Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпропетровський державний аграрно-економічний університет

№ 10, 2014

УДК 338

Ю. П. Макаренко,
д. е. н., професор кафедри банківської справи, Дніпропетровський національний університет ім. О. Гончара, м. Дніпропетровськ

ВИКОРИСТАННЯ МІЖНАРОДНОЇ ЕЛЕКТРОННОЇ МЕРЕЖІ МІЖБАНКІВСЬКИХ РОЗРАХУНКІВ SWIFT

U. P. Makarenko,
Doctor of Economics, Professor, Department of Banking, Dnipropetrovsk National University named after O. Gonchar, Dnipropetrovsk

USING INTERNATIONAL ELECTRONIC NETWORK OF THE INTERBANK SETTLEMENTS SWIFT

У статті розглянуто застосування міжнародної електронної мережі SWIFT по передачі і обробці даних для виконання міжбанківських розрахунків та наведені її особливості. Запропоновано для захисту повідомлень при їхній передачі по лінії зв'язку до пункту допуску використовувати схему підключення за допомогою спеціальних пристроїв шифрування, погоджених з SWIFT.

This paper describes the application of the international SWIFT electronic network for transmission and processing of data for the performance of interbank payments and listed its features. Proposed to protect messages during their transmission on a communication line to the point of admittance to use diagram using special encryption devices, agreed with SWIFT.

Ключові слова: *інформаційна мережа, мережа передачі банківських даних SWIFT, міжнародні міжбанківські розрахунки , банківська інформація, старт-картка.*

Keywords: *information network, data transmission network of SWIFT banking, international interbank payments, banking information, start-card.*

ВСТУП

На сучасні інформаційні мережі покладається навантаження по передачі і обробці даних у багатьох сферах людської діяльності на національних і міжнародних рівнях. Сюди належать виробництво, управління, торгівля, банківська діяльність, міжурядові зв'язки, матеріально-технічне постачання, пошук злочинців. Крім того, такі мережі об'єднують бази даних для наукових досліджень, дають змогу здійснювати резервування квитків у глобальному масштабі (в тому числі на авіалініях, залізниці, морському транспорті), накопичують дані про стан навколишнього середовища. Інформаційні мережі передачі даних не дублюють наявну розгалужену комутаційну мережу телефону і телеграфу. Незважаючи на гігантські розміри світової телефонної мережі, вона не може впоратись із зростаючими інформаційними потоками, особливо ділової інформації. Це навантаження беруть на себе мережі передачі даних, які є новим кроком у розвитку інформаційних технологій, і потребують подальшого ґрунтовного дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика створення мережі передачі і обробки даних та розвитку інформаційних технологій протягом останніх десятиліть займала провідне місце в економічних дослідженнях і знайшла своє відображення в працях Антонюка В.А., Аранчій В.І., Височан О.С., Єрьоміної Н.В., Завгороднього А. Г., Зацеркляного М.М., Куркова М.С Мельникова О.Ф., Некрасенко Л.А., Пономаренка В.С. Сендзюка М.А. Шквір В.Д. та інших видатних вчених.

Разом з тим можна стверджувати, що не всі проблеми пов'язані з використання міжнародних електронних мереж досліджені в повній мірі, а деякі питання щодо використання міжбанківських розрахунків SWIFT потребують уточнення.

ПОСТАНОВКА ПРОБЛЕМИ

У своїй повсякденній роботі будь-який банк постійно має справи з іншими банками. Виникає необхідність у надійних системах для обміну фінансовою інформацією і здійснення взаєморозрахунків, тому виникає необхідність уточнення підходів щодо побудови таких систем, а саме:

- побудова системи передачі міжбанківських повідомлень і фінансової інформації на основі загальнодоступних комп'ютерних мереж;
- організація спеціалізованої системи на основі спеціальних корпоративних комп'ютерних мереж.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В усіх великих країнах існують національні системи для здійснення міжбанківських операцій великих країн. У США використовуються Fedwire – мережа федеральної резервної банківської системи, CHIPS – міжбанківська платіжна мережа, Bankwire. У Франції міжбанківські розрахунки засновані на системі SIT. У Великобританії застосовуються системи CHAPS (C1earing Houses Payment System) і BAC (Bankers Automated Clearing Services).

Розглянемо особливості деяких з цих систем. Fedwire – мережа федеральної резервної банківської системи США.[4]

Системою Fedwire володіє і керує Федеральна резервна система банків (ФРС) США. Ця система використовується для перекладу коштів між 6 тис. банків, об'єднаних у 12 резервних округів з 12 центральними регіональними банками (ЦРБ).

ЦРБ і окремі інші великі банки – члени ФРС мають власні сервери, що працюють у режимі on-line. Більш дрібні банки мають термінали системи Fedwire. Третя група банків – так названі «незалежні» учасники системи Fedwire працюють у режимі off-line і здійснюють міжбанківські операції по телефонних лініях зв'язку, що комутируються, із ними або передають інформацію прямо через інший-банк ФРС.

CHIPS (C1earing Houses Interbank Payment System) – телекомунікаційна мережа створена в 1970 р. у США для замін паперової системи розрахунків чеками на електронну систему розрахунків між Нью-Йоркськими банками й іноземними клієнтами. Усі банки розділяються на головні банки, розрахункові банки і банки – учасники системи CHIPS. Усього до системи приєднано 140 банків, при цьому вона працює приблизно з 10 тис. рахунків. Система CHIPS працює в режимі off-line. Передбачено нагромадження і наступне відправлення повідомлень, при цьому забезпечується збереження цілісності даних у центральної БД.

В даний час системи Fedwire і CHIPS обслуговують до 90 % міжбанківських внутрішніх розрахунків США.

Bankwire – мережа для обслуговування приватного сектору, що була організована в 1952 р. десятьма банками США. Після ряду реорганізацій була створена система Bankwire-II, послугами якої користується система кредитних карт MasterCard.[1]

Дана система здійснює нагромадження і наступне відправлення повідомлень. При відправленні повідомлення передаються в спеціалізовані могутні комп'ютерні центри по швидкісних виділених каналах, а потім попадають до адресатів.

Телекомунікаційна система BACS (Англія), що була створена в 1968 р. і, за станом на 1988 р., мала 16 банків-акціонерів. Пізніше система була перетворена в систему BACSTEL.

Система надає два види послуг для абонентів: «сервіс за графіком» (передача повідомлень у режимі off-line) і «сервіс за вимогою» для передачі коротких повідомлень по каналах загальнодоступних телекомунікаційних мережі.

Телекомунікаційна клірингова система SIT (Франція), її проект був розроблений у 1982-83 р. найбілішими банками Франції. Взаємодія БС у системі SIT відбувається на основі виділених каналів загальнодоступної мережі Transpac. Використовується протокол X.25. Відмінною рисою даної мережі є те, що плата за надання каналу не залежить від відстані між банками-абонентами. Система SIT взаємодіє з платіжними системами Viza і MasterCard.

Уже наприкінці 60-х років минулого століття стало очевидним, що традиційні «паперові» банківські системи розрахунків не можуть забезпечити надійний і швидкий зв'язок між банками та їх філіями в різних країнах. Крім того, різні банки використовували різні, часом несумісні, системи розрахунків. Тому в 1973 році було засноване Співтовариство Всесвітніх Міжбанківських Фінансових Телекомунікацій – Society for World-Wide Interbank Financial Telecommunication (SWIFT), яке є ведучою міжнародною організацією в сфері фінансових телекомунікацій. Основними напрямками діяльності SWIFT є надання оперативного, надійного, ефективного, конфіденційного і захищеного від несанкціонованого доступу телекомунікаційного обслуговування для банків і про ведення робіт зі стандартизації форм і методів обміну фінансовою інформацією.

Створена цим товариством SWIFT мережа передачі даних одна з найвідоміших мереж, створена з ініціативи фінансових організацій. Мережа забезпечує оперативне зберігання та пересилання банківських документів різного типу між банками, підключеними до мережі SWIFT, але не забезпечує виконання жодних розрахункових чи інших операцій з банківської обробки повідомлень. Головна мета створення SWIFT і її основна функція, полягають у забезпеченні користувачам цілодобової високошвидкісної передачі банківських даних за умови високого ступеня контролю даних та захисту від несанкціонованого доступу.[2]

Дані передаються по мережі шляхом пакетної комутації у вигляді структурованих повідомлень кожне з яких призначене для виконання певної фінансової операції. Для кожного підключеного вузла (банку) мережа забезпечує індивідуальне підтвердження приймання повідомлення та його обробки.

У 1968 р. була почата робота над проектом створення міжбанківської системи SWIFT (Society for World-Wide Interbank Financial Telecommunication).

Метою її створення було забезпечення всіх банків, що беруть участь у проекті, (і інших фінансових організацій) захищеної від несанкціонованого доступу, надійною, високошвидкісною і цілодобово працюючою системою для передачі банківської інформації.

На початку 70-х рр. система почала функціонувати. Зараз швидкими темпами відбувається впровадження нової модернізованої системи SWIFT-2.

Вартість передачі одного повідомлення в системі SWIFT виявляється менше, ніж вартість його передачі по телексу.

Особливістю SWIFT є використання єдиних для всіх користувачів правил і понять. Стандартизовані типи повідомлень мережі охоплюють сфери переміщень платежів клієнтів, міжбанківський рух платежів, дані про торгівлю грошима і валютою, виписки з платіжних рахунків банків, і т. п.

Стандартизація типів повідомлень переданих по мережі SWIFT була виконана Міжнародним комітетом зі стандартизації. У 1974-80 рр. розробку типових повідомлень було завершено. Наприкінці 1993 р. була додана група нових фінансових стандартів SWIFT Alliance, де визначаються інтерфейси для зв'язку з національними глобальними мережами комп'ютерів по телексу і факсу.

Застосування стандартних форматів повідомлень у рамках системи SWIFT дає наступні переваги:

виключається можливість різної інтерпретації повідомлень відправником і одержувачем;

можливий повний контроль за передачею інформації на основі постійної фіксації трансакцій у системі;

банк-користувач системи може автоматично генерувати щоденний звіт по проведених операціях.

У цілому система SWIFT являє собою глобальну всесвітню мережу на основі комп'ютерних центрів, з'єднаних різними каналами зв'язку. Основні комп'ютерні центри розташовані в США і Голландії. Ці центри зв'язані з регіональними хост-комп'ютерами, що встановлюються в країнах, що вступили в співтовариство SWIFT. Повідомлення від банку-відправника надходить через модем по відповідних каналах (комутованих або виділених телефонних лініях) у регіональний хост-комп'ютер. Відповідальність за передачу повідомлення до регіонального хост-комп'ютер несе банк-відправник. У регіональному центрі системи SWIFT повідомлення перевіряються на відповідність стандартам, накопичуються, шифруються і передаються по призначенню. Структура мережі SWIFT має два рівні (рис.1).

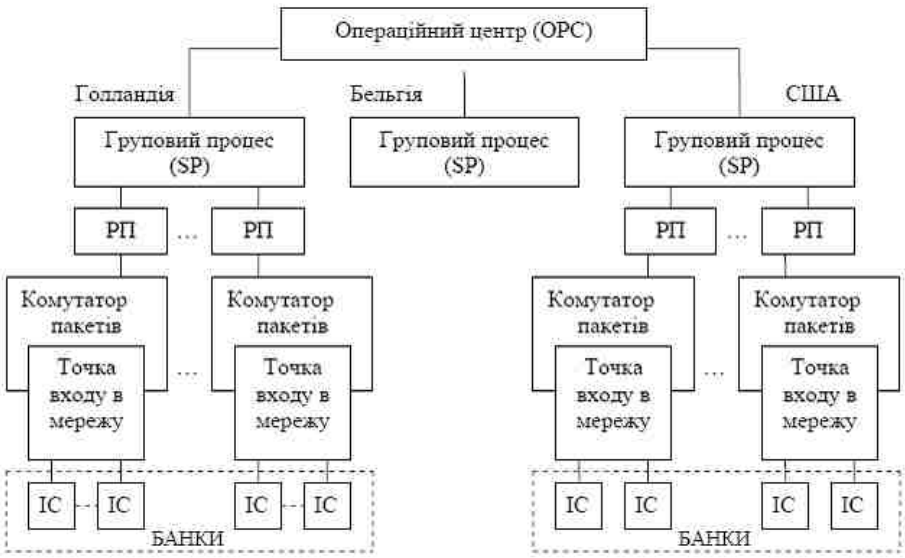

Рис. 1. Архітектура SWIFT

На верхньому (першому) рівні вона містить два Операційні Центри (ОЦ), один з яких розташований в США, а інший в Голландії. Другий рівень утворюють Регіональні Процесор (РП), які розміщені у більшості країн, банки яких приєднані до системи. Україна підключена до Австрійського РП. ОЦ становлять ядро мережі, вони з'єднані каналами зв'язку між собою і відповідними Регіональними Процесорами. Користувачі з'єднуються з РП виділених каналах зв'язку. Кожен РП відіграє роль концентратора повідомлень, через який дані передають в ОЦ.

Говорячи про програмно-апаратну реалізацію системи SWIFT, слід зазначити той факт, що всі можливі варіанти такої реалізації теж чітко стандартизовані. Як інтерфейси різних рівнів для підключення до мережі SWIFT використовуються інтерфейси ST200, ST400 і ST500 (табл. 1), які мають різну продуктивність і можуть бути реалізовані на основі різних комп'ютерних платформ. Основні характеристики стандартних інтерфейсів приведені в табл. 1.

Таблиця 1.
Стандартні інтерфейси SWIFT

Типи інтерфейсу	Комп'ютерна платформа	Призначення й особливості
ST200		Стандартний інтерфейс. Термінали розраховані на невеликий трафік (число повідомлень – до 10 у день). Обробка повідомлень виконується «вручну» (переносом текстових файлів у БС)
ST400	IBM RS/600 і AS400, DEC VAX і micro VAX HP U, Sun Sparkstation	Інтегрований інтерфейс підвищеної продуктивності. Орієнтований на автоматизовану обробку повідомлень. БС повинна мати ПО взаємодіє із системою SWIFT
ST500		Інтерфейс реального часу. Реалізується автоматизована, цілодобова обробка повідомлень SWIFT паралельно з роботою БС

Програмну реалізацію системи розглянемо на прикладі терміналів системи SWIFT-2. Для них можна використовувати різні модифікації програмного пакета TurboSWIFT фірми MIC Data Corp. (табл. 2).

Таблиця 2.
Модифікації пакета TurboSWIFT

Назва	Продуктивність, повідом./день	Особливості застосування
TurboSWIFT 100	100	Підтримка ОС UNIX (модель «клієнт-сервер») і графічний стандарт інтерфейсу користувача X-Windows
TurboSWIFT T250	250	Обробка повідомлень і генерація звітів на основі SQL-СУБД
TurboSWIFT 750	750	Зв'язок із БС на основі мережних протоколів TCP/IP, SNA, ВЗС і ін.
TurboSWIFT 3000	3000	Максимальна продуктивність у режимі OLTP досягає 10 000 повідомлень **у** годину
TurboSWIFT 3000+	>3000	Використовується надійна багаторівнева система захисту

У системі SWIFT застосовується багаторівнева система захисту інформації, що забезпечує гарантії зберігання і конфіденційності переданих даних. Широко використовуються криптографічні методи, що відповідають стандартам ISO.[5]

В силу специфічних вимог, які висуваються до конфіденційності переданої фінансової інформації, мережа SWIFT забезпечує високий рівень захисту повідомлень. SWIFT використовує широкий діапазон профілактичних наглядових заходів для забезпечення цілісності і конфіденційності її мережного трафіку, безперебійного забезпечення доступу до її послуг користувачам. Забезпеченню безпеки сприяє системний підхід, у рамках якого для забезпечення інтегральної безпеки системи приділяється увага всім компонентам: програмному забезпеченню, терміналам, технічній інфраструктурі, персоналу, приміщенням. При цьому враховується повний спектр ризиків від захисту від шахрайства до мінімізації вразливості фізичних ресурсів від наслідків неавторизованого доступу і навіть від природних і техногенних катастроф.

За організацію безпеки та за надійність роботи в мережі SWIFT несе відповідальність Генеральна Інспекція – група спеціалістів, до обов'язків якої входить перевірка діяльності в мережі. Крім цього, періодично проводяться перевірки зовнішніми аудиторами безпеки. Генеральна Інспекція підпорядкована безпосередньо лише Раді Директорів, яка керує діяльністю SWIFT.

Крім цілого ряду організаційних заходів для гарантування безпеки на програмному рівні мережа SWIFT автоматично виявляє випадки несанкціонованого доступу або необгрунтованого проникнення в роботу РП. Автоматично фіксуються і аномалії та відхилення від норм параметрів мережі. Додатково до цього кожному повідомленню при його вводі в мережу автоматично присвоюється послідовний вхідний номер, а при виводі – вихідний.

Всі пересилання повідомлень кодуються з використанням шрифтів, які змінюються через випадкові проміжки часу. Система контролю доступу до мережі включає в себе місцеві паролі для вузлів, журнальні файли, в яких зберігається інформація про кожне підключений до мережі та універсальну систему ідентифікації банків – BIC-код.

У SWIFT існує строгий поділ відповідальності між користувачами і Співтовариством за підтримку безпеки. Користувач відповідає за правильну експлуатацію, за фізичний захист терміналів, модемів і ліній зв'язку до пункту доступу і за правильне оформлення повідомлень. Вся інша відповідальність лежить на SWIFT, що відповідає за безупинне функціонування мережі, за захист від несанкціонованого доступу до неї, за захист повідомлень, що пересилаються, від усіх видів впливів після пункту доступу.

Один з важливих елементів забезпечення безпеки – фізична безпека приміщень. Доступ в усі будинки SWIFT строго контролюється; в операційних центрах персонал має право пересуватися лише у визначених зонах. Розроблено спеціальні інструкції на випадок вторгнення, пожежі, збоїв харчування і т. д. Пункти доступу, які працюють без участі персоналу, контролюються спеціальними системами, що стежать за входом і за приміщенням, за станом навколишнього середовища і станом устаткування.

Для захисту терміналів передбачене розмежування доступу користувачів на основі паролів, а з 1993 р. – на основі смарт-карток. SWIFT висуває строгі вимоги до процедури підключення терміналів до мережі. З метою забезпечення безпеки термінал може бути автоматично відключений самою системою в тому випадку, якщо виявлена перешкода, перервана лінія, або виявлені кількаразові помилки при передачі, повідомлення з неправильним номером і ін. Системою ведеться файл, де автоматично фіксуються усі відключення кожного терміналу, для того, щоб виявити лінії низької якості і некваліфіковане обслуговування терміналів.[3]

Для захисту повідомлень при їхній передачі по лінії зв'язку до пункту, допуску рекомендується використовувати схему підключення за допомогою спеціальних пристроїв шифрування, погоджених з SWIFT.

Безпека комунікацій SWIFT забезпечується шифруванням усіх повідомлень, переданих по міжнародним лініях зв'язку, що робить їх недоступними третім особам. Повідомлення запам'ятовуються також у зашифрованому виді, тому і персонал не може їх прочитати без спеціального доступу.

До програмно-технічних методів захисту відносяться:

коди підтвердження дійсності повідомлення, створювані під час введення даних спеціальними алгоритмами, що базуються на змісті повідомлень. Хоча алгоритм відомий усім, ключ знає лише відправник і одержувач. Ключі рекомендується змінювати раз у півроку;

контроль послідовності повідомлень. Повідомленням SWIFT присвоюються унікальні вхідні і вихідні номери в кожному сеансі зв'язку. Вхідні послідовності повідомлень обробляються слайснпроцесорами, а вихідні – одержувачами, так що ці номери верифікуються в процесі прийому і передачі і якщо вони не відповідають очікуваній послідовності, то повідомлення не тільки не пропускаються, але і відключається термінал користувача. Цей механізм гарантує, що кожне повідомлення не буде знищене або продубльоване. Запобігання передачі помилкових повідомлень, що містять спотворені послідовності незахищені ключами аутентифікації, є обов'язком користувача.

Захищеною є і сама архітектура системи (два операційний центри) у системі широко використовується резервування апаратних засобів. Усі канали зв'язку

працюють лише з зашифрованою інформацією, а доступ до телекомунікаційного устаткування строго обмежений.

Передані повідомлення захищаються від можливої втрати при збої в роботі устаткування, в центрах обробки інформації зберігаються копії всіх переданих повідомлень, а факт одержання кожного з них підтверджується індивідуально. При виникненні яких-небудь сумнівів користувач може запросити копію будь-якого відправленого на його адресу повідомлення. З огляду на використання ряду додаткових заходів, включаючи апаратні засоби захисту каналів зв'язку, мережа забезпечує надійний захист інформації від несанкціонованого доступу, втрати чи перекручування.

Безпрецедентні міри безпеки, використовувані в мережі SWIFT її багаторазове резервування технічних засобів дозволили дотепер уникнути будь-яких – серйозних аварійних ситуацій у мережі SWIFT і її несанкціонованого використання.

Економічна доцільність використання SWIFT у системі міжбанківських відносин полягає в наданні швидкого і зручного обміну інформацією між: фінансовими інститутами, розташованими будь-де на Землі, ефективне використання коштів за рахунок прискорення проведення і одержання підтверджень, збільшення продуктивності системи, підвищення рівня банківської автоматизації, зменшення ймовірності помилок.

ВИСНОВКИ

Швидкий розвиток банківської активності призводить до значного зростання об'ємів інформації, якою необхідно оперувати, що викликає збільшення інформаційних потоків в локальних МПД(мережа передачі даних) банків. Тому при створенні таких МПД повинно бути передбачено збільшення з часом об'єму інформації, яка передається і усунення можливості виникнення вузьких місць. Важливим моментом є передбачення можливості наступних модернізацій МПД. В цьому випадку МПД банку не перетвориться в догму, яка гальмує діяльність всієї організації, а буде ефективним, зручним і простим інструментом управління, який дозволить підвищити якість і продуктивність роботи.

Сучасні банківські інформаційні технології базуються на концепції відкритих систем і на архітектурі клієнт-сервер замість файлових серверів. Це дозволяє реалізовувати оперативний доступ до віддалених баз даних і запуск програм на віддалених робочих станціях, організовувати глобальну телекомунікаційну мережу, проводити інтеграцію неоднорідних локальних мереж з базовим протоколом TCP/IP.

Високопродуктивна, розподілена по філіалах банківська інформаційна система (БІС) характеризується формулою ОС UNIX + SQL-сервер -+ Монітор транзакцій + Сервер. Монітор транзакцій забезпечує неможливість використання методу тиражування даних (реплікацію даних) і використання розподілених баз даних. Це означає, що клієнт «не може» обігнати процедуру оновлення інформації шляхом реплікації і, наприклад, зняти гроші зі свого рахунку два рази в різних відділеннях банку.

В банківській інформаційній системі з монітором транзакцій все робиться за участю сервера (всередині нього), а по лініях зв'язку передається мінімум інформації. Крім того, використання монітора транзакцій полегшує створення програм. Тому, що вони розбиті ніби на дві частини, одна відповідає за представлення інформації, а інша за її обробку.

Сервери БІС повинні бути високонадійні, в них зокрема має бути передбачено дублювання процесорів і дискової пам'яті. А крім того в них необхідно передбачити можливість розвитку за рахунок масштабування. Програмне забезпечення для таких серверів повинно мати наступні властивості:

- мати гнучку відкриту систему кодування;
- забезпечувати повну обробку даних за всі дати;
- забезпечувати можливість конфігурування споживачем;
- мати єдину систему банківського обліку;
- забезпечувати використання управлінської інформації і інструментів фінансового контролю;
- забезпечувати можливість вводу повної «банківської операції» розділеної на складові частини;
- мати уніфікований набір кодів і визначень.

Задача обробки фінансових повідомлень характеризується відсутністю єдиного стандарту і багатогранністю форматів повідомлень, збільшеним потоком інформації, необхідністю зниження вартості обробки повідомлень і т. д. Крім того, формати повідомлень мають багато полів і часто змінюються, що вимагає від системи гнучкості і можливості для подальшої швидкої модифікації Основний підхід для розв'язку такої проблем – використання спеціальної простої мови опису форматів повідомлень.

Монітори транзакцій являють собою відкрите, гнучке середовище для розробки і для управління мобільними додатками, які орієнтовані на оперативну обробку розподілених транзакцій. До найважливіших характеристик моніторів транзакцій відносять можливість масштабування, підтримку функціональної повноти Й цілісності додатків, досягнення максимальної продуктивності при обробці даних при невисоких вартісних показниках.

Локальна МПД банку об'єднує робочі місця і всі периферійні пристрої в єдиний інформаційний простір. Переваги такого об'єднання наступні:

- підвищення сумарної обчислювальної потужності і ефективності всіх комп'ютерів мережі завдяки перерозподілу виконуваних завдань між ними;
- підвищення надійності БІС в цілому;
- економія засобів, тому що при наявності мережі непотрібно мати декілька принтерів, сканерів і ін. периферійних пристроїв;
- підвищення ефективності праці, тому що швидкість передачі Інформації по мережі завжди більша ніж швидкість переміщення співробітників зі змінними носіями інформації;
- підвищення ефективності менеджменту, тому що управління фірмою можна здійснювати, не відриваючись від робочого стану і не відволікаючи від роботи співробітників;
- організація централізованої системи забезпечення інформаційної безпеки фірми шляхом захисту баз даних і резервування інформації. Локальна МПД банку підвищує продуктивність праці, дозволяє повністю автоматизувати виробничі процеси, а при підключенні до мережі Internet забезпечує кожному співробітнику доступ до практичне необмежених інформаційних ресурсів людства. Але при початку побудови БІС необхідно передбачити фінансові витрати на придбання обладнання і комплектуючих БІС, а також витрати на навчання технічного персоналу, який буде підтримувати її працездатність і безпеку. Крім того при побудові локальної БІС слід врахувати внутрішні і зовнішні фактори.

До внутрішніх факторів відносять існуючу інфраструктуру підприємства, офісу, банку, персонал, технічний персонал, уже наявні засоби інформаційних технологій. БІС повинна задовольняти (відповідати) «параметрам» банку. В іншому випадку банк не зможе ефективно розв'язувати свої завдання і не зможе ефективно працювати з погано розробленою банківською інформаційною системою.

Стабільна робота БІС без збоїв в мережі і збереження цілісності даних в ній в значній мірі залежить від того наскільки кваліфіковано і надійно захищена БІС від впливу зовнішніх факторів до яких відносять стихійні лиха, збої системи електроживлення і захищеність БІС від спроб проникнення зловмисників (несанкціонований доступ).

Тому установку і наладку МПД для банку повинні виконувати лише спеціалісти фірми, яка має статус сертифікованого інсталятора. В такому випадку, коли на якій-небудь ділянці мережі трафік зросте, або виникне необхідність добавити в мережу іще декілька робочих місць необхідність міни конфігурації і оптимізації мережі не перетвориться в проблему, важку для розв'язку.

ЛІТЕРАТУРА.

1. Антонюк В.А., Курков М.С. Інформаційні системи і технології у фінансах: Навч.-метод. посіб. для самостійного вивч. дисц.- К.:КНЕУ, 2005.-140с.

2. Аранчій В.І., Некрасенко Л.А., Зоря О.П., Макаренко Ю.П., Аранчій Д.С. Інформаційні системи і технології у фінансах Навч. посібник.[Аранчій В.І., Некрасенко Л.А., Зоря О.П. та ін]- Полтава.: РВВ ПДАА, 2009.-400 с. 3.Зацеркляний М. М., Мельников О.Ф. Інформаційні системи і технології у фінансово-кредитних установах. Навчальний посібник.- К.: професіонал, 2006.-432с.

4.Єрьоміна Н.В. Банківські інформаційні системи: Навчальний посібник.-К.: КНЕУ, 2000.-230с.

5.Інформаційні системи і технології в обліку: Навч посібник/ Шквір В.Д., Завгородній А.Г., Височан О.С. – Львів: Вид-во Нац. ун-ту «Львівська політехніка», 2003.- 268с.

REFERENCES.

1. Antonyuk A.V, Kurkov M. S(2005). *Information systems and technologies in finance* [Information systems and technologies in finance], KNEU, Kyiv,Ukraine

2. Aranchii V.I., NekrasenkoI.A., ZorjaO.P, Makarenko Yu.P., Aranchii D. S. (2009) *Information systems and technologies in finance*.[Information systems and technologies in finance]-RVV PDAA, Poltava, Ukraine

3. Zacerklânij M.M, Melnikov, O.F. (2006) *Information systems and technologies in the financial and credit institutions* [Information systems and technologies in the financial and credit institutions]: Professional, Kyiv, Ukraine

4. Eryomina N. V. (2000)Bank information systems KNEU, Kyiv,Ukraine

5. Škvìr V.D., Zavgorodnij A. G., Vysochan O. S. (2003).*Information systems and technologies in accounting* [Information systems and technologies in accounting] Lviv Polytechnic, Lviv, Ukraine

Стаття надійшла до редакції 10.10.2014 р.