79-109

8. Дорошенко А.Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах: учебн. пособ./ А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с.

9. Евсеев С.П. Механизмы обеспечения аутентичности банковских данных во внутриплатежных системах коммерческого банка / С.П. Евсеев, В.Е. Чевардин, С.А. Радковский // Збірник наукових статей ХНЕУ. - Х.: ХНЕУ, 2008. - Вип. 6. - С. 40 - 44.

10. Єрьоміна Н.В. Банківські інформаційні системи: Навч. Посібник. – К.: КНЕУ, 2000. – 170-210с.

11. Задірака, В. К. Методи захисту банківської інформації [Текст] / В. К. Задірака, О. С. Олесюк, Н. О. Недашковський. – К.: Вища школа, 1999. – 264 с.

12. Закон України «Про банки і банківську діяльність» від 7 грудня 2000

року № 2121-III (із змінами та доповненнями)

13. Закон України "Про захист інформації в автоматизованих системах": Закон України від 05.10.94 № 80/94-ВР // Відомості Верховної Ради України. - 1994. - № 31. - Ст. 286.

14. Запечников С. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2007. – 320 с.

15. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD): СОУ Н НБУ 65.1 СУІБ 1.0:2010 [Текст]. – К.: НБУ, 2010. – 209 с.

16. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. 368 с.

17. Иванов М.А. Криптографические методы защиты в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

18. Інструкція про міжбанківський переказ грошей в Україні в національній валюті(№110 від 17.03.2004)

19. Корченко А.А. Банківська безпека / А. А. Корченко, Л. Н. Скачек, В. А. Хорошко. – Київ, 2014. – 185 с.

20. Мао Венбо. Современная криптография. Теория и практика: Пер. с англ. – М.: Изд. дом «Вильямс», 2005. – 786 с.

21. Ленков С.В, Перегудов Д,А., Хорошко В.А. Методі и средства защиты информации. В 2-х томах.- К: Арий, 2008-Том I. Несанкционированное получение информации.

22. Міжбанківські розрахунки в Україні [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua/control/uk/ publish/

23. Олійник А.В., Шацька В.М. Інформаційні технології у фінансових установах: Навчальний посібник. – Львів: “Новий Світ-2000”, 2007. – 436 с.

24. ПОЛОЖЕННЯ про захист інформації в Національній системі масових електронних платежів (№119 від 02.06.2008)

25. Постанова Про затвердження «Вимог Національного банку України

до програмного комплексу «Операційний день банку»»(N 106 від 12.05.95)

26. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD) [Текст]. – К.: НБУ., 2010. – 67 с.

27. Чмора А.Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2001, 256с.

28. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ, 2002. – 816 с.

29. Security of Internet Banking – A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Electronic resource]. – Available at: http://www.thailawforum.com/articles/internet-banking-thailand.htm

30. Національний банк України [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua/.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)