МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ БАНКІВСЬКОГО БІЗНЕСУ

КАФЕДРА БАНКІВСЬКОЇ СПРАВИ

Мельник Роман Олексійович

ОРГАНІЗАЦІЯ БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ КЛІЄНТІВ У МЕРЕЖІ ІНТЕРНЕТ.

Спеціальність 8.03050802 – банківська справа

Дипломна робота за освітньо-кваліфікаційним рівнем «магістр»

Студент групи БСм-51
Р.О. Мельник
_____

Науковий керівник:
К.е.н. доц. Я. І. Чайковський
_____

Дипломну роботу допущено
до захисту:

«___»_____2013р.

Завідуючий кафедрою банківської справи,

Доктор економічних наук, професор

О.В. Дзюблюк

_____

Тернопіль – 2013

ЗМІСТ

ВСТУП

Актуальність теми магістерської роботи полягає в тому, що останні роки банківська система нашої країни переживає бурхливий розвиток новітніх банківських технологій. Незважаючи на недоліки існуючого українського законодавства, що регулює діяльність банків, ситуація неухильно змінюється на краще. Пішли в минуле ті дні, коли ви могли б легко зробити спекулятивних операцій з валютою та шахрайстві. Сьогодні все більше банків покладається на професіоналізм своїх співробітників і нові технології.

Важко уявити собі більш благодатне підгрунття для впровадження нових комп'ютерних технологій, ніж банківська діяльність. Справді, майже всі проблеми, які виникають в ході діяльності банку досить легко автоматизувати. Швидкі і якісні обробки великих потоків даних є одним з основних завдань будь-якому банку. Володіючи новітньою комп'ютерною мережею, яка може впоратися із зростаючим потоком інформації. Крім того, саме банки мають достатні фінансові засоби, щоб використовувати найсучасніші технології. Але ми не повинні вважати, що середній банк готовий витрачати величезні суми на комп'ютеризацію. Банк є передусім фінансової установою, призначеним для отримання прибутку, тому що вартість модернізації повинні бути зіставлені з передбачувана користь її реалізації. Згідно світовій практиці середня вартість банківських комп'ютеризації становить не менше 17% від загальних річних витрат бюджету.

Інтерес до розвитку комп'ютеризованих банківських систем (БС) визначається не бажанням отримати короткострокову вигоду, але в основному стратегічні інтереси. На практиці, інвестиції в такі проекти починають приносити прибуток лише через певний період часу, необхідний для навчання та адаптації системи до конкретних умов. Інвестування в обладнання, програмне забезпечення, комп'ютерне та телекомунікаційне і забезпечити основу для переходу до нових обчислювальних платформ, банки, в першу чергу, прагнуть знизити вартість і прискорити вашу роботу рутиною і

перемогти в конкурсі. Нові технології допомагають банкам змінити взаємовідносини з клієнтами та знайти нові ресурси для отримання прибутку.

Проблеми, з якими стикаються всі фінансові установи: інтеграція успадкованих систем в розподілену архітектуру локальних мереж. Девід Стюарт, головний консультант з нових технологій в глобальні концепції, вважає, що сьогодні попит на людей, які розуміли мереж вище, ніж будь-коли раніше. На його думку, в даний час у сфері зайнятості в банку програмістом уподобання, а не в касу.

Огляд літератури з теми дослідження. Питанням використання аналізованої послуги фінансовими установами приділяло увагу багато науковців серед яких можна виділити Д.Н. Гусєв, М.А. Домніна, І.Л. Близнюк, Г.А. Титоренко. Проте досі не до кінця дослідженими залишаються механізми впливу описаного банківського продукту на пасиви та фінансовий стан установи.

Мета і завдання дослідження. Метою магістерської роботи є аналіз організації банківського обслуговування клієнтів у мережі Інтернет, розробка ефективних заходів обмеження впливу недосконалості правової бази на вітчизняну економіку загалом і банківську систему зокрема. Розробка пропозицій по удосконаленню уже існуючих банківських інтернет послуг .

Об'єкт і предмет дослідження. Об'єктом дослідження є зарубіжна та вітчизняна банківські системи.

Предметом дослідження є процес взаємодії банківських установ з клієнтами за допомогою інтернет технологій.

Методи дослідження. Дослідження по даній темі проводилося на основі використання статистичних, математичних методів, методів прогнозування, техніко-економічного і фінансового аналізу а також методів спостереження.

Інформаційна база роботи. Статистичну і аналітичну основу дослідження складають закони України, постанови та декрети Кабінету Міністрів України, укази Президента України, нормативні документи Національного банку України.

Наукова новизна роботи полягає у теоретичному визначенні поняття «Інтернет-банкінг» в умовах посиленого та засобів зв'язку, та в обґрунтуванні впливу розвитку технологій на розвиток банківських продуктів, у аналізі ефективності впровадження нових банківських послуг і запропоновано можливі дії для подальшого розвитку банківських технологій в Україні.

Практичне значення роботи полягає у тому, що в майбутньому результати дослідження даної тематики можуть бути використані для вдосконалення та впровадження нових банківських інтернет-послуг.

Структура роботи. Дипломна робота складається зі вступу, 3 розділів, висновків, списку використаних джерел і додатків.

Розділ 1. Суть та напрямки використань нових інформаційних технологій та систем в банківській діяльності

1.1 Роль Інтернет в банківській діяльності та засоби його використання

За умов сьогодення, прогресивний економічний розвиток держави унеможливлюється без банківської системи розвинутої на достатньому рівні, та на стан якої в свою чергу впливає як зміни на рівні світової банківської системи, так і стан внутрішньої економічної і політичної ситуації. Усі зміни відбуваються внаслідок макроекономічних процесів у масштабі світової економіки: різкий науково-технічний підйом, інтеграція, лібералізація, які безпосередньо впливають на усі банківські установи, незважаючи на рівень їх розвитку, та місця розташування. Головною особливістю банківської системи за умов сьогодення є карколомний розвиток комп'ютерних і телекомунікаційних технологій, який забезпечує скорочення часу обробки інформації, та дозволяє комплексно автоматизувати діяльність, розробивши механізм дистанційного обслуговування клієнтів і запропонувавши оновлений набір послуг.

Майже всі найвідоміші світові фінансові інститути давно вже не уявляють своєї діяльності без використання Інтернету. Слід також зазначити, що різні події, що відбуваються в нашій країні і, присвячених цій темі, зміна його характеру з чисто освітнього до більш практичним. Пропонується наступне: самостійне онлайн обслуговування, як справжню революцію, особливо в банківській сфері. Сьогодні було досить зручно для пошуку і вибору відповідної експлуатації та обслуговуванні клієнтів на банки. Оплати (або інший переклад) також можна виконувати по мережі. Крім того, більшість банків пропонують своїм клієнтам можливість самоперевірки. Це приносить більше вигоди для клієнта, так що прискорює процес обслуговування і розширює спектр послуг. Віддалене управління банківськими рахунками через

Інтернет, або Інтернет-банкінг, завдяки широкому спектру фінансових послуг, найбільш динамічних і prespektyvnyy лінія Інтернет-рішень у фінансовому sfereri.

Суть та зміст поняття Інтернет-банкінг розглядалися під найрізноманітнішим авторськими підходами. На мою думку, найбільш вдалою, є формулювання, відповідно до якого Інтернет-банкінг розглядається, як надання послуг банком, з моніторингу, управління рахунками та здійснення банківських транзакцій через Інтернет.При цьому користувач, як правило, не потребує спеціального програмного забезпечення для доступу до своїх рахунків. Він може здійснювати всі дії по управлінню рахунками з будь-якого комп'ютера, підключеного до мережі Інтернет, і розпізнається банком за допомогою системи авторизації. [5]. Майже у всіх випадках додатково потрібено електронний цифровий ключ , іншим варіантом маже бути спеціальне програмне забезпечення, тільки при цьому він повинен з легкістю встановлюватись на будь-який інший ПК.

По своїй суті Інтернет-банкінг являє собою логічне продовження таких різновидів віддаленого банкінгу, як PC banking: тобто доступ до банківського рахунка за допомогою ПК, що здійснюється при прямому модемному з'єднанню з банківською мережею, telephonebanking: ведення рахунків за телефоном та videobanking: система побудована на інтерактивному спілкуванні клієнта з персоналом банку. На сьогоднішній день клієнт може з легкістю здійснювати, знаходячись за комп'ютером вдома чи в офісі, більше ніж 85% усіх банківських операцій. Відповідно користь для банкірів та їхніх клієнтів визначається наступним: перші значно скорочують витрати по утриманню густої філіальної мережі і значно підвищують ефективність банківських операцій, а інші отримують додаткові зручності [4].

Існує два основних чинника, що вказують на ступінь розвитку Інтернет-банкінгу в будь-якій країні. Першим з ний є цифровий простір країни, який має бути розвиненим, користувач може мати у своєму розпорядженні достатню кількість загально-цікавих ресурсів рідною мовою. Другий, населення країни має звикнути користуватися Інтернетом у повсякденному житті, мати достатньо

тривалий досвід користування мережею, адже ніхто не починає з придбання через Інтернет банківських продуктів. Використовуючи Інтернет можна керувати своїми грошима – економлячи на грошові перекази і оплату комунальних послуг, уникати походів у банківські відділення та довготривалих черг біля кас. Доступ до свого рахунку для користувачів Інтернет-банкінгу відкритий цілодобово і звідусіль, де є доступ до Інтернету, і це надає цим послугам ще більшої переваги.

Серед програмістів і співробітників ІТ-індустрії Інтернет-банкінг дуже популярний [52 с.24]. Пояснюється це тим, що багато з таких фахівців виконують роботу для зарубіжних замовників, а для отримання винагороди активно використовують платіжні картки, і не тільки в Україні і, як наслідок, виникає необхідність використання послуг Інтернет-банкінгу.

Інші ж українці ставляться до такої послуги з нерозумінням, побоюванням або зовсім ігнорують [52 с.73]. Третина українських користувачів Інтернет проводять банківські операції в режимі онлайн. Третина (29,6%) українськх користувачів мережі Інтернет хоча би один раз на місяць проводять платежі з допомогою онлайн сервісу, а один з десяти отримує онлайн-виписки за своїми рахунками. Це оприлюднила компанія GfkUkraine за результатами опитування серед Інтернет користувачів в Україні. Найпопулярнішим сервісом Інтернет-банкінгу для українських користувачів, за даними GfkUkraine, є система Приват24 (ПриватБанк). Послугами Приват24 користуються 77% з опитаних.

Системи Інтернет обслуговування серед інших українських банків: 20% з опитаних зазначили, що обслуговуються онлайн у Райффайзен Банку Аваль, 13% - ПУМБ, 10% - Альфа-банку і 6% - Дельта-банку. Інтернет-користувачі надають перевагу використовувати задля спілкування з банківськими працівниками традиційні канали комунікацій - але 7% з опитаних на сьогодні спілкуються з банками за допомогою соціальних мереж. Водночас, 36% готові за необхідності зв’язатися з менеджером банку через соцмережу, а кожен п'ятий опитаний в майбутньому готовий повністю замінити візити в банк спілкуванням з фінустановою в соцмережі. Але є і банки-консерватори які

обережні і вважають, що Інтернет-банкінг масовому клієнту не потрібен зовсім, або потрібен в усіченому варіанті, а тому пропонують обмежений набір пов'язаних з Інтернетом послуг: перевірка стану карткового та інших рахунків, перегляд виписок по рахунках, блокування операцій по карті.До поняття самообслуговування часто ставляться з недовірою або розглядають його як крайній засіб при відсутності інших можливостей обслуговування клієнтів. Але останнім часом, в основному завдяки розвитку інформаційних технологій, веб-сервісів і нових можливостей телефонного зв'язку, самообслуговування, нарешті, було оцінено по достоїнству як ефективний спосіб розширити канали спілкування із клієнтами, давши їм можливість взаємодіяти з компаніями в будь-який час і в будь-якому місці.

Інтернет-банкінг є складовою частиною політики, спрямованої на збільшення обсягу залучених коштів, та впровадження нових банківських послуг, які користуються попитом на ринку, і його пропонують клієнтам все більша кількість установ вітчизняної банківської системи. Питанням використання аналізованої послуги фінансовими установами приділяло увагу багато науковців серед яких можна виділити Д.Н. Гусєв, М.А. Домніна, І.Л. Близнюк, Г.А. Титоренко. Проте досі не до кінця дослідженими залишаються механізми впливу описаного банківського продукту на пасиви та фінансовий стан установи.

Інтернет-банкінг має на меті покращення якості обслуговування клієнтів, оскільки володіє рядом наступних переваг, зокрема зростання оперативності здійснення операцій, доступність для клієнта (операції здійснюються в режимі реального часу без відвідування офісу банку), необмеженість, тобто здатність здійснювати платежі майже будь-якого призначення, та контрольованість, оскільки будь-яке списання коштів з карткового рахунку одразу відображається у відповідних виписках [78, с. 63].

Інтернет-банкінг виступає в ролі універсального інструмента збільшення залучених коштів шляхом зростання клієнтської бази комерційного банку та розглядається як ефективний метод залучення нових клієнтів за допомогою створення більш зручних умов дистанційного використання обумовленого

спектру послуг. Це дає змогу керівництву установи впливати на пасиви банку з мінімальними витратами часу. Однак використання даного методу має певні особливості, які стосуються його впливу на фінансовий стан фінансового посередника та основні показники його діяльності, оскільки надання цієї послуги пов'язано з виникненням певних ризиків. Фінансові установи повинні враховувати їх при впровадженні цього продукту на ринку.

При використанні Інтернет-банкінгу потрібно враховувати певні ризики, а саме:

- операційний;
- правовий;
- стратегічний;
- ризик втрати ділової репутації;
- ризик ліквідності .

Операційний та правовий ризик виникають у процесі здійснення основної діяльності установи. Перший виникає через ненадійність використання інформаційних систем потрібних для Інтернет-банкінгу, проблеми у роботі персоналу з цією послугою та аварійні ситуації з апаратною складовою. Правовий ризик стосується можливості порушення банком законодавства країни, недостатнього опрацювання договорів з клієнтами на надання цієї послуги, порушень договору зі сторони клієнта чи банку при використанні цього продукту та інших юридичних аспектів. Все це потребує детального вивчення при використанні нового банківського продукту.

Стратегічний та діловий ризик виникають не тільки у процесі здійснення основної діяльності, а і при перспективному плануванні. Перший виникає внаслідок помилок при впровадженні системи Інтернет-банкінгу, недоліків стратегічного плану розвитку в розрізі використання цього продукту, неправильного вибору програмного забезпечення та спектру послуг, які надаються завдяки цьому комплексу. Діловий ризик перш за все стосується можливості втрати конфіденційних даних клієнтів, незадоволення користувачів якістю даного продукту, проблем з безперервністю функціонування системи. Врахування наведених ризиків вкрай важливе для успішного довгострокового

застосування даного інструменту збільшення притоку залучених коштів. Також потрібно пам’ятати, що комерційні банки в системі Інтернет-банкінгу можуть використовувати лише ті засоби захисту, які пройшли сертифікацію у визначених державних органах та є ліцензованими [22 с. 228].

Найважливішим є ризик ліквідності. Він прямо пов'язаний з метою використання Інтернет-банкінгу банком. Його виникнення може бути спричинене недосконалим управлінням описаними раніше ризиками, а також недоліками політики контролю ліквідності в умовах застосування цього продукту. Ефективному менеджменту цієї категорії має приділятись найбільше уваги, оскільки вона спричиняє найвагоміший вплив на фінансовий стан комерційного банку.

Банк, який активно використовує переваги комплексної системи дистанційного банківського обслуговування, надає своїм клієнтам реальну можливість оперативно і максимально ефективно керувати власними фінансовими потоками [56 , с. 68]. Завдяки цьому, він стає більш привабливим для потенційних користувачів і виникають нові можливості для залучення коштів та отримання прибутку за рахунок їх використання в майбутньому.

1.2 Перші приклади інтерактивної роботи фінансових закладів в Інтернеті

Інтернет-банкінг або як його ще називають на заході E-banking - це технологія дистанційного банківського обслуговування, яка дозволяє вкладникам банку отримувати доступ до інформації про свої рахунки і здійснювати операції по них, використовуючи Інтернет. Система Інтернет банкінгу бере свій початок з 80 років минулого століття, коли в США була створена систем HomeBanking. Ця система давала можливість вкладникам перевіряти свої рахунки, підключаючись до комп'ютера банку через телефон. Надалі, у міру розвитку Інтернету і Інтернет технологій банки починають вводити системи, які дозволяли вкладникам отримувати інформацію про свої рахунки, через Інтернет. Вперше послуга переказу грошових коштів з рахунків була введена в 1994 році в США Стенфордським федеральним кредитним спілкам, а вже в 1995 році був створений перший віртуальний банк - SecurityFirstNetworkBank. Але, на розчарування засновників проекту, він зазнав фіаско через сильний недовіри з боку потенційних клієнтів, які, в ті часи, не дуже-то довіряли такому нововведенню.

Першим банком, що досягли успіху в онлайн банкінгу, став Bank of America. До 2001 року він став першим, серед всіх банків, що надають послугу Е-банкінгу, чия база користувачів цією послугою перевищила 2млн клієнтів. На той момент ця цифра становила близько 20% всіх клієнтів банку. А в жовтні все того ж 2001 року і все тим же Bank of America була побита взята планка в 3млн. грошових переказів, здійснених за допомогою послуги онлайн банкінгу на загальну суму понад 1млрд. $ США. В даний час в країнах Західної Європи та Північної Америки послугами Е-банкінгу користуються більше 50% всього дорослого населення, а серед повнолітніх користувачів Інтернету ця цифра сягає 90%.

«Маркетингові дослідження показують, що роздрібний клієнт, звикає до користування Інтернет-банкінгом, починає залишати на своєму банківському рахунку грошей спочатку більше, а потім значно більше, ніж йому потрібно для

щомісячних Інтернет-оплат. Тому що спочатку він утруднюється точно підрахувати необхідну суму і залишає з невеликим запасом, щоб не витрачати зайвий час на повернення готівки на свій рахунок. А потім просто звикає, що залишаються на банківському рахунку надлишки все одно доступні за допомогою карти, причому відсоток втрат на знімання готівки навіть в «чужому» банкоматіпорівняно менше, ніж відсоток втрат при оплаті послуг через термінали.

До того ж, виявляється, у багатьох магазинах карту просто беруть до оплати без жодних втрат. А по золотих картам ще й знижки дають. Ну і так далі. Таким чином, Інтернет-банкінг починає змінювати модель поведінки роздрібного клієнта в сторону, корисну для банків ... Мова йде про дуже цікавий феномен поведінки роздрібного клієнта, який дозволяє всерйоз розглядати Інтернет-банкінг, як інструмент, що приносить банку помітні додаткові кредитні ресурси, а не тільки комісійні доходи»

Деякі банківські установи Інтернет-банкінг розвивають як додаткову послугу в першу чергу тому, що клієнту зручно, і для будь-якого банку зручності клієнтів - головна мета. При такому підході, банк не одержує значну економію, однак, виграє. Клієнтам пропонується широкий спектр послуг, вони можуть робити багато звичайних операцій, і вони доступні по телекомунікаційних каналах зв'язку. Інтерактивність у поєднанні з можливістю «людського» контакту із співробітниками банку в офісі і по телефону. Цей підхід можна назвати сервіс-орієнтованої, і банки, які тримають на цьому ставку, називаються багатоканальними банками. Як правило, великі роздрібні банки, які хочуть йти в ногу з передовими тенденціями і очікувати в майбутньому для досягнення раціоналізації своєї роздрібної мережі.

Існує інший підхід, який полюгає у мінімізації витрат і з цією метою організована система "віртуальних" банків, які працють тільки через Інтернет і інші канали доступу. Проте останнім часом в США демонструються ознаки уповільнення потоку клієнтів у віртуальні банки. Експерти пояснюють,що це надто великі надії з точки зору якості обслуговування у віртуальних банках, змушуючи замовників перейти на обслуговування у звичайних банках, які

надають послуги дистанційних банківських послуг. Причинами називають також низький показник надійності віртуальних банків, депозит-гарантійних схем і низької рентабельності їх роботи через величезні витрати на рекламу.

Корпоративна мережа банку являє собою окремий випадок великої корпоративної мережі. Очевидно, що специфіка банківської діяльності накладає жорсткі вимоги щодо захисту інформації в комп'ютерних мережах банку. Не менш важливу роль при побудові корпоративної мережі відіграє потреба забезпечення безперебійної роботи, а також переривчасті збої у її роботі можуть призвести до величезних втрат. І, нарешті, потрібно забезпечити швидку і надійну передачу великих обсягів даних, оскільки багато банківських програмних додатків повинні працювати в реальному часі.

Є основні вимоги до корпоративної мережі банку.

Мережа об'єднується в структуровані і контрольовані замкнуті системи, що включають: окремі комп'ютери і локальні обчислювальні мережі (LAN), хост-сервери, робочі станції, телефони, факси, АТС, банкомати, термінали онлайн.

Мережа забезпечує надійну роботу і потужну систему захисту. Тобто, Гарантований Uptime помилок в разі несанкціонованого доступу.

Там встановлена система зв'язку між філіями банку на різних рівнях (як муніципальних, так і філій іногородніх).

У зв'язку з сучасними тенденціями у сфері банківських послуг (наприклад, обслуговування за телефоном, цілодобовий доступ до банкоматів та он-лайн терміналів, розвиток мережі платіжних терміналів у торговельних закладах існує необхідність у конкретних банках. У телекомунікаційних рішеннях . Істотну роль грає швидкий, надійний і безпечний віддалений доступ клієнта до сучасних банківських послуг.

Головною особливістю українського Інтернет-банкінгу є те, що керівництво банку розглядає можливість виходу в Інтернет скоріше як модний крок. Хоча це, безумовно, дуже перспективний напрямок. Цікаво, в першу чергу, для громадськості і буде рости разом з розвитком роздрібного Інтернет-банкінгу. Але в Україні є обмеження: немає вітчизняного фондовому ринку,

доступ на західні ринки обмежений, крім того, громадськість не готова до цього кроку. Валютний ринок не готовий до цієї торгівлі, а вітчизняні підприємства не мають права брати участь у валютних спекуляціях.

Схема використання системи "банк-клієнт" така: банк купує (або розробляє) систему і потім продає або безкоштовно надає доступ до неї своїм клієнтам (рис.1.2.1.).

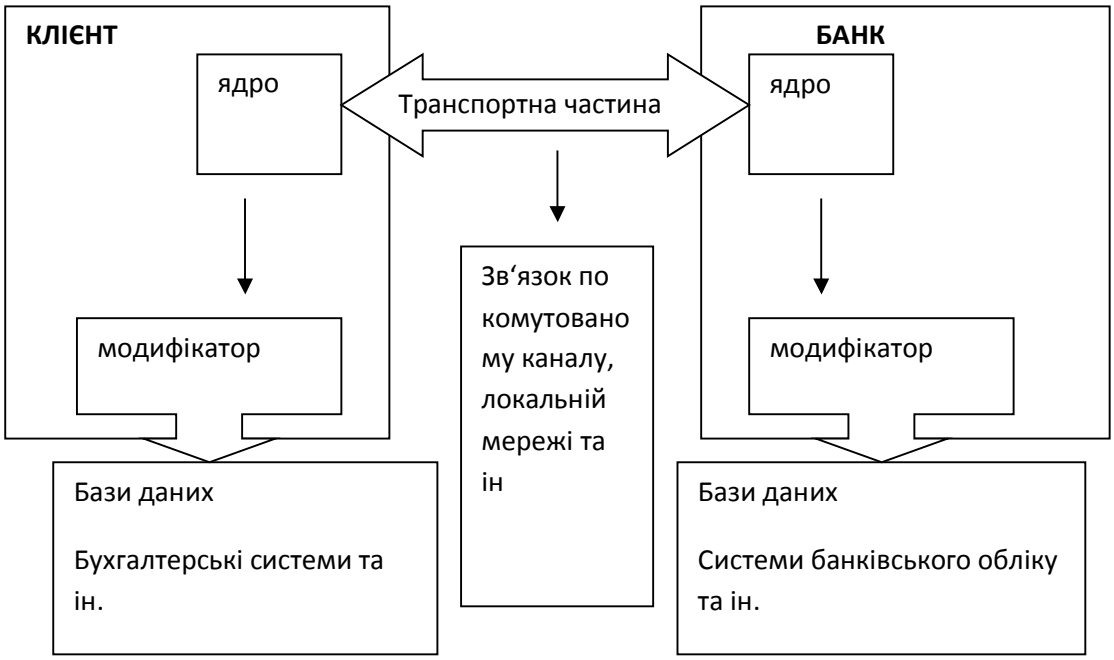

Рис.1.2. 1. Загальна схема функціонування системи „банк-клієнт”

З точки зору фінансових послуг для банківської системи "Клієнт-банк" нічого принципово нового, основні зміни, внесені в організаційній області. "Банк-Клієнт" може тільки виключити з технологічного ланцюжка обробки фінансового документа процедуру передачі паперового оригіналу з рук клієнта в руки операторів і перевести його в електронний вигляд. Супроводжуючих цей процес операції ідентифікації і аутентифікації документа теж виконуються автоматично. Далі документи в електронному вигляді абсолютно ті ж етапи обробки за умови сучасних технологій у формі паперового документа.

Сьогодні в Україні Interpnet не в змозі дати набагато більше, ніж «Клієнт-Банк». У західних умовах - як на те, що робота Interpnetu відкриває доступ до багатьох ресурсів. В українських же умовах, коли, щоб отримати банківську

виписку або відправити платіжне доручення, використання Мережі не так привабливо.

Крім того, більшість банків використовують Україну в якості зразка Interpnet, яка надає на своїх сайтах лише про себе, своїх послуг, координує. Але це не Interpnet-банкінг, тому що вони не надають ніяких послуг через власні сайти. В даний час в Україні може бути розділена на 11 банків, хоч якось "рухатися" у напрямку Interpnet банкінг "Аваль", Приватбанк, "Промінвестбанк" Перший Український Міжнародний Банк (ПУМБ) ВАБанк, "Райффайзенбанк Україна", Київський міжнародний банк, "ING-Barings Україна "Трансбанк, Мегабанк Експрес Банк і" Мрія ".

Промінвестбанк активно розвивається дистанційного банківського обслуговування, які дозволяють клієнтам отримати широкий спектр банківських послуг без відвідування банку. Успішна робота системи "Дистанційний моніторинг рахунків клієнтів", "банківська Interpnet". Для корпоративних клієнтів банк з широкою мережею підрозділів, що працюють у різних регіонах України, розвинений сервіс "Корпоративний контроль», яка дозволяє клієнту в свій штаб цілодобово і без вихідних моніторинг вихідних платежів своїх відомств для прийняття рішень щодо їх здійсненності, своєчасності та відповідності корпоративним вимогам підприємства, щоб підтвердити або виключити їх з оплати. За допомогою системи «Клієнт-Банк» є 13600 клієнтів банку 2600 клієнтів використовували центру голосового виклику банку.

Перший Український Міжнародний Банк. У березні 2001 року Банк реалізував проект, який дозволяє клієнтам отримати інформацію про свої рахунки через Interpnet. На даний момент клієнти можуть отримати ПУМБ 6 видів виписок за рахунками, із заявою за датою заяви і закінчуючи рухом валюти на місяць. У липні банк реалізував проект «Клієнт - Банк», яка дозволяє клієнтам здійснювати повний контроль над Interpnet рахунку. До цих пір, проте, це не працює, тому що ця технологія може бути реалізована тільки після затвердження положення НБУ, що регулюють здійснення активних операцій через Interpnet рахунків.

ВАБанк. Банк провів "тест" для співробітників системи, яка дозволяє власникам кредитних карт, емітованих трасу через сторінку Interpnet всіх банківських операцій від їх «візитною карткою» рахунків. Будь-яка відміна кредитної картки оперативно відображаються у виписці по рахунку, яку можна переглянути, відвідавши веб-сайт банку та введення правильного пароля.

Райффайзенбанк Україна. За даними агентства "Інтерфакс-Україна", голова ради Ігоря Францкевича кінці липня оголосив, що банк реалізував проект для підключення системи Клієнт - Банк Канал Interpnet. Використовуючи цю послугу, клієнти банку зможуть не тільки отримати довідку про стан своїх рахунків, а й відправити платіжне доручення, а також відкритий кредит, перебуваючи в будь-якій точці світу.

Приват. У лютому 1999 року "ПриватБанк" запропонував своїм клієнтам спеціальну карту Interpnet, який можна використовувати тільки для платежів мережі Interpnet (Interpnet в магазинах, які приймають картки Visa платежів з використанням). Interpnet карти можуть забезпечити доступ до карткового рахунку разом з "нормальним" карту, що дозволяє зберегти секретну кімнату "перший" звичайних карт при здійсненні платежів Interpneti. Interpnet карта має PIN-код і з його допомогою ви не можете отримати гроші в банкоматі.

«Аваль». У 1999 році банк «Аваль» запропонував клієнтам можливість отримання виписки з рахунку по електронній пошті (електронною поштою адресу клієнта). У даний час спільно з американською компанією, ім'я якого не розкривається, банк, створений ТОВ "Informeks", що спеціалізується на реалізації Interpnet комерція (продаж товарів і послуг компаній-клієнтів через Interpnet). "Informeks" є sertyfikovannim "хостинг-провайдер" (представницьких) в Україні німецько-американська компанія IntershopCommunication. Серед проблем "Informeks" - реалізація Interpnet комерції і "хостінг" (більш формально називається розміщення, обслуговування та захисту інформації клієнта до сервера компанії) і надання електронних платежів за допомогою банківських платіжних систем. В даний час "Informeks" надає київська компанія "Новий вітер", NoosUkraine, FlamingoDigitalUkraine і веде переговори з іншими компаніями.

Крім того, «Аваль» реалізувала ряд проектів з INT і вже відбув чотири платежу Interpnet-магазинів. Особливості цих Interpnet, магазини, які насправді платити карта може бути видана тільки банком «Аваль», і що служив в магазині Interpnet, клієнти повинні відвідати цей магазин банк і отримати спеціальне ПЗ, що дозволяє захистити оплати (цифрові сертифікати, необхідні для авторизації платежів).

Програми в «мобільній» поля вже реалізовано "Аваль" і ПриватБанк, працюючи відповідно з операторами UMC та Київстар GSM. Суть в тому, що служби, використовуючи певні комбінації клавіш набрані на мобільних клієнтах банківських телефону може дізнатися, скільки грошей знаходиться в їх «мобільних» рахунку. За наявною у нас інформацією, готується аналогічний проект ВАБанку з ЗАТ «Українська radyosystemи" (Wellcom).

Пільги для нових банківських технологій очевидно ілюструє першу мережу банку SecurityFirstNetworkBank (SFNB). Цей банк в даний час більше 10 000 клієнтів по всій території Сполучених Штатів. Тим не менш, у нього є тільки одна гілка знайомі і той факт, тільки тому, що Наглядова комітет операцій (організація контролю за діяльністю банків у США) поки не має достатньої правової основи для регулювання діяльності банків, які існують тільки в кіберпросторі. Банк орієнтується в першу чергу на користувачів Інтернету, число яких складає більше 10 мільйонів чоловік.

Обчислювальний центр Атланти має тільки Hewlett-Packard серверів під Unix. Сервер комп'ютерного центру (інформаційні сервери, безпеки і сервери баз даних) мережевого IOBase-T з TCP / IP. Компанія має намір модернізувати мережу до 100 Мбіт / с. Перехід глобальної мережі здійснюється два резервних каналів T-1 через фільтруючий маршрутизатор для захисту мережі. Клієнти звертаються до банку через вузол WorldWideWeb (http://www.sfnb.com).

Інший приклад - компанія SharlesSchwab, яка має 3,5 мільйона клієнтів і активи на $ 2 млрд. - одна з найбільших інвестиційних компаній, прийняв Інтернеті.

У травні 1997 року Schwab відкрила доступ до клієнтів через Інтернет на сайт WorldWideWeb (http://www.Schwab.com). Є й інші методи доступу:

відділення та брокерські на ПК з використанням власного програмного забезпечення називається StreetSmart.

На сьогоднішній день обсяг операцій, здійснюваних з використанням ПК, становить 15% від діяльності компанії. У той же інтернет-послуги доступні тільки тим клієнтам, чий рахунок Schwab становить не менше $ 5000. Платежі здійснюються через Інтернет, набагато менше, ніж звичайних зборів.

Одним з перших надану можливість веб-банкінгу в Приват банківського ринку, і ця система вже функціонує і називається Приват24. Насамперед, Приват24 послуг для фізичних та юридичних осіб різні. Якщо люди можуть виконувати ряд операцій з наявними в їх карти і звичайні рахунку (відкриття, звичайно, Privat) юридичної особи через веб-браузер тільки звіт за період і сальдо рахунку поточних операцій (слід зазначити, що тих, хто не використовує "Клієнт-банк", але хоче віддалено контролювати стан рахунку, ми можемо рекомендувати даний сервіс через свою простоту, простоти використання і низької вартості -. 10 грудень в місяць) (rys. 1.5.).

Нехай список послуг для фізичних осіб більше. У зв'язку Приват24 пропонуються в Інтернеті всі рахунки, відкриті на вас як особистість (у тому числі рахунки і Interpnet пластикової карти), з яким ви можете виконувати наступні операції:

контроль залишків рахунку;

отримання виписок за рахунками;

Intra-платежів рахунків фізичних та юридичних осіб;

міжбанківські платежі в межах України на рахунки фізичних та юридичних осіб;

перетворення при переказі коштів між рахунками (картковими і поточними);

відкривати рахунки в національній та іноземній валютах.

Ті, хто тісно співпрацювати зі своїми платіжними картами (наприклад, робити покупки в звичайних магазинах і Interpnet) по достоїнству оцінить перших двох послуг, які насправді підписати контракт на використання

системи - "залишки контролю облікових записів" і "отримувати виписки по рахунках". Той факт, що контроль за рухом грошових коштів на карт для

місяць, як звичайно, немає ніякого способу, щоб рішуче: контролювати правильність скасування або отримання карти ви зможете тільки після 10-го числа наступного місяця у пресі, яка доступна в своїй галузі. І якщо ви не згодні з будь-якої угоди, то ви оскаржити його не дуже довго. Використовуючи той же Приват24 скасування може контролювати і потік карти в режимі реального часу, заяви і залишки на рахунках в Інтернеті. Це по-перше.

Друга велика можливість - це можливість переводити кошти між картковими рахунками та міжбанківські платежі в межах України на рахунки фізичних і юридичних осіб. Якщо перше зрозуміло, це має бути зроблено з другим пунктом: грошовий переказ на рахунок іншої особи можна без проблем з фразою "передача особистих коштів", яка полягає у передачі підприємством коштів не так просто . для цього вам потрібно буде вказати в номер платежу і дата документа (рахунки-фактури, договору), згідно з яким компенсація. Без цієї інформації ви будете перерахування грошових коштів відмовлено. Платежі здійснюють до 17 годин і 15 хвилин, проведеного в поточному днів, після чого - таким чином.

Гідно оцінять ці функції користувачів системи Webmoney, які почали свою роботу в Україні в webmoney.com.ua. З Приват24 гривні на WM, або навпаки, отримувати гривню безпосередньо у Вашу пластикову карту в обмін на WM може бути протягом декількох хвилин до декількох годин, в залежності від ефективності роботи операторів.

1.3 Законодавча база України, щодо порядку здійснення криптографічного захисту інформації в Україні

Для побудови та подальшого розвитку інформаційного суспільства в нашій країні, одним з першочергових напрямів є створення нормативно-правової бази, яка б регулювала інформаційні відносини на законодавчому рівні.

На законодавчому рівні відносини, пов'язані з інформацією, інформаційно-комунікаційними технологіями, визначаються як пріоритетні. Законом України „Про пріоритетні напрями розвитку науки і техніки” поміж семи п’ятим пріоритетом визнано новітні комп'ютерні засоби та технології інформатизації суспільства.

За останнє десятиліття в Україні прийнятий досить законів і правил, які були покладені в основу правового регулювання інформаційних відносин в тому числі й електронних записів.

Законодавство, засноване на принципах відкритості та свободи інформації, безпека інформації, безпеки особистості, суспільства і держави відповідно до Конституції України. Законодавство, покликане регулювати конфлікти між потребами особи, суспільства і держави в розширенні спектру вільного обміну інформацією та деякі обмеження на її поширення.

Перелік законів України, Верховної Ради України, актами Президента України та Кабінету Міністрів України, актами окремих міністерств наведені в таблиці 1.3.1, які є нормативно-правової бази для правового регулювання інформаційних технологій , так і безпосередньо, два з наступних законодавства, які стосуються предмета дослідження. Цей закон "Про електронний цифровий підпис" і "Про електронні документи та електронних документів." Ці закони

регулюють загальні відносини в електронні документи. Це має сенс розглянути їх докладніше.

Закон України "Про електронні документи та електронний документі» був прийнятий у травні 2003 року. Цей закон встановлює основні організаційні та правові засади електронного документообігу та використання електронних документів. У контексті цього Закону, електронний документ розглядається як документ, який zafiksovuyetsya інформація у вигляді електронних даних, включаючи відомості, необхідні документи та електронний документ як сукупність процесів створення, обробки, передачі, відправки, отримання, зберігання, використання та отримання електронних документів, які повинні бути виконані за допомогою перевірки цілісності та, при необхідності, підтверджується факт надходження цих документів. Електронний підпис потрібно реквізит використовується для ідентифікації автора або електронному документі Послідовники інших бізнес електронного документа. У свою чергу, вплив електронного документа не може бути відмовлено тільки тому, що вона має форму онлайн. Законом регулюються правові відносини у питаннях:

- електронного підпису;
- електронного цифрового підпису;
- правового статусу електронного документа та його копії;
- одержання електронних документів;
- оригіналу електронного документа;
- відправлення та передавання електронних документів;
- обігу електронних документів, що містять інформацію з обмеженим доступом;
- перевірки цілісності електронного документа;
- зберігання електронних документів та про архіви електронних документів;
- вирішення спорів між суб'єктами електронного документообігу;
- організації електронного документообігу;
- права та обов'язки суб'єктів електронного документообігу;

- відповідальність за порушення законодавства про електронні документи та електронний документообіг;
- вирішенню спорів між суб'єктами електронного документообігу.

Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають під час використання електронного цифрового підпису. В цьому Законі визначено терміни:

електронний підпис – це дані в електронній формі, які призначені для ідентифікації підписувача цих даних, що додаються до інших електронних даних або логічно з ними пов'язані ;

електронний цифровий підпис – це один з видів електронного підпису, що отриманий за результатом криптографічного перетворення набору електронних даних, і який додається до цього набору або логічно з ним поєднується та дає змогу ідентифікувати підписувала та підтвердити його цілісність. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Електронний цифровий підпис призначається для забезпечення діяльності фізичних та юридичних осіб, і здійснюється з використанням електронних документів. Електронний підпис не може бути визнаний недійсним лише через те, що він не ґрунтується на посиленому сертифікаті ключа і має електронну форму . Закон також зазначає:

- суб'єктів правових відносин у сфері послуг електронного цифрового підпису;
- особливості застосування електронного цифрового підпису;
- права і обов'язки підписувача;
- відповідальність за порушення законодавства про електронний цифровий підпис;
- центр сертифікації ключів;
- визначає іноземні сертифікати, ключі тощо.

У таких країнах як ЄС, Канаді, США та ін. цифрові підписи й сертифікати затверджені як еквівалент власноручного підпису на законодавчій основі. Країни ЄС ухвалили національні законодавчі акти, що цілком відповідають Директиві Європарламенту та Ради Міністрів ЄС 1999/93/ЄС про систему електронних підписів, яка застосовується в межах Співтовариства, та рішенню Комісії 2000/709/ЄС Європарламенту і Ради. На сьогодні усі положення Директиви 1999/93/ЄС реалізовано у вигляді технічних європейських та міжнародних стандартів (ETSI та RFC).

Проте, провідні українські юристи кажуть, що Закон України «Про електронний цифровий підпис" не знайдено жодного європейського або міжнародного права в цілому. На підтвердження цьому, наприклад, "електронного підпису" у визначенні ЄС - електронний підпис ЄС та додаткові вимоги до надійності, яка технічно означає, що шлях для створення підпису повинні задовольняти вимогам стандартів FIPS 140-1, 140 - 2 Рівень 2, 3 (Федеральні стандарти обробки інформації, США). Цей термін у законі України не існує, а є термін «електронного підпису», який відповідає ЄС електронного підпису в криптографії з відкритим ключем. З точки зору ЄС і відповідають європейським і міжнародним стандартам ввів термін «кваліфікованої електронного підпису", яка схожа на нашу закону №.

З метою подальшого розвитку нормативно-правової бази, необхідної - визнати членство України в Міжнародній організації по стандартизації ISO у практиці, ратифікувати міжнародні договори, розробки і здійснення необхідних технічних та інших стандартів, які діють у Європі, і адаптувати існуючі із законами ЄС. Паралельно з цим, слід зазначити, що навіть прискорений дій у цій області не буде в змозі забезпечити швидкий ефект нових відносин в електронних документах через відставання розвиваються підзаконними актами. І вже тим більше, впровадження електронних документів в практиці державних установ, які тісно пов'язані з необхідністю реформування практичної роботи

державних службовців, і, отже, прискорення адміністративної реформи та електронного бізнесу прийняти Закон України "Про електронну торгівлю".

Таблиця 1.3.1

Перелік нормативно-правових актів щодо застосування електронного документообігу

№ п/п	Назва документа	Дата введення в дію
1.	Закон України «Про електронні документи та електронний документообіг»	22.05.2003
2.	Закон України «Про електронний цифровий підпис»	22.05.2003
3.	Закон України «Про телекомунікації»	18.11.2003
4.	Закон України «Про інформацію»	02.10.1992
5.	Закон України «Про державну таємницю»	21.01.1994
6.	Закон України «Про обов'язковий примірник документів»	09.04.1999
7.	Закон України «Про Національну програму інформатизації»	04.02.1998
8.	Постанова Верховної Ради України «Про Концепцію національної інформаційної політики»	03.04.2003
9.	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»	05.07.1994
10.	Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2005–2007, 2007–2015 роки»	09.01.2007
11.	Закон України «Про стандартизацію»	11.01.2006

12.	Закон України «Про Національну систему конфіденційного зв'язку»	10.01.2002
13.	Закон України «Про Національний архівний фонд та архівні установи»	24.12.1993
14.	Постанова Кабінету Міністрів України «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу»	26.05.2004
15.	Постанова Кабінету Міністрів України «Про затвердження Порядку акредитації центру сертифікації ключів»	13.07.2004
16.	Постанова Кабінету Міністрів України «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності»	28.10.2004
17.	Розпорядження Президента «Про приєднання до Угоди про створення Міжнародної системи документального шифрованого зв’язку Співдружності Незалежних Держав»	06.12.2005
18.	Постанова Кабінету Міністрів України «Про затвердження Порядку обов’язкової передачі документованої інформації»	28.10.2004
19.	Постанова Кабінету Міністрів України «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої	28.10.2004

	влади»	
20.	Постанова Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган»	28.10.2004
21.	Служба безпеки України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави»	27.11.1998
22.	Постанова Кабінету Міністрів «Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади»	17.10.1997
23.	Постанова Кабінету Міністрів «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу»	26.05.2004
24.	Постанова Кабінету Міністрів «Про затвердження Порядку акредитації ЦСК»	13.07.2004
25.	Постанова Кабінету Міністрів «Про затвердження Положення про ЦЗО»	28.10.2004
26.	Постанова Кабінету Міністрів «Про затвердження Порядку застосування ЕЦП»	28.10.2004
27.	Постанова Кабінету Міністрів «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади»	28.10.2004

28.	Постанова Кабінету Міністрів «Про затвердження Порядку обов'язкової передачі документованої інформації»	28.10.2004
29.	Указ Президента України «Положення про порядок здійснення криптографічного захисту інформації в Україні»	15.09.1998
30.	Держкомзв’язку «Перелік і Порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи "Електронний Уряд”»	15.08.2003

Відсутність чітко сформульованого і систематизованого законодавства як із питань захисту і безпеки, так і в області електронної комерції взагалі не зупиняє тих, хто всерйоз зайнявся Інтернет-бізнесом. Необхідне для них юридичне обґрунтування власної діяльності вони складають самотушки, вишукуючи у численних законодавчих актах, указах і інструкціях. Але для тих, хто лише роздумує про нову справу, правова невизначеність є одним із бар'єрів на шляху в Інтернет. Та все-таки почалися зміни до кращого в законодавчому середовищі, і дають підстави сподіватися, що в недалекому майбутньому юридичні питання будуть урегульовані краще.

Криптографія асиметричних ключів представляє собою найбільш надійний спосіб захисту інформації, який забезпечує вирішення всіх перерахованих вище завдань. Суть його полягає утому що клієнт створює пари ключів (секретний і відкритий), із яких відкритий ключ передається в Банк, секретний знаходиться в розпорядженні клієнта і відомий тільки йому. Передані дистанційні розпорядження спершу шифруються і підписуються електронно-цифровим підписом на секретному ключі клієнта. Банк в свою чергу перевіряє підпис за допомогою відкритого ключа.

Використовуючи криптографічний захист велике значення має надійне збереження секретного ключа. Задля збереження можуть використовуватися звичайні носії інформації (дискета, жорсткий диск) або захищені носії (смарт-картки, таблетки пам'яті). Найнадійнішим представляється спосіб, коли збереження робиться в EEPROM-пам'яті смарт-картки і криптографічні обчислення також робляться в пам'яті смарт-картки. За такого способу секретний ключ клієнта ніколи не покидає захищеного простору смарт-картки, чим і забезпечується найвищий ступінь захисту секретної ключової інформації від несанкціонованого доступу до інформації.

Одним з недоліків криптографічного захисту є необхідність навчання клієнтів користуватися такими засобами. При використанні смарт-карток і таблетки-пам'яті недоліком ще є висока ціна (від 5 долл.) і необхідність використання спеціальних картрідерів.

Ліцензійна палата України Департамент спеціальних телекомунікаційних систем і захисту інформації СБ України видала наказ N 104/81 від 17.11.98 р.. Зареєстровано в Міністерстві юстиції України 30 листопада 1998 р. vd981117 vn104/81 N 760/3200 про затвердження Інструкції про умови і правила здійснення підприємницької діяльності (ліцензійні умови), пов'язаної з розробкою, виготовленням, ввезенням, вивозом, реалізацією і використовуванням засобів криптографічного захисту інформації, а також з наданням послуг з криптографічного захисту інформації, і контроль за їх дотриманням.

1. Загальні положення

1.1. Ця Інструкція розроблена відповідно до Законів України "Про підприємництво" (698-12), "Про інформацію" (2657-12) і "Про державну таємницю" (3855-12); Положенням про порядок здійснення криптографічного захисту інформації в Україні, затвердженим Указом Президента України від 22 травня 1998 року N 505/98; Положенням про Ліцензійну палату України, затвердженим Указом Президента України від 16 липня 1997 року N 648/97, і у виконання ухвали Кабінету Міністрів України від 3 липня 1998 року N 1020 (1020-98-п) "Про порядок ліцензування підприємницької діяльності". Дія

Інструкції розповсюджується на всіх суб'єктів підприємницької діяльності, які здійснюють діяльність у області криптографічного захисту інформації, незалежно від їх організаційних форм господарювання і форм власності.

1.2. Інструкція визначає умови і правила здійснення підприємницької діяльності (ліцензійні умови), пов'язаної з розробкою, виготовленням, ввезенням, вивозом, реалізацією і використовуванням засобів криптографічного захисту інформації, а також з наданням послуг з криптографічного захисту інформації, і контроль за їх дотриманням.

1.3 Використані в даній Інструкції терміни мають таке значення:

заявник - суб'єкт підприємницької діяльності, який подав заяву на здійснення певного виду діяльності;

криптографічний захист інформації - вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її достовірності, цілісності, авторства і тому подібне;

засіб криптографічного захисту інформації - програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації;

разовий (сеансовий) ключ - спеціальні дані, які задають програму роботи засобу криптографічного захисту інформації на певний проміжок часу;

устаткування криптографічного захисту інформації - технічні засоби, які взаємодіють із засобами криптографічного захисту інформації або керують ними, а також можуть впливати на їх криптографічні якості;

товари подвійного використовування - окремі види виробів, устаткування, матеріалів, програмного забезпечення і технологій, а також роботи і послуги, св’язані з ними, які, окрім основного цивільного призначення, можуть бути використані під час розробки, виробництва або використовування озброєння, військової або спеціальної техніки, які є об'єктом покупки-продажу або обміну.

1.4 До засобів криптографічного захисту інформації відносяться:

- апаратні, програмні і апаратно-програмні засоби, які реалізують криптографічні алгоритми перетворення інформації;

- апаратні, програмні і апаратно-програмні засоби, системи і комплекси захисту від нав'язування неправдивої інформації, включаючи засоби імітозащити і "електронного підпису", які реалізують криптографічні алгоритми перетворення інформації;

- апаратні, програмні і апаратно-програмні засоби, системи і комплекси, предназначениє для виготовлення і розподілу ключових документів, які використовуються в засобах криптографічного захисту інформації, незалежно від виду носія ключової інформації;

- системи і комплекси (зокрема ті, які входять в системи і комплекси захисту інформації від несанкціонованого доступу НСД), до складу яких входять апаратні, програмні і аппаратнопрограммниє засоби, які реалізують криптографічні алгоритми перетворення інформації.

1.4 Особливі вимоги для персоналу, об'єктів, таємниці (безпека), інформаційно-обчислювальних систем, регулюючи стенди, виробничі приміщення і області, вимірювальної техніки та контролю, технічного та оперативного обліку підприємств регулюються відповідними положеннями та іншими Департаменту правил.

2. Умови діяльності у галузі криптографічного захисту

2.1. Суб'єкти господарювання повинні мати:

- Повний робочий день співробітників, як заявленої діяльності та обсягу роботи (за кількісним складом, професійної підготовки, досвіду і кваліфікації); кошти, необхідні для проведення зазначених заходів.

2.2. Суб'єкти господарювання повинні мати внутрішнє положення, яке визначає завдання і функції кожного структурного підрозділу, функціональні обов'язки кожного фахівця і свою відповідальність за збереження конфіденційної інформації у виставі.

2.3. Суб'єкти господарювання повинні забезпечити секретність (при виконанні робіт, пов'язаних з державною таємницею).

2.4. В установчих документах комерційної організації, повинні бути надані для здійснення своєї діяльності.

3. Додаткові умови мають бути дотримані при розробці та виробництві засобів криптографічного захисту інформації

3.1. Суб'єкти господарювання повинні мати:

- Інформаційні та комп'ютерні системи (в області програмного забезпечення, апаратних засобів і програмного забезпечення захисту криптографічних);

- Введення в експлуатацію стендах, розроблених для моделювання обладнання у довільні інтервали роботи;

- Відповідні виробничі потужності і районів, засоби вимірювання та контролю і правильні інструменти.

3.2. Суб'єкти господарювання повинні мати свої власні можливості провести ремонтно-реставраційні роботи (виробництво засобів криптографічного захисту інформації).

4. Додаткові умови, яким повинні слідувати використання криптографічного захисту інформації

Підприємець повинен мати:

- Правильне технічної та експлуатаційної документації;

- Інструкції та графіки з технічного обслуговування обладнання, яке потребує періодичного обслуговування.

5. Особливі умови, яким необхідно слідувати

Залежно від важливості інформації для особистості, суспільства, держави та правового режиму доступу до інформації певного набору заходів у галузі криптографічного захисту інформації:

- Положення закону працює в галузі криптографічного захисту, яка застосовується до державної таємниці;

- Положення закону працює в галузі криптографічного захисту конфіденційної інформації створюються за наказом уряду, або у власності держави;

- Положення закону працює в галузі криптографічного захисту конфіденційної інформації.

Обраний особливі умови повинні бути відображені у відповідній ліцензії пункт, який видається суб'єктам підприємницької діяльності.

6. Правила, яких необхідно дотримуватися у галузі криптографічного захисту

За час своєї діяльності, відповідно до отриманої ліцензії, підприємці повинні дотримуватися таких правил:

- Записуйте від загального обсягу виконаних робіт;

- У відповідності з правовими та нормативно-технічної керівних документів;

- Містять обладнання і контрольно-вимірювальної апаратури в умовах, що забезпечують їх збереження і захист від пошкоджень.

7. Права та обов'язки підприємств

7.1. Суб'єкти господарювання при здійсненні діяльності у галузі криптографічного захисту мають право:

- Звернувшись у відділ по консультації та допомогу, необхідну для здійснення діяльності litsenziyuyetsya;

- Отримувати інформацію від відділу з правової та методичної бази в галузі криптографічного захисту,

- Оскаржити дії Департаменту у відповідності з законом.

7.2. Суб'єкти господарювання при здійсненні діяльності у галузі криптографічного захисту інформації необхідно:

- Здійснювати свою діяльність відповідно до вимог Правил;

- Встановіть для забезпечення секретності, якщо інформація про роботу, виконану є таємницею;

- Встановіть для забезпечення безпеки, якщо інформація про виконаної роботи є конфіденційною;

- Для того щоб співробітники департаменту, які мають відповідні повноваження для виконання наглядових функцій на своїй території та надавати їм всю необхідну інформацію;

- Негайно повідомляти відділ будь-якому випадку в результаті цікаву структуру (и) може отримати інформацію про несанкціоновану роботи, що мають секретний або конфіденційного характеру;

- Негайно інформувати Департамент змін в операційних умовах, визначених цим Положенням;

- Відповідно до Положення про здійснення криптографічного захисту України, затвердженого Указом Президента України 22 травня 1998 р. N 505/98, для криптографічного захисту інформації є державною таємницею, та службової інформації створених за замовленням органів державної влади або яке належить державі реалізувати і використовувати криптосистем і засобів криптографічного захисту дозволено використовувати;

- Відповідно до Положення про здійснення криптографічного захисту України, затвердженого Указом Президента України від 22 травня 1998 р. N 505/98, для криптографічного захисту конфіденційної інформації та використовувати її для реалізації криптосистем і засобів криптографічного захисту, які пройшли сертифікацію.

Суб'єкта підприємництва не може передавати ліцензію на використання інших.

8. Контроль за виконанням суб'єктами підприємницької діяльності умов і правил здійснення діяльності у області криптографічного захисту інформації

8.1. Перевірка виконання суб'єктом підприємницької діяльності ліцензійних умов і правил здійснення діяльності у області криптографічного захисту інформації здійснюють Департамент і Ліцензійна палата. Про термін проведення перевірки Департамент повідомляє у письмовій формі суб'єкта підприємницької діяльності за десять календарних днів до її проведення.

8.2. Контроль за виконанням суб'єктами підприємницької діяльності ліцензійних умов проводиться Департаментом і Ліцензійною палатою України планово не більш один раз на рік, а також за рекламацією замовника або для вирішення питання щодо відновлення дії ліцензії.

8.3. У разі порушення суб'єктом підприємництва ліцензійних умов здійснення діяльності у області криптографічного захисту інформації

Департамент видає обов'язкові для виконання суб'єктом підприємницької діяльності розпорядження щодо усунення порушень або зупиняє дію ліцензії на певний термін або до усунення цих порушень.

8.4. У повідомленні про зупинку дії ліцензії, яка видається суб'єкту підприємницької діяльності у письмовій формі в строк не пізніше 5 днів з дня ухвалення рішення, указуються підстави такого рішення.

8.5. Дія ліцензії може бути відновлене у разі усунення знайдених порушень. Рішення про відновлення дії ліцензії ухвалюється Департаментом на підставі акту контрольної перевірки.

8.6. У разі повторного або грубого порушення суб'єктом підприємницької діяльності умов здійснення певного виду діяльності ліцензія може бути анульована.

До грубих порушень умов здійснення діяльності у області криптографічного захисту інформації відносяться:

- невиконання вимог нормативно-правових, нормативно-технічних і методичних документів, які регламентують здійснення діяльності у області криптографічного захисту інформації;

- незабезпечення режиму секретності (режиму безпеки);

- виконання робіт з порушенням вимог проектної документації;

- залучення до виконання робіт фахівців, рівень підготовки яких не відповідає вимогам цієї Інструкції.

8.7. Рішення про анулювання ліцензії ухвалюється Департаментом на підставі акту контрольної перевірки.

8.8. У повідомленні про анулювання ліцензії, яке видається суб'єкту підприємницької діяльності у письмовій формі в строк не пізніше 5 днів з дня ухвалення рішення, указуються підстави такого рішення.

Висновки до розділу 1

Інтернет-банкінг є складовою частиною політики, спрямованої на збільшення обсягу залучених коштів, та впровадження нових банківських послуг, які користуються попитом на ринку, і його пропонують клієнтам все більша кількість установ вітчизняної банківської системи.

Інтернет-банкінг виступає в ролі універсального інструмента збільшення залучених коштів шляхом зростання клієнтської бази комерційного банку та розглядається як ефективний метод залучення нових клієнтів за допомогою створення більш зручних умов дистанційного використання обумовленого спектру послуг. По своїй суті Інтернет-банкінг являє собою логічне продовження таких різновидів віддаленого банкінгу, як PC banking: тобто доступ до банківського рахунка за допомогою ПК, що здійснюється при прямому модемному з'єднанню з банківською мережею, telephonebanking: ведення рахунків за телефоном та videobanking: система побудована на інтерактивному спілкуванні клієнта з персоналом банку. Характеристика нормативно-правової бази, яка регулює інформаційні відносини в державі та забезпечує реалізацію державної політики в питаннях документообігу, діловодства, дає систематизовану теоретичну базу дослідження під час запровадження електронного документообігу. У контексті сучасних уявлень діловодство та документообіг є одним із найважливіших засобів керування в установі та складовою здійснюваних у ній процесів інформаційного менеджменту, зокрема реалізованих за допомогою новітніх інформаційних технологій.

В якості прикладів передових технологій, що використовуються в банківській справі, ви можете зателефонувати в бази даних на основі моделі "клієнт-сервер" (характерне використання Unix операційних систем і баз даних Oracle); взаємодія кошти для міжбанківських платежів, оплата послуг, це зосереджено на Інтернет, або так звані віртуальні банки, банківські експертно-

аналітичні системи, використовують принципи штучного інтелекту і багато іншого.

Придбання та встановлення, і, особливо, розвивають свою систему Інтернет-банкінгу - задоволення не з дешевих. Крім того, перехід до віддаленої службі потрібна істотна коригування (реінжиніринг) бізнес-процесів і пов'язаних з цим зборів банку. Однак багато банків вкладають кошти в цей бізнес. Аналіз показує, що така поведінка пов'язана з банками тверезий розрахунок і об'єктивні чинники.

Щодо основних можливостей, пропонованих використання банку Інтернету, слід зазначити, що мережа Інтернет, в принципі, застосовні до різних областей банку - від взаємодії з клієнтами для обміну інформацією з іншими банками.

Головна перевага Інтернет-банкінгу - простий у використанні і економію часу. Таким чином, ми повинні подбати про те, щоб уникнути складної процедури доступні, тривалості і складності операцій. Система повинна бути максимально простою у використанні і працювати швидко. Ті, хто досягає успіху зможуть захопити більшу частину ринку.

Однак той факт, що використання банківської системи і роботи в Інтернеті більшість людей соціально активних, дає надію, що їх кількість буде достатньо, щоб принаймні на початковому етапі, на ранніх стадіях розгортання Інтернет-банкінгу. Зараз переважна більшість банкірів вважають, що зручність використання Інтернет-послуг у найближчому майбутньому стане важливим фактором у залученні коштів клієнтів у банках.

Що стосується психологічних труднощів, то вони повинні pryrahuvaty бояться втратити свої гроші в Інтернеті. Інтернет-банкінг не йдуть на користь численні публікації на масовий злом і крадіжку комп'ютерних систем. Тим не менше, я думаю, що ця проблема носить технічний і правової коріння, ніж технічні або будь-які інші.

РОЗДІЛ 2. КОМПЛЕКСНИЙ АНАЛІЗ ВИКОРИСТАННЯ БАНКАМИ МЕРЕЖІ INTERNET В КОМЕРЦІЙНИХ ЦІЛЯХ.

2.1 Переваги та недоліки Інтернет як середовища передачі фінансової інформації

На рахунок зручності і банку, і для клієнта в використанні Інтернет-простору то навряд чи хто заперечить. Спробуємо розглянути основні позитивні сторони :

Зменшення вагомості «географічної складової» при роботі з клієнтами. Ще донедавна зросли об'єми міграції, через зміну місць постійного проживання і роботи клієнтів, і це позбавляло банки тієї частини клієнтів, що користувалися їхніми послугами за територіальною складовою, тільки тому, що банк знаходився в беззаперечній близькості від їхнього місця проживання або роботи. Банки втрачали клієнтів, що довіряли «бренду» банку, і які змушені були залишити банк, у зв’язку з переїздом в іншу країну або регіон, де не розміщенні філії цього банку. Виходячи з цього, при дистанційному обслуговуванні банк має можливість надавати свої послуги клієнтам, незалежно від того де вони знаходяться, потрібен тільки доступ до мережі інтернет.

Немає часових меж. Час набуває все більшої цінності, і це особливо болюче для ділових сфер, коли час це гроші, а гроші ніколи не сплять. Глобалізація діяльності міжконтинентальних бізнес-структур, які знаходяться в різних часових поясах, надавало їм незручності з різницею в часу для прийнятті ділових рішень. Зазвичай в клієнта банку ухвалення рішення про користування послугами банку прямо залежить від часу обслуговування, необхідного для цієї або іншої послуги. За цих умов грає велику роль також швидкість комунікацій та інтернет-процесів і якість інформації, що передається. З погляду тимчасових витрат, очевидно, що для клієнтів цілком вигідніше використовувати цілодобову систему дистанційного обслуговування за невелику плату, ніж нести великі втрати.

Постійне підвищення якості комунікацій. Сама процедура обміну даними важлива як для клієнта так для банку, тому особливої уваги потребує питання якості комунікаційних процесів. Комунікації при дистанційному банківському обслуговуванні через Інтернет характеризуються високим ступенем інтерактивності і зменшенні часу, необхідного для передачі, збереження й опрацювання даних.

Підвищення конкурентоспроможності. Інтернет-банкінг дозволяє легко збільшувати бізнес-процеси, як число «віртуальних» філія в такій системі або послуги не залежить від зростання числа клієнтів, ні зниження. В інтерактивному середовищі глобальної комп'ютерної мережі дозволяє створювати абсолютно нові банківські продукти та створити попит на їх зв'язок з інтернет-маркетингу.

Зниження витрат. Використовуючи Інтернет, щоб запропонувати банківські послуги, що дає реальну економію коштів, зниження експлуатаційних витрат за рахунок скорочення витрат на управління філіями, економія на заробітній платі. Jupiter Communications підрахували, що середня вартість операції через філію в 1,07 долара поштою - 0,73 доларів. По телефону - 0,54 доларів. У банкоматах - 0,27 доларів. А Інтернет - 0,02 доларів.

Інтеграція бізнес-процесів з іншими фінансовими продуктами і послугами, які використовують віддалений доступ до фінансових рахунках. До цих пір одним з основних умов для ефективної роботи, і, отже, "виживання" дистанційного банківського обслуговування через глобальну мережу Інтернет інформації.

Організація даних клієнтів. В області банк не тільки отримує щомісячний дохід клієнта, але і всю інформацію про оподаткування відсотків за кредитами, переказ грошових коштів на рахунках, кредитних операцій і довіру клієнтів, а також купівельні звички та уподобання. Ця інформація досить, щоб зробити всеосяжний профіль клієнта.

Слід відзначити і недоліки. Робота з віддаленими каналами доступу неминуче відкриває нові можливості для зловживань, тому що безпека повинна

прийняти при розробці стратегій Телебанкінг важливе місце. Далеко від клієнта, банк втратив можливості людського спілкування.

Проблеми, пов'язані з інтернет-банкінгом, звичайно, більш ніж достатньо. Деякі з них пов'язані зі специфікою банківської справи, у зв'язку з унікальністю Інтернет індустрії. У ній вистачає, як філософських, організаційних, фінансових, технічних, кадрових, юридичних, проблем і навіть соціальні та психологічні. Розглянемо найважливіші.

Організаційні проблеми. Розробка і впровадження програмних систем, за винятком самих примітивних завжди вимагає значних організаційних зусиль. Якщо сума розподілених систем таких зусиль багаторазово зростає і для платіжних систем дійсно здорово, тому що вони перерахували обов'язкових домовленостей додається координація між усіма учасниками (зазвичай багато, і вони гетерогенні), або навіть створення умов для спільного розвитку. Крім того, професійні дії, необхідні, щоб принести нові системи оплати абітурієнтів. Досить проблем і при контакті з владою.

Фінансові проблеми. Той факт, що нові технології привели до активний споживач фінансових ресурсів, знають усі, але от масштаби споживання далеко не кожен. На знак визнання піонерів Росії Інтернет-банкінг - представники Гута-банк і Автобанк, їх вже відносно розкручується платіжних систем буде в змозі погасити тільки 2 - 3 років при зберіганні зростаючого числа клієнтів і збільшення обороту коштів.

Якщо повернення системи онлайн оплата не пройшла, то харчовий "Інтернет - Клієнт" Інша справа - вони спочатку думали, як прямо засіб збільшення прибутку. Їх завдання - забезпечити якісне обслуговування клієнтів. Оцінити окупний чи ні "Інтернет - Клієнт" важко, тому що основна частина - непрямі вигоди. У будь-якому разі, той, хто впроваджує систему Інтернет повиннен бути готовий до основних витрати. При цьому істотно, щоб уникнути помилкових спроб досягти рентабельності проекту в короткостроковій перспективі - за рахунок збільшення вартості обслуговування клієнтів. Інтернет не ставить за меті рішень - він розрахований на маси і

deshevist обслуговування. Але вартість банківської системи Інтернет може бути дуже високою.

Існує ще один важливий фінансовий аспект Інтернет-банкінгу - учасник системи електронних платежів, як правило, потрібна для резервування (тобто заморожування) певну суму грошей. Таким чином, у разі міжбанківських платежів резервних фондів - це залишки на кореспондентських рахунках (розміри залишків може регулюватися) для клієнтів - це обмежує баланси, і т.д. Іншими словами, для зручності онлайн оплати гроші повинні бути виключені з активна циркуляція. Красиво вирішити цю проблему шляхом введення платіжним засобом, за допомогою якого можна оплатити в будь-якому місці (як у віртуальному і реальному світі). Схожі пропозиції - вони з області електронних грошей і смарт-карт - знаходяться на ринку, але вони все ще не мають головне - маса.

Фінансові проблеми і проблема рентабельності і вартості мікроплатежів. Ми знаємо, що Інтернет зручно робити невеликі придбання. Всього мікроплатежів за традицією на даний час менше 1 долара. Можливість виконання цих операцій з низьким відсотком є важливою перевагою системи з точки зору клієнтів, але його власники, це означає головний біль з точки зору прибутковості. Тим не менш, є приклади систем, які успішно справляються з цією проблемою, наприклад, допомагати або PayCash.

Кадрові проблеми. Якість та ефективність вирішення будь-якої проблеми залежить від кваліфікації, та якості персоналу. Для розвитку і підтримки інтернет-банкінгу сьогодні потрібно багато програмістів (і тих, хто працює не тільки в області інтернет-технологій), системних адміністраторів, веб-дизайнерів, веб-програмістів, фахівців в комп'ютерній та комунікаційної безпеки, економіки, маркетингу та юристів. Вони повинні мати гарне уявлення про світ Інтернету, який не завжди легко осягти. Важко, наприклад, знайти адвоката, який також є експертом з електронної комунікації, і це буде коштувати дорого. Те ж саме відноситься до професіоналів мережевої безпеки.

Я вважаю, що ступінь проникнення інтернету в повсякденне життя поступово з'являються суміжні професії, необхідні для роботи в області інтернет-банкінгу.

Пам'ятаючи про проблеми, що виникають при роботі в Інтернеті, ми повинні принести їх можливі рішення.

Невизначеність стандартів захисту даних від несанкціонованого доступу і стандартів електронних платежів (можна почекати затвердження необхідних стандартів у найближчому майбутньому).

Перевантаження мережі, необхідність у підвищених вимог до продуктивності серверів і пропускної спроможності каналів зв'язку через обсяг переданих даних і необхідності постійного оновлення, зростаючі (іноді ця проблема вирішується за рахунок використання виділеної смуги частот в мережі Інтернет) .

Різні обмеження потужності обробки інформації стандартними засобами доступу (існує кілька рішень цієї проблеми). Один з них вже широко поширений в світі і полягає в написанні спеціалізованого програмного забезпечення, яке використовує Інтернет і т.д., пов'язаних з використанням мови програмування Java, розроблений Sun Microsystems спеціально для використання серед інтернет).

2.2 Взаємодія з клієнтами банку через Інтернет. Фінансова інформація в мережі Інтернет

Використання глобальних комунікацій і зокрема Інтернету в якості каналу розповсюдження фінансової інформації - ризикове завдання. Розвиток цих проектів викликає ряд нових проблем, таких як, забезпечити доступ до успадкованих систем і як вирішити питання безпеки. Скрізь, де клієнт просить, необхідно забезпечити йому доступ до однієї бази даних.

Серед можливостей, наданих WWW-сервером банку клієнту, слід згадати можливість отримання інформації про поточний рахунок, взаємодію депозитарію та інші послуги. Що стосується здійснення грошових переказів у нашій країні для реалізації цього завдання вимагає часу. Проблеми безпеки в здійсненні таких проблем є не простою, але підходи зарубіжних банків заслуговують на увагу.

У сучасному світі у себе вдома через Інтернет на основі так званої віртуальної приватної мережі (VPN). Використання ВПМ організації використовують Інтернет в якості мережі і як глядач інтерфейс. Сьогодні ВПМ мають високий ступінь безпеки, але тому що вони засновані на прийняті рішення за умов обмеженої можливості їх мережевої взаємодії. Web-технології спочатку не дуже добре підходить для цілей захисту, у той же час, перехід до захищеного середовищі ще більше ускладнює проблему.

Необхідною умовою для розробки методу innshoho оплати вважається безпеки електронних транзакцій у відкритих мережах, а також для захисту серверів від несанкціонованого доступу. Нещодавно розроблені стандарти, такі як SKIP (простий ключ управління для інтернет-протоколу) з Sun Microsystems для захисту корпоративної мережі, а також SET (Secure Electronic Угоди) компаній Visa і MasterCard для шифрування платіжних операцій в Інтернеті готуємо технічну основу для надійної та безпечної проведення платежів через Інтернет.

Тепер група інженерної підтримки пропонованого стандартних засобів

безпеки в Інтернеті IPSec (Internet Protocol Security). Сумісність з IPSec надати перших виробників брандмауерів і стека TCP / IP.

Фірма Edify клієнти автоматизації програмного забезпечення доступу до інформації, розвитку їх додатків, спеціально для управління електронних банківських послуг. Тепер Edify пропонує продукт під назвою електронна платформа робочої сили. Вона призначена для забезпечення фінансовими установами для перемикання в інтерактивний режим. Основна проблема це рух є той факт, що в першу веб розглядати тільки як засіб розміщення статичної інформації. Сьогодні вони повинні з'єднати безліч інформації (часто зберігається в різних місцях) в єдину систему. Важливо також, що фінансові установи часто не можуть дозволити собі витрачати багато грошей на впровадження цих технологій у вигляді веб-тільки там, і хто знає, на який термін вкладені кошти окупляться.

Інтернет є багатим джерелом різноманітної фінансової інформації, необхідної банкам використовувати. Фінансові ресурси Інтернету можна розділити на такі групи:

Інформацію по різних компаніях;

Останні новини, що впливають на поведінку ринку, що представляють інтерес для фінансових установ;

Архіви фінансової, юридичної та іншої інформації, яка може бути використана для фінансового аналізу, такого як котирування, курси валют, інформація про діяльність компаній, закони і т. д.;

Оперативну фінансову інформацію в режимі реального часу (цит. біржовому та позабіржовому ринках для різних фінансових інструментів).

Розглянемо кожну з цих груп окремо:

Інформація про компанію. Через інтернет ви можете отримати інформацію про компанію, біржі, брокерські контори і т.д. Інше важливе джерело інформації про компанію, яка виступає в державних і комерційних організацій, які спеціалізуються на таких послугах. Однак, якщо послуги Pathfinder, наприклад, збір і аналіз інформації про найбільших компаніях США в традиційній манері, навряд чи доступно, використання Інтернету робить це

можливим. Під Гроші & Business Server зазначеного магазину Фортуна компанія надає доступ до своєї бази даних 500 найуспішніших компаній США.

Дуже корисне джерело інформації про компанії є проект Едгар (електронного збору даних і пошукова). Це база даних Комісії з цінних паперів США, що містять електронні файли великих і середніх американських корпорацій. Відповідний сервер забезпечує не тільки вихідні файли, але може працювати з ними, витяг найбільш цінної інформації для кінцевого користувача. Крім того, ряд українських фінансових установ має свій власний сервер, який містить інформацію про компанії, що представляють інтерес для клієнтів і партнерів.

Новини. Майже всі великі компанії, що працюють в індустрії новин світу з інформаційними серверами в Інтернеті. Інформаційне агентство «Рейтер» (Reuters), відоме у фінансовому світі через потужні засоби доступу до змісту інформації, має активну позицію в Інтернеті. Інтернет-технології широко використовуються у внутрішній корпоративній мережі Reuters. Можливість працювати в стандарті вбудований інтернет Reuters 3000 серії продуктів, які скоро з'являться на ринку.

Взагалі кажучи, своєчасне отримання важливих новин є настільки важливим для банку, що часто використовується для цієї мети, за допомогою систем спеціального призначення. Спільного ринку у своєму роді згадка Reuters, Dow Jones Telerate, Tenfore.

Значний обсяг інформації, який об'єднує аналітичні огляди, статті та довідкові бази даних на серверах skoplyuyetsya різних організацій.

Операційної та фінансової інформації. У всьому світі, особливо в США, в даний час активно розвиваються спеціалізовані сервісне пропозиція для тих, хто хоче підключитися до потоку професійної фінансової інформації за невелику суму. Загалом, набори серверів, фінансових послуг можуть бути розділені на наступні групи:

Дані з світових фондових бірж і ринків, котирування національних валют і процентні ставки. Вони бувають з затримкою в декілька секунд до 15 хвилин.

Результати первинної обробки даних професійних експертів. MarketScope обстеження та аналіз ефективності інвестицій у галузі та окремі компанії Zacks,

довідкову інформацію про компанію з S & P StockGuide, торговельні Vickers звітів і багато іншого.

Створення віртуального портфеля, який включає в себе акції, що цікавить користувача. Операційна портфоліо, можна прискорити і автоматизувати процес отримання інформації. Віртуальний портфель здатний відображати набір дій в якості інвестора в і передбачать, і надалі система буде автоматично відслідковувати зміни, що відбуваються в акції на ринку і повідомляти власника портфеля.

Додаткові послуги включають в себе актуальні новини від провідних інформаційних агентств, таких, як Reuters, BusinessWire, PR Newswire та інші. Ви можете переглянути заголовки останніх повідомлень або запитати всі новини з певної теми або компанії. Дуже зручно об'єднання новин з віртуальним портфелем. У цьому випадку інвестор отримує всі новини по віртуальному портфелі перерахованих акцій.

Прикладами компаній, що надають спеціалізовані фінансові інформаційні послуги InterQuote, QuoteCom, PC пропозицію ітд.

Іноді стандартні засоби Інтернету і, зокрема, WWW не задовольняють систем службової інформації. У цьому випадку розроблені спеціалізовані забезпечення сервера і клієнта, який використовує протокол TCP / IP і стандартних каналів передачі даних, але шляхом надання користувальницького інтерфейсу і набір аналітичних інструментів (Reuters).

Здебільшого, безкоштовна інформація непридатна для комерційного використання, особливо у фінансовому секторі, як це передбачено на тимчасовій основі і без будь-яких гарантій надійності і точності. Найбільш поширений спосіб у світі платного доступу до інформаційних ресурсів, щоб підписатися. Користувачі можуть платити абонентську плату і отримує доступ до певних інформаційних ресурсів на фіксований термін. Іноді вона є більш ефективною фіксації дій користувача з подальшою їх оплати.

Таким чином, сьогодні можна говорити про поступової інтеграції потужних професійних інструментів для фінансового Інтернеті інформаційних технологій. Можна з упевненістю сказати, що потенціал Інтернету як засобу

розподілу фінансових даних досить великий, і з часом ви можете очікувати, що загальне використання мережі в професійної фінансової діяльності зросте.

Що може надати інтернет-банкінг для потенційного клієнта? Проект в області інтернет-банкінгу повинен мати стратегію для розгортання бізнесу, який працюватиме, точне позиціонування продукції в Інтернеті в залежності від фактичної структури попиту і характеристик цільової групи клієнтів. Не поспішайте копіювати західний досвід - потрібно взяти ближчий погляд на те, що клієнт хоче.

Головна перевага інтернет-банкінгу - простість у використанні і економя часу. Таким чином, ми повинні подбати про те, щоб уникнути складної процедури доступу, тривалості і складності операцій. Система повинна бути максимально простою у використанні і працювати швидко. Ті, хто досягає успіху зможуть захопити більшу частину ринку.

Більшість онлайн-банкінг розглядають як додатковий з основним, хоча багато хто не виключає можливість повного переходу, якщо він в змозі запропонувати більш вигідні та привабливі умови служби. А якщо це репутація надійного банку, то таким чином, одним з варіантів позиціонування інтернет-банк - в якості офісу для оплати поточних рахунків. Цей варіант зажадає мінімального по інвестиціях банку, обмеженого порівняно легкими системами безпеки. Наприклад, коли клієнт змушений постійно вести і періодично виконання договору платежі: комунальні, телефон, пейджер, Інтернет і т. д. У цьому випадку майже завжди ми знаємо заздалегідь, і суму платежу і його частоту. Як клієнт банку, який може значно спростити оплату цих послуг заздалегідь "запрограмувавши" платежі принаймні на рік вперед. Привабливість таких послуг є очевидно-виправдана. Тому одне з опитувань, проведеного серед потенційних користувачів "домашнього банку" показало, що багато респондентів коли-небудь платили онлайн і хотіли б зробити комунальні платежі регулярними і дистанційними.

В даний час поняття інтернет-банкінгу охоплює цілий ряд програмних продуктів з певним ступенем умов можна розділити на такі групи:

Системи управління клієнтів ("Інтернет-Клієнт банку" або коротко -

"Інтернет - Клієнт»).

Платіжні і розрахункові системи, у тому числі ті, в яких Інтернет використовується тільки як засіб передачі інформації.

Системи для обробки карт (вони можуть бути частиною системи оплати).

Системи онлайн торгівлі цінними паперами.

Інтерфейсні модулі для взаємодії із зовнішніми системами електронної комерції (наприклад, модулі, що реалізують зв'язку "банк - Магазин" - вони також можуть розглядатися як частина платіжної системи).

Тим часом, на практиці, тим більше, ми знаходимо комплексні рішення, такі, як "платіжна система управління обліковими записами, інтерфейс для інтернет-магазину та обробки" - якому, до речі, широко відома розрахункової системи CyberPlat. А, приміром, програма, яка автоматизує утиліти можуть взаємодіяти як з системою управління обліку та обробки складних пластикових карт.

Тепер коротко позначити конкретні особливості та проблеми кожного класу.

Система управління рахунком. Системи цього типу використовуються більше, ніж інші на ринку. Кількість банків, які мають потребу в них набагато перевищує загальну кількість людей, які потребують інші типи. В іншому випадку, і не доведеться - від "Інтернет - Клієнт" чекає серйозна допомога в тих випадках, коли звичайні «Клієнт - Банк» пропонується тільки проблеми.

Основна проблема "Інтернет - Клієнт", пов'язана з безпекою, у тому числі з юридичної точки зору (втім, це є досить складним завданням для всіх банківських інтернет-продуктів), а також складність реалізації зручним рішенням в сучасних інтернет-технологій програмування.

Реалізація цих програмних продуктів, пов'язаних з необхідністю буквально величезною організаційної роботи. Чи не надзвичайно складна система, що включає розробку безлічі шлюзів і зовнішніх інтерфейсів, однак, у порівняння не йде обсяг роботи, і, звичайно, витрати на створення умов експлуатації. Однак існує універсальних рішень, на основі яких бажаний діапазон може бути відносно швидко - вони починають пропонувати розробників програмного забезпечення.

Системи онлайн торгівлі цінними паперами. В он-лайн торгівлі цінними

паперами, є позиція розробників, що у цьому виду бізнесу беруть участь не всі кредитні установи. Комплекси онлайн-торгівлі цінними паперами від ступеня попиту відповідно до системи "Інтернет - Клієнт" і в будь-якому випадку вони повинні в три рази нижче, ніж необхідно для "клієнта". До речі, загальна оцінка показує відмінний приклад використання інтернет-технологій у практиці.

Модулі взаємодіють із зовнішніми системами електронної комерції. Головною особливістю процесу створення модулів, які взаємодіють із зовнішніми системами, електронної комерції, є обов'язковою роботи з розробниками цих систем. Це також важливо для розвитку тут були дуже залучає експертів з предметних областей (наприклад, в електронній комерції, страхування тощо) ..

Клієнти можуть використовувати для роботи в будь-який з підтримуваних каналів доступу або використовувати різні комбінації каналів, залежно від ситуації. Наприклад, ви можете використовувати комп'ютер на роботі в управлінні рахунками стільникових телефонів роботи - по дорозі додому і звичайних телефонів або інтерактивного телебачення - вдома. Як правило, замовлення формуються і передаються клієнтам, які користуються самообслуговування, але при необхідності, клієнт може здійснювати угоди за допомогою Call-центру банку.

Залежно від типу операції, клієнт дає відповідний наказ, і незалежно від відстані можуть бути оброблені в режимі реального часу (онлайн) або певною частотою (в автономному режимі). Приклади операцій, що проводяться в Інтернеті, є валюті конверсійні операції, в якій валюта продається буде списана з вашого рахунку і зараховуються на Рахунок, придбаних протягом декількох секунд і може бути використаний для виконання цих операцій. Але сплата мит повинна бути виконана в автономному режимі.

2.3 Практичне відображення послуг Інтернет-банкінгу

Українські банки все ширше впроваджують технології інтернет-банкінгу, що забезпечує дистанційне банківське обслуговування через Інтернет. Близько 10 українських банків надають послуги повноцінного інтернет-банкінгу Система грошових переказів по Україні й за кордон "PrivatMoney" - це унікальний програмний комплекс, що завдяки інтернет-технологіям дозволяє практично миттєво здійснювати відправлення й виплату грошей. Перевагою системи "PrivatMoney" є здійснення грошових переказів, яка не вимагає наявності рахунку в банку: для відправлення або одержання грошей достатньо пред'явити паспорт, заповнити бланк із зазначенням прізвища та ім'я відправника, одержувача, суми та країни призначення (при відправленні). Зручність пошуку переказу забезпечується унікальним контрольним номером, що повідомляється одержувачеві та використовується ним при одержанні грошових коштів.

Також платіжною системою "PrivatMoney" можна використовувати у інтернет – банкінгу. Для цього у системі Приват24 перейти на вкладку Перекази PrivatMoney відправити(або отримати, якщо переказ здійснено Вам) та заповнити усі дані. Що досить легко та зручно не гаючи часу у черзі банку.

Наразі послугу грошових переказів "PrivatMoney" надають 3700 пунктів обслуговування на території України, Росії, Латвії, Білорусії, Молдови, Вірменії, Азербайджану, Грузії, Португалії та Кіпру. Мережа учасників і партнерів системи включає банки та системи грошових переказів країн СНД, Балтії та зарубіжжя, серед яких – системи грошових переказів "Анелік," "Алюр" (СТБ-Експрес), "Золота Корона" (СтранаЕкспресс), Пошта Росії, Ощадбанк Росії, "Intesa Sanpaolo" тощо. За допомогою системи грошових переказів "PrivatMoney" Ви маєте можливість відправити або одержати переказ у більш ніж 100 країнах світу!

Характеристика "PrivatMoney"

Висока швидкість переказу – переказ доступний до виплати з моменту надання йому контрольного номера. 10 хвилин – час на повідомлення відправником контрольного номера одержувачу.

Операції з переказами здійснюються в наступних видах валюти: міжнародні перекази: у доларах США та євро;

виплата переказу – БЕЗКОШТОВНО.

Тарифи на здійснення переказів:

Сума переказу	Клієнтська оплата
0,01 - 50,00	2,00 UAH
50,01 - 100,00	4,50%
100,01 - 200,00	4,00%
200,01 - 500,00	3,50%
500,01 - 600,00	3,00%
600,01 - 800,00	2,50%
800,01 - 1000,00	2,00%
1000,01 - 10000,00	1,50%
10000,01 и более	1,00%

Беручи до уваги, що зручність дистанційного обслуговування полягає у відсутності необхідності відвідувати відділення банку, то основний інтерес представляє онлайн-проекція стандартних банківських операцій: погашення кредиту, відкриття депозиту, замовлення нової пластикової карти, блокування скомпрометованої карти. Погасити заборгованість за позикою дозволяють системи всіх банків з десятки лідерів, за винятком Укрсоцбанку. Депозити в режимі онлайн дозволяють відкривати Приват24, MyAlfaBank і ПУМБ. Замовити картку з веб-банкінгу дозволяють тільки ПриватБанк, ПУМБ і Форум. А ось заблокувати свою картку можна ще і в Укрсоцбанку, і в Укрексімбанку.

Для реєстрації потрібно перейти на сайт КБ ПриватБанк, та обрати пункт реєстрація. Заповнюємо усі дані, та успішно реєструємся (Рис 2.3.1).

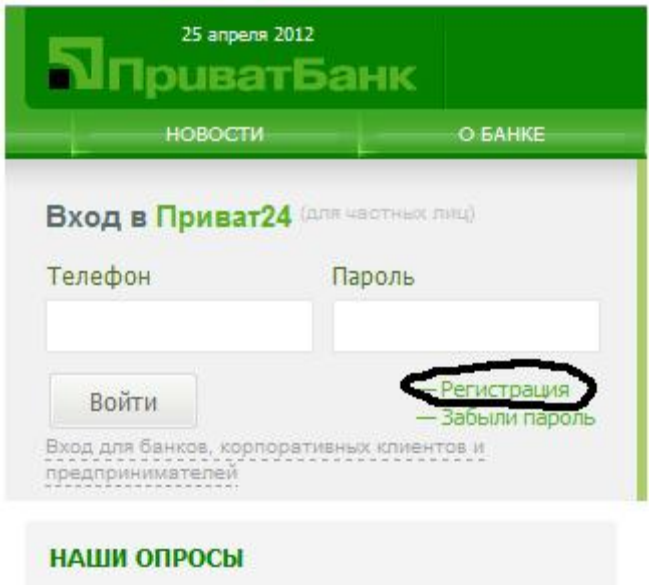

Рис.2.3.1 Реєстрація у системі Приват24

Далі, заходимо в систему інтернет – банкінгу АТ «Приватбанк» - «Приват 24», вводячи логін і пароль. Через деякий час на ваш мобільний телефон приходить смс із підтверджуючим паролем для входу в систему. Вводимо цей пароль у відповідне поле і входимо у свій профіль в системі «Приват 24»(Рис. 2.3.2)

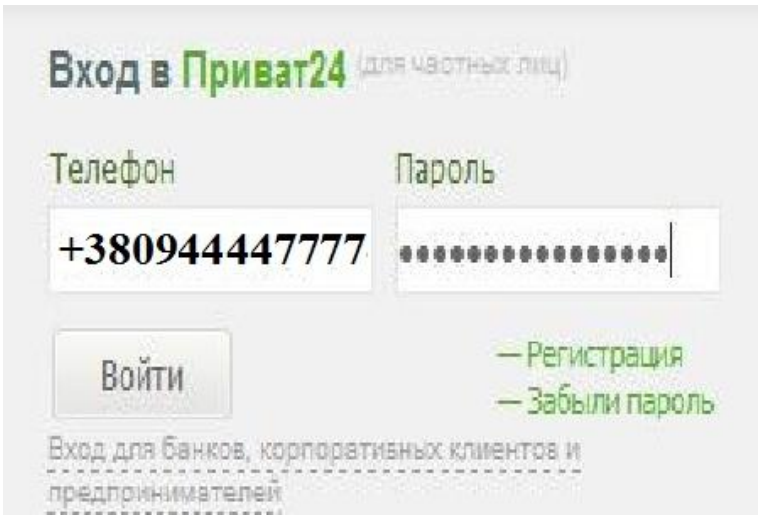

Рис.2 Вхід у систему Приват24

Сторінка користувача виглядає наступним чином: (рис 2.3.3)

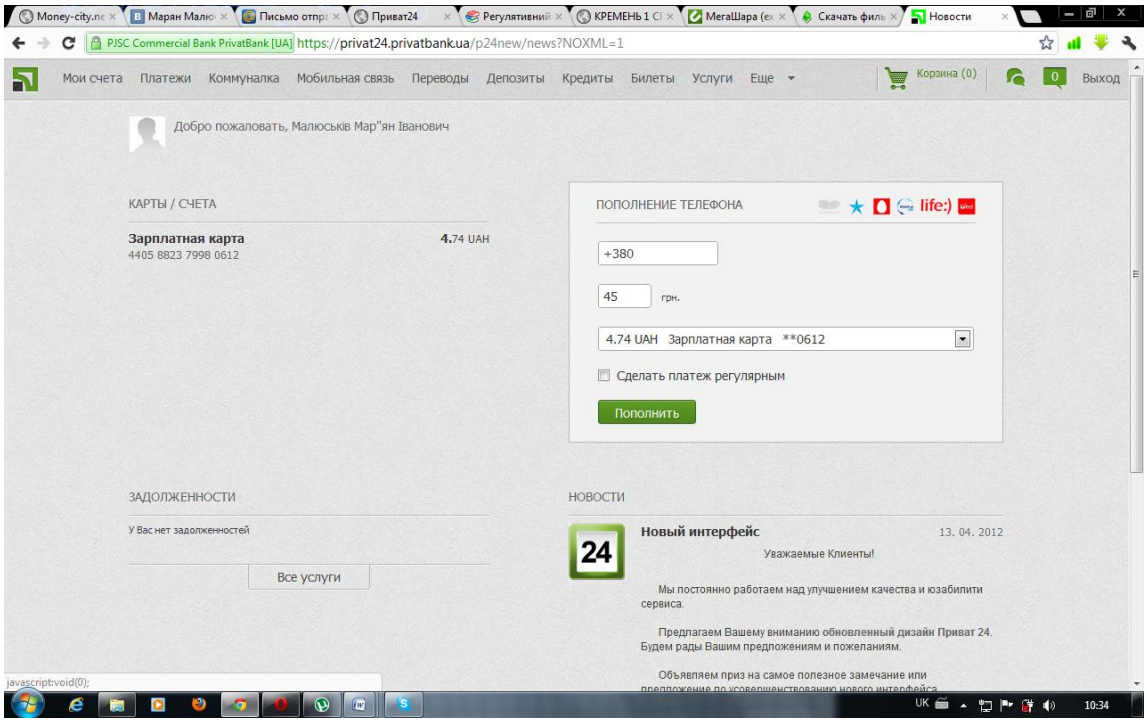

Рис 2.3.3 Сторінка користувача.

У системі Приват24 переходимо на вкладку налаштування ⟶ картки ⟶ додати куртку…Вписуємо номер картки та відсилаємо запит(Рис. 2.3.4).

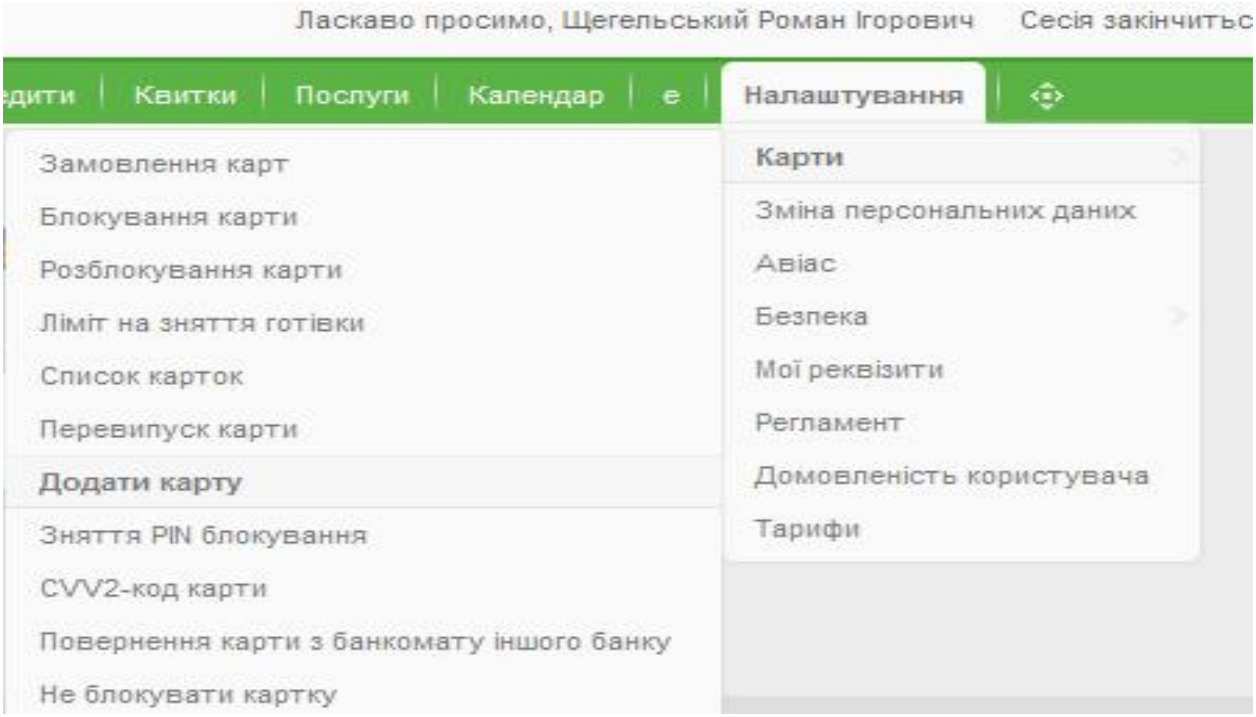

Рис.4 Додавання платіжної картки

Однією із найзручніших та напевно найпопулярнішою із послуг є поповнення мобільного телефону. Для цього обираємо на верхні панелі розділ

«Мобільний зв'язок » і вводимо суму, номер та кредитну картку з якої буде знята сума(Рис. 2.3.5). Підтверджуємо операцію.

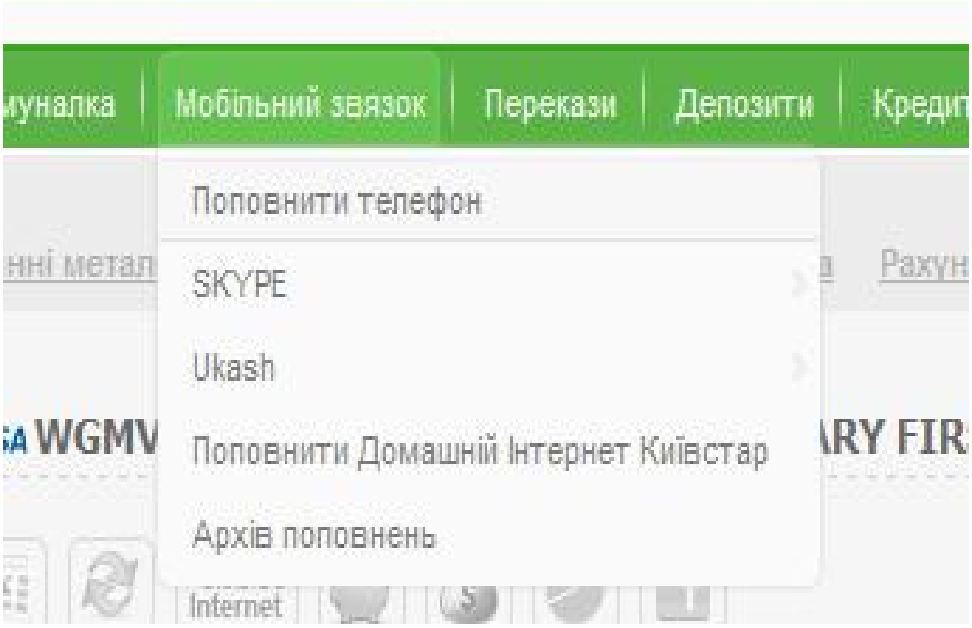

Рис. 2.3.5 Поповнення мобільного зв’язку

Для отримання виписки переходимо на вкладку моЇ рахунки, обираємо картку, встановлюємо дату з якої хочемо отримати виписку та натискаємо “відобразити виписки” (Рис. 2.3.6)

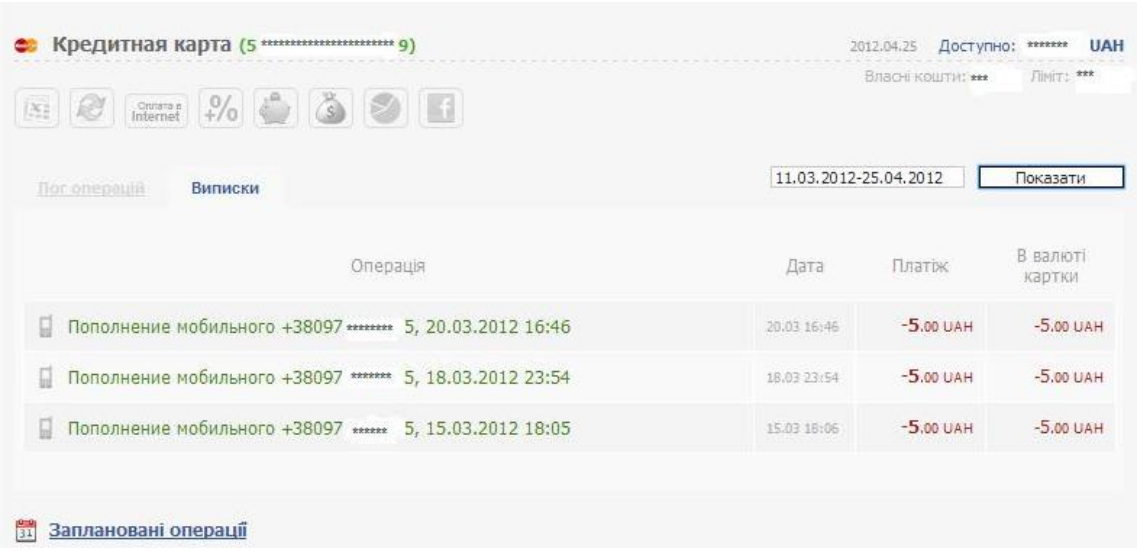

Рис. 2.3.6 Відображення виписки у інтернет-банкінгу Приват24

Експортування виписки у Excel. У вкладці мої рахунки обираємо платіжну картку та використовуємо функцію “експорт в Excel”, і за декілька

секунд у Вас відображатиметься виписка у MS Excel(Рис. 2.3.7)

	A	B	C	D	E
1	Дата транзакции	Номер карты	Операция	Сумма	Сумма в валюте карты
2	20.03.2012 16:46:14	*******9	МОБ СВЯЗЬ П24. 28550120: СПИСАНИЕ ЗА ПОПОЛНЕНИЕ МОБИЛЬНОЙ СВЯЗИ. ТЕЛЕФОН:+38097*********5. ДАТА: 03.20.2012 16:46:11. IDPAY: 31999638(С КАРТЫ 5*** **** **** ***9 НА КАРТУ) СПИСАНИЕ С КАРТОЧНОГО СЧЕТА.	-5.00 UAH	-5.00 UAH
3	18.03.2012 23:54:45	*******9	МОБ СВЯЗЬ П24. 28369052: СПИСАНИЕ ЗА ПОПОЛНЕНИЕ МОБИЛЬНОЙ СВЯЗИ. ТЕЛЕФОН:+38097*********5. ДАТА: 03.18.2012 23:54:42. IDPAY: 31758512(С КАРТЫ 5*** **** **** ***9 НА КАРТУ) СПИСАНИЕ С КАРТОЧНОГО СЧЕТА.	-5.00 UAH	-5.00 UAH
4	15.03.2012 18:06:01	*******9	МОБ СВЯЗЬ П24. 28099436: СПИСАНИЕ ЗА ПОПОЛНЕНИЕ МОБИЛЬНОЙ СВЯЗИ. ТЕЛЕФОН:+38097*********5. ДАТА: 03.15.2012 18:05:56. IDPAY: 31412290(С КАРТЫ 5*** **** **** ***9 НА КАРТУ) СПИСАНИЕ С КАРТОЧНОГО СЧЕТА.	-5.00 UAH	-5.00 UAH

Рис. 2.3.7 Експортування виписки у Excel

Також за допомогою Приват 24 можна здійснювати оплату комунальних послуг. Для цього переходимо на розділ «Комуналка» (рис 2.3.8)

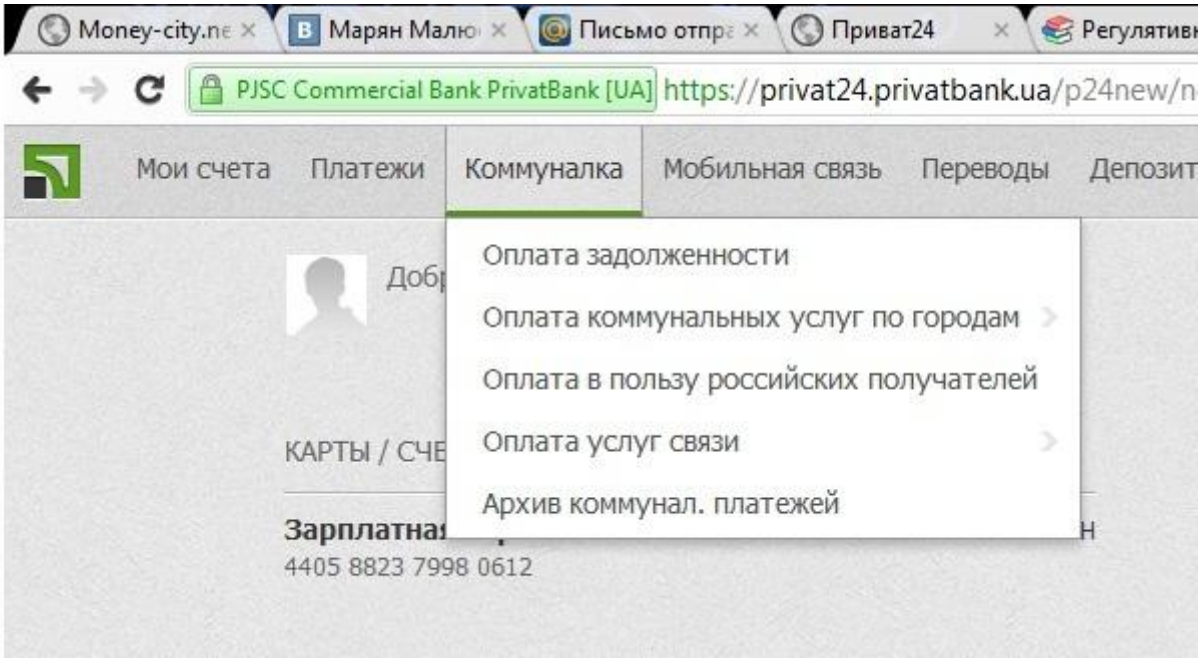

Рис 2.3.8 Список комунальних платежів.

Вибираємо потрібний вид платежу і здійснюємо оплату.

Для онлайн-замовлення особистої картки клієнта заряд, наприклад, має Клюєв Максим Миколайович використовувати будь-який ПК, де є доступ в Інтернет. Використовуючи зручний браузер, наприклад, Internet Explorer, клієнт відвідує веб-сайт www.pib.com.ua (дод.).

Браузер Internet Explorer спростити пошуки нової інформації в Інтернеті і

перегляд ваших улюблених веб-сайтів. Вбудований генератор часу IntelliSense Зберегти, припускаючи, що виконання деяких стандартних операцій, таких як автоматичне заповнення полів для веб-адрес і форми для користувача, і автоматичного визначення стану мережі та з'єднання.

Перед замовленням картки клієнтам слід звернутися до застосовних нормативних актів Банку, які розміщені на веб-сайті банку в електронному вигляді (додаткові B), а саме:

Порядок розрахунків з використанням пластикових карток міжнародних платіжних систем і карткових правил використання (додаткового B);

Договір пластикової карти і виконанню розрахунків за операціями з картами (дод. D);

Тарифи Рахунки і міжнародних платіжних карток для фізичних осіб (додатковий E).

Для замовлення карт Клієнт заповнює дані у вигляді "Інтернет клопотання про звільнення особистих карток" (додаткового K), а саме:

1. Вибір типу карти відповідно з переліком карт, емітованих банком.

2. Вибір валюти карткового рахунку:

Грн;

Долари США;

Євро.

3. Заповнює дані про себе:

прізвище, ім'я, по батькові (українською мовою);

ім'я (по-латині) відповідно з паспортом;

Український паспортні дані: серія номер, коли і ким виданий;

паспортні дані: серія номер, коли і ким виданий;

дата народження та місце народження.

адреса місця проживання: країна, поштовий індекс, місто, вулиця, номер будинку та квартири;

ідентифікаційний номер платника податків;

Ваш номер телефону: Місто (робота, дім) та мобільні;

адресу електронної пошти.

Вказує, дівоче прізвище матері.

Заповнює дані про місце роботи (навчання):

назва організації;

адреса організації;

посада особи клієнта;

номер контактного телефону;

електронної пошти.

Вибір методу отримання виписки по рахунку.

7. Вибір місця, в якому карта буде отримати серед список філій, уповноважених Промінвестбанку по операціях з картами (додатковий L).

У «О-лайн заявка на видачу особистої карти" автоматично заповнюється відповідно до тарифного карт для клієнтів дані "PV", "ГА", "КСВ" і "ППО", що означає, відповідно, розмір початкового внеску, гарантія покриття розміром плати за відкриття рахунку і збори для розрахункових операцій з картами.

При необхідності, клієнт буде додано до "он-лайн заявка на випуск персональних карт" власного транспортного засобу в електронному вигляді.

Закінчено Клієнт "Інтернет клопотання про звільнення особистих карток" послав по електронних каналах зв'язку у відділення банку. Філія комплаенс щоденні перевірки онлайн-додатків. Якщо у вас є додаток на клієнтській співробітник з питань дотримання не пізніше, ніж наступного дня після отримання заяви, пов'язані з клієнтом для уточнення даних і підтвердити заявку.

Філія комплаенс після отримання "Інтернет клопотання про звільнення особистих карток":

- Виводить "онлайн заявка на випуск персональних карт";

- Виконувати відповідно до фінансових обачності моніторингу на його присутність у списку тих, хто підтримує тероризм. У разі клієнта в цьому списку клієнт відмовляється випускати карти та інформує відповідального співробітника фінансового моніторингу;

- Передає "Інтернет клопотання про звільнення особистих карток» у філії безпеки підрозділ для перевірки даних, зазначених Клієнтом.

Після перевірки клієнта до трьох (3) робочих днів, уповноважений отрядник безпеки візує "онлайн заявка на випуск персональних карт» і повернути його у відповідність Партнери офіцера.

У випадку "Інтернет клопотання про звільнення особистих карток" Клієнт отримав невірну інформацію, він не візується роботи підрозділу безпеки Дочірні та залежні суспільства повертається до дотримання. Ця галузь має право відмовити Клієнту отримувати карти, пославши йому повідомлення на електронну адресу, вказану в "Онлайн заявка на випуск персональних карт."

Для випуску особисту гілку карт рішення про видачу картки, бланки та подати до Департаменту електронному вигляді набору файлів виступити із заявою, особистих карток.

Створення і відправка в відділення Промінвестбанку карти платіжною карткою департаменту Промінвестбанку протягом 5 (п'яти) робочих днів після отримання електронного файлу до нього. Після отримання відповідності Партнери офіцера листівку послати клієнтам електронного листа, заявляючи про те, щоб його карти і адресу, за якою він може отримати його.

Якщо клієнт відмовився від карти або протягом місяця після того як він спрямований електронного повідомлення, прийняті суддею не отримали його, карта була знищена і відправлена із застосуванням платіжних карток Промінвестбанку припинення карти.

Комп'ютеризація банків в Україні супроводжується поліпшеною технологією реалізації основних банківських операцій і підвищити загальну керованість банків. Використання сучасних інформаційних технологій може вирішити поточні завдання аналізу банківських операцій і, як наслідок, поліпшення фінансово-кредитних та інвестиційних банків.

Автоматизована банківська система в цілому, являє собою особливу форму організаційного управління сучасним банком засновані на використанні фундаментальних наукових та прикладних положень інформації та кібер-синтезу.

Використання сучасних інформаційних технологій у банку як один з основних інструментів підтримки і розвитку банківського бізнесу на основі

наступних принципів: комплексний підхід до автоматизації широкого спектра банківських функцій і процедур, модульний принцип побудови, відкритості інформаційних технологій , ваги системи, можливість якого був для великого числа користувачів доступ до даних в реальному часі, можливість моделювання банківських функцій і бізнес-процесів, наявність захисту від несанкціонованого доступу ззовні, наявність надійної системи резервного копіювання та архівування.

Експлуатація автоматизації економічних процесів на основі використання сучасних комп'ютерних технологій і повинні відображати системний підхід до автоматизації бізнес-процедур управління на основі цих типів їх експлуатації: технічних, інформаційних, математичних, програмним, лінгвістичним, організаційне, методичне, юридичний супровід.

Кредитів є основною діяльністю банку. Таким чином, поліпшення кредитування банк приділяє значну увагу, представляючи комп'ютерних технологій для автоматизації функцій управління кредитами.

Окремих конкретних питань, пов'язаних з виконанням завдань банківському кредитуванню фізичної особи. Кредитування було і залишається провідним прибутковим банком пункту. Кредитування автоматизації процесів найбільш трудомістких і тривалих через необхідність брати до уваги велику кількість кредитних вимог. Цей процес повинен спочатку розглянути наступні вимоги:

обслуговування та оновлення бази даних по виданих кредитах;

підтримуються різні типи гривні і кредитів в іноземній валюті;

гарантувати, що всі операції з кредитами;

набір конфігурації діяльність кредитних;

настройка параметрів, що визначають технологічне порядок операцій з кредитами різних видів;

Наявність гнучких механізмів відсотків по кредитах;

здійснення гнучкої настройки для різних методів фінансування;

Використання пластикових карт для отримання кредиту;

забезпечити оперативне отримання звітної інформації про існуючі та закриті кредити;

можливість розрахунку кредитними якого попереднього і подальшого періоду.

Набір функцій управління кредити об'єднати свої системи автоматизації: прогнозування і планування, облік і контроль, аналіз і регулювання. Кожен з цих комплексів здійснюється на відповідній стадії інформаційної технології обробки з використанням фіксованих апаратних засобів і програмного забезпечення, на виділених робочих станцій (НД).

У Промінвестбанку автоматизований засіб, підсистема управління кредитів у стадії технології мають наступні характеристики.

Прогнозування та планування: визначення стратегії кредитування, портфель заявок на кредити, розрахунок кредитоспроможності клієнта, оцінка ризиків під час кредитної; прибутковість операцій планування, складання кредитних договорів, складання графіка кредитів, складання графіка виплати відсотків за кредитами, План-погашення, розрахунок резервів за кредитами.

Облік і контроль: відкриття рахунків, облік операцій за кредитними рахунками, нарахування відсотків, контроль за здійсненням угоди.

Аналіз і правил: звітність, аналіз, технічне обслуговування рішень.

Ці особливості, а також пакет додатків, що належать до класу задач стратегічного маркетингу. Кожна задача не буде вирішена по кожному кредиту окремо, і в цілому для процесу кредит на певний період. Для автоматизації цієї функції, Банк використовував стандартні статистичні пакети програмного забезпечення для обробки даних (статистичні Exsel функцій).

Інші етапи обробки інформації технології автоматизованої функції, які пов'язані з конкретними кредитів.

Системи автоматизованого розрахунку кредитоспроможності позичальника полягає у визначенні показників точності на останньому врегулювання до кредитів отримала свою нинішню фінансовий стан і перспективи змін і здатністю при необхідності мобілізувати грошові кошти з різних джерел і забезпечити швидку конверсію активів у ліквідні активи .

Метод визначення кредитного рейтингу полягає в наступному. Відповідно до бухгалтерської та статистичної звітності клієнта розрахункові значення

відповідних коефіцієнтів і порівнюючи їх з нормативними. На основі цього порівняння дано рекомендації про можливість кредиту. Якщо ви хочете більш глибокого аналізу аналізує нинішнє промислової активності клієнтів, беручи до уваги представлені дані більше часу і додаткові показники розраховуються.

Вихідні дані для розрахунку вибраних документів, отриманих від клієнта бази даних і поточної інформації, що міститься у відділі кредиту ARM. З клієнт отримує наступні документи: заявку на кредит, включення чартерної компанії, свідоцтво про реєстрацію, бухгалтерський баланс, звіт про доходи. На підставі цих документів створюються масиви "Вхід", "баланс", "фінансові результати", "Кредит-Рейтинг", "кредитна історія позичальника», «Документація», «Висновок», яка записує всі необхідні параметри для розрахунку. Довідкової інформації встановити кредит узятий з клієнтів каталогу каталог балансу, фінансової звітності перелік одиниць обладнання, еталон показників і керівних принципів для визначення кредитоспроможності банку, а також архівні файли, які містять інформацію про всіх кредитів, наданих банком.

Використовуючи інформацію, отриману недавно баз даних на АРМ кредитного відділу за допомогою спеціального програмного пакету розрахункових значень кредитоспроможності позичальника.

Автоматизація в кредитних договорів є виконання наступних процесів: створення нових угодах, переглянути список операцій, редагувати окремі записи, видалення окремих угод.

Введення нової угоди є заповнити наступні поля послідовних операцій файлу: номер операції, код валюти, реєстраційний номер та ім'я клієнта банку, вид кредиту, дати початку і закінчення угоди, сума угоди, відсотки швидкість, тип особового рахунку, номер особового рахунку для угоди і стан транзакції. Список договорів розглянуті через екранну форму документа, в результаті чого запис з файлу має справу з користувацьких атрибутів (кількість угод, реєстраційний номер та ім'я клієнта, і т.д..). У період проведення експертизи не може вносити зміни в поля. Він використовує спеціальну процедуру "Edit".

Автоматизація операцій з кредитними рахунками здійснюється типова картина вхідних документів. Вхідного документа перед виведенням на рахунки

кредитних операцій служать командами або меморіальних ордерів кредитування рахунку і доходи і витрати документів.

Перша операція в технології вхідних повідомлень є операторів ручного введення документів через екран шаблонів. При цьому здійснюється програмним управлінням інформацією, записаною в полі введення файлу. У робочих банківських днів (ОДБ), за умови повторного введення документів, вже іншими художниками в "Kontrolniy Ok". Коли ви бачите повідомлення "Документ ввічливості», інформація передається на наступну операцію - платіжний документ, що записи зберігаються у файлі дати платіжних документів - бізнес-операції відображається у бухгалтерському обліку. Основна база даних організована таким чином, що можна встановити дату для визначення грошових потоків і використовувати ці значення для розрахунку відсотків по кредитах.

Відсотки за кредитами, це спеціальний програмний модуль для всіх клієнтів або для певних облікових записів. Програма дозволяє розрахувати зміну на початку, тому що швидкість заставки інтерес. Результати розрахунку записуються в спеціальний файл, з якого інформація надається після екрану записуються в первинній базі даних.

Контроль за виконанням угод на кредити нести спеціальне програмне забезпечення та почати через ЕМ, які вказують на функції особистого і групового угоди про контроль.

Особисті засоби управління на екрані після конкретного типу та низку угод з урахуванням змісту угоди і дані з кредитних рахунків: залишки та рух грошових коштів дані щодо обчислення та сплати сум за інтерес.

Група контролю кредиту на основі фактичних даних, отриманих на екрані, а при необхідності - на основі таблиці, опубліковані в пресі.

Список таблиць задається в меню, і користувач визначає, які таблиці повинні бути підготовлені. Вони суми і процентні ставки за кредитами протягом дня, включає індивідуальний рахунок кредиту протягом зазначеного періоду, кількість угод, суми і процентні ставки за кредитами. Протягом останніх трьох документів певний період або дату, на яку документ.

Звіти по кредитах проводиться автоматично на основі бази даних, розвідки ОДБ формується пакет програмного забезпечення.

Для цього пакету програмного забезпечення з ARM статистичної звітності. Екранне меню пакета дається для звітів, які повинні бути представлені в той же день. Таким чином, без адекватного розвитку інформаційних систем і технологій автоматизації банку на кредитування не можливо своєчасного та ефективного процесу обслуговування клієнтів. Тому програми, які приходять з роботи відділу кредитних працівників дозволить своєчасно і належним чином виконувати свої обов'язки. Використання автоматизованої банківської системи дозволяє банкам скоротити витрати і час на обслуговування клієнтів, контроль за виконанням банківських операцій у режимі реального часу, для прийняття обгрунтованих рішень якомога швидше, що впливає на якість і конкурентоспроможність банківських установ.

Висновки до розділу 2

Таким чином, сьогодні можна говорити про поступової інтеграції потужних професійних інструментів для фінансового Інтернеті інформаційних технологій. Можна з упевненістю сказати, що потенціал Інтернету як засобу розподілу фінансових даних досить великий, і з часом ви можете очікувати, що загальне використання мережі в професійної фінансової діяльності зросте.

Що може надати інтернет-банкінг для потенційного клієнта? Проект в області інтернет-банкінгу повинен мати стратегію для розгортання бізнесу, який працюватиме, точне позиціонування продукції в Інтернеті в залежності від фактичної структури попиту і характеристик цільової групи клієнтів. Не поспішайте копіювати західний досвід - потрібно взяти ближчий погляд на те, що клієнт хоче.

Головна перевага інтернет-банкінгу - простість у використанні і економя часу. Таким чином, ми повинні подбати про те, щоб уникнути складної процедури доступу, тривалості і складності операцій. Система повинна бути максимально простою у використанні і працювати швидко. Ті, хто досягає успіху зможуть захопити більшу частину ринку.

Більшість онлайн-банкінг розглядають як додатковий з основним, хоча багато хто не виключає можливість повного переходу, якщо він в змозі запропонувати більш вигідні та привабливі умови служби. А якщо це репутація надійного банку, то таким чином, одним з варіантів позиціонування інтернет-банк - в якості офісу для оплати поточних рахунків.

РОЗДІЛ 3. ПЕРСПЕКТИВИ РОЗВИТКУ ІНТЕРНЕТ-БАНКІНГУ НА СУЧАСНОМУ ЕТАПІ ДІЯЛЬНОСТІ БАНКІВСЬКОЇ СИСТЕМИ.

3.1 Економічна вигода та ефективність використання вже існуючої в банку технічної бази

Інтернет та банківські послуги в цілому зробили свій вплив на відділення банків, банкомати та банківські центри обігу. Одначе, на сьогодні системи за таким типом не дуже поширені. Розвиток таких систем занадто сильно стримується відсутністю чіткої правової основи для комерційних розрахунків в інтернет просторі. Крім того, проблеми безпеки залишаються в силі для цих розрахунків.

Слід зазначити, що якість ліній в Україні, обмежуючи при цьому надійність використанням он-лайн. Швидкість передачі даних обмежена, що призводить до значного збільшення часу при роботі з великими обсягами даних, особливо через міжнародні шлюзи.

Всі ці проблеми дуже накладаються на повільну прогресію технологій, заснованих на інтернет в українських банках. Клієнти, як правило, не мають доступу до філій банку через електронну пошту або веб-хостингу. Найбільш поширене використання Інтернету українських банків розповсюдження рекламної інформації в WWW.

Але ми не повинні забувати, що мережа Інтернет є єдиною в світі системою, яка об'єднує всі існуючі мережі комп'ютера в світі - від національного до приватної. Все це пов'язує, за останніми оцінками, близько 50 мільйонів комп'ютерів. Ця всесвітня "мережа мереж" є структурою комп'ютерів, швидко зростаючих у світі, а загальна кількість користувачів збільшується щомісяця на 12%. Відносна простота використання вартості і низької сприяли швидкому зростанню числа користувачів послуг Інтернету. Це значно розширює аудиторію для комерційних компаній.

Прогрес у використанні інтернет-банку (у тому числі український) неминучий, і уже неможливо уявити собі банк без Інтернету.

З введенням нових послуг, які ви використовуєте програмне забезпечення вже є в банку. Цей спосіб полягає в установці системи, призначеної для обробки транзакцій "он-лайн", що в елементах інтернет-банкінгу. Будуть доступні 24 години на добу, система бере на себе операції клієнтів у реальному часі, і обмін bek-файлів Office банк знаходиться в автономному режимі. Іншими словами, банк будує міцний міст між їх віртуальним офісом в Інтернеті і bek-офісу, що дозволяє основні банківські операції, в тому числі отримання заяви, переводити кошти між рахунками, робити гроші на депозитах і т.д. Таким чином, клієнт може працювати з своїми рахунками в будь-якому випадку - з банком за рахунок грошових коштів через банкомати, робити покупки і мати доступ до операцій по рахунках зі свого домашнього комп'ютера, а банк йде на новий рівень банківських послуг.

Але технічними труднощами навіть у цьому рішенні, це перша реалізація. На додаток до звичайних тут додаються труднощі, пов'язані з вибором технології інструменту і програмного забезпечення. Чи не напружуються суперечка про те, чому віддаєте перевагу: Java або ActiveH, HTML або щось ще?

Слід зазначити, що більшість підходів ще не врегульовано, тому для реалізації рішення, яке завжди буде свідомим, робота з усіма версіями браузерів не вдасться. Проте головний кут повинен бути установлений не «просувати» продукт а зручність клієнта. Стара перевірена технологія більше не зустрітися сьогодні (HTML - найяскравіший приклад), змушує виробників шукати і пробувати нові інструменти.

По-друге, створити бажану конфігурацію. Складність полягає у величезній різноманітності системного програмного забезпечення для Інтернет-систем. Це також проблема вибору веб-сервер, проксі-сервер, міжмережевий екран, поштовий сервер, FTP-сервера, і т.д. Додайте до цього кількість компаній, які виробляють аналогічну продукцію, і ви розумієте, що завдання встановлення і налаштування, необхідні для експлуатації обладнання та програмного забезпечення не є тривіальною. Отже, там, як правило, починають переважати людські та фінансові підходи - привілейованих систем, які є знайомими або співробітниками автоматизації, або легше вчитися, або фахівців, які будуть

коштувати банку менше. До речі, саме тому хороші шанси програмного забезпечення компанії Microsoft, як відомо, що експерти в області Unix зустрічаються рідше, і на ринку праці більше.

Українські банки все частіше застосовують технології інтернет-банкінгу, що дає розвиток банківських послуг через Інтернет.

Близько 10 українських банків надають повний банківських інтернет-пакет [1 www.aub.org.ua]. Критерій корисності це можливість для клієнта банку, який має доступ до мережі Інтернет, переводити кошти на будь-який банківський рахунок у будь-який вітчизняний банк. Більшість банків може тільки здійснювати перекази всередині банку і на рахунки в інших банках (комунальні послуги, електрику, телефон і т.д.). Поширенням інтернет-банкінгу представлені переваги, які вона надає для клієнтів і банку. Сучасні інтернет-технології дозволяють банкам істотно прискорити і спростити робочий процес, зменшуючи кількість паперової роботи. Управління аккаунтом Інтернет дозволяє не тільки заощадити час, але й дає суттєві переваги. Так, деякі банки знижують ставки по операціях через Інтернет, в той час як інші нав'язати фіксовану ставку за операцію, а інші - єдиного внеску на будь-яку кількість замовлень, що особливо вигідно для корпоративних клієнтів.

Інтернет-банкінг значно знижує вартість банківських операцій, що дозволяє банкам надавати клієнтам віддалену допомогу. Потреба клієнта тільки доступ в Інтернет і захист ключа цифрового підпису.

За даними Internet World Stats, в Україні в даний час 15,3 млн. користувачів інтернету. До 2012 року вони складуть близько 31,4 млн. з них 15,3 млн. чоловіки тільки 5,2% користувалися інтернет-банком. В абсолютному вираженні - це 800 000 осіб. Лідери ринку на початку грудня 2010 року Приватбанк своїм Інтернет-банкінгом 540 000 клієнтів. На другому місці Перший український міжнародний банк - 91 000 користувачів, а потім Укрексімбанк – 81 000, Universal Bank – 50 800 і п'ятий OTP Bank – 43 000 клієнтів. Активно працюють у цьому напрямку, як Альфа-Банк, Укрсоцбанк, VAB Банк, СЕБ Банк і банк Фінанси та Кредит. Щомісячний приріст користувачів інтернет-банкінгу становить 3 тис. осіб. Але банкіри кажуть, що

це дуже мало. За даними компанії GFK Україна, тільки 2% клієнтів банків перевірили в Інтернеті залишок за непогашеними кредитами, або перевірка балансу по рахунку поточних операцій. Залишок коштів на депозитні рахунки і пластикові карти ще менше - 1%. Це незначне використання онлайн-банкінгу надихають банки для запуску служб. Запуск безкоштовний Інтернет-банкінг, форум оголосив, що робить його відмінним вибором. З 2012 року службу інтернет-банкінгу також планує ввести Platinum Bank [2 www.delo.ua].

При обслуговуванні клієнтів через інтернет-банк, послугу повинні відповідати таким основним принципам банківської діяльності:

• наявність. Як і будь-які інші банківські продукти послуги що здійснюється через Інтернет повинні бути доступні для всіх. Це означає, що не повинно бути обмеження клієнтів, за видами економічної діяльності та багато іншого.

• простота у використанні. Кожен з пропонованих банку продуктів повинні бути максимально легкими. Робота з ними не повинно займати багато часу у клієнта, процес розвитку повинен бути швидкими і доступними.

• конфіденційність. Банк повинен забезпечити клієнту захищену інформацію, яка відноситься безпосередньо до клієнта і його підрядних робіт від несанкціонованого доступу. Цей принцип особливо актуальний для обслуговування клієнтів через Інтернет.

• ефективність. Всі операції, здійснювані клієнтом повинні бути у банку «в реальному часі». В іншому випадку послуги через Інтернет безглузді.

• складності. Сьогодні практичне дотримання цього принципу є справою майбутнього через недосконаліть національного законодавства не дозволяє ідентифікувати особу, не відвідуючи банк.

• збереження цілісності інформації. Інформація про роботу з будь-якого не може бути змінена, змінена або доповнена.

• аутентифікація. Покупці і продавці повинні бути впевнені, що всі сторони, що беруть участь в угоді, є тими, хто за кого себе видають.

• гарантії ризиків продавця. Через онлайн-торгівлі, продавець піддається впливу багатьох ризиків, пов'язаних з відмовами продуктами недобросовісності

покупця. Величина ризику повинна бути узгоджена з постачальником платіжної системи та інших організацій, що входять в ланцюжку продажів за допомогою спеціальних угод.

• Зведення до мінімуму операційні витрати. Плата за обробку операцій, замовлення та оплата, звичайно, включені в їх вартість, тому зниження ціни угод збільшилася конкурентоспроможність.

Зверніть увагу, що угода повинна бути оплачена в будь-якому випадку, навіть якщо покупець відмовляється від товарів [3, с.59 Микола Деменков. Інтернет-технології в обслуговуванні клієнтів банку [Текст] // Банківська справа. – 2009. - №1. – с. 58-64].

Простота у використанні Інтернету для клієнтів за наступними пунктами:

1. Використовуючи Інтернет, клієнт має можливість у реальному часі відслідковувати коштів на його рахунок і своєчасно вносити всі необхідні платежі. Це дає йому можливість ефективно використовувати фінансові ресурси що дає переваги його бізнесу, і в результаті - забезпечує додаткові банківські ресурси.

2. За допомогою інтернет-системи обслуговування, що мають віддалений доступ до рахунку, банк клієнту дозволяє уникнути необхідності відвідувати кожен офіс банку, що є необхідною умовою для економії вашого часу.

3. Нові системи через доступний і зручний інтерфейс дозволяють з мінімальними зусиллями підготувати ваучери для банку, щоб уникнути можливих помилок .

4. Нові системи забезпечують раніше недосяжні можливості мобільності і масштабованість, за допомогою якого користувач може вибрати найбільш зручні та ефективні процедури для управління особистими фінансами. Система дозволяє організувати одночасну роботу з необмеженим числом робочих місць в офісі, щоб розподілити силу співробітництва і т.д. [3, с. 59-60 Микола Деменков. Інтернет-технології в обслуговуванні клієнтів банку [Текст] // Банківська справа. – 2009. - №1. – с. 58-64].

5. Відносні розміри накладів: вони 2 - 3 рази нижче, ніж у звичайних банків і веб-транзакцій витрати 5 - 10 разів менше, ніж при використанні

традиційних каналів. Таким чином, витрати на фінансові операції в офісі 1,07 USD. Пошти США - 0,73, по телефону - 0,35, в банкоматах - 0,27, через глобальну мережу - 0,10 доларів. США [4 Михайлюк Г.О. Розвиток Інтернет-банкінгу як нетрадиційної банківської операції - www.rusnauka.com /1_KAND_2010/Pravo/9_57264. doc.htm].

Основні активні операції, які здійснюються через Інтернет є кредитування фізичних осіб. Існує така схема кредитування через Інтернет: рішення, прийняте банком протягом 10-15 хвилин після оформлення клієнтів онлайн заявки на кредит і вивчити його доцільність. Онлайн-заявку можна знайти на сайті інтернет-магазину. Через 10-15 хвилин після натискання покупця кнопку "Відправити", працівник банку, пов'язаний з клієнтом за вказаними контактними даними профілів і повідомити рішення банку про надання йому кредиту. Програма кредитування онлайн сума кредиту для кожного клієнта розраховується автоматично і індивідуально. Початковий внесок становить 0%. Сума кредиту видається покупцю коштів і зараховується на рахунок інтернет-магазину. Це дуже привабливо для більшості інтернет-магазинів, тому що, звичайно, вони впевнені в повній оплати товару та, що кредит буде використовуватися для покупки у нього. Програма кредитування Інтернет може бути запущена практично відразу: інтернет-магазин не потребує технічного програмного забезпечення, придбання обладнання, набір додаткового персоналу. Простий механізм для отримання кредиту покупцеві. Він побудований таким чином, щоб після рішення банку за кредитом до покупця як тільки достатньо, щоб отримати в банк з документами підписати кредитний договір, то банк буде автоматично повідомляти інтернет-магазин про те, що покупець має позику та можливість поставки йому товару.

Сьогодні жоден з національних банків не може надавати кредити через Інтернет повноцінно. Тобто, при оформленні кредиту клієнту через Інтернет ще потрібно йти в банк, для ідентифікації. Але в цьому випадку, он-лайн кредитування взагалі втрачає сенс. Це пов'язано з недосконалістю законодавства та відсутністю технології цифрового підпису, яка дозволила б ідентифікації людини, який потрапив на сайт з великої відстані.

Отже, банківська система України все ще далека від європейських стандартів Інтернет, причина цього полягає в необхідності відвідати хоча б один раз клієнтом банку, що знижує майже до нуля сутність дистанційного обслуговування.

Для нормального та належного функціонування онлайн-платежів в Україні потрібно ввести систему цифрових підписів, що дозволить ідентифікувати людину на відстані. Слід зазначити, що цифровий підпис видається одночасно з паспортом та ідентифікаційним кодом і процес має бути обов'язковим. Незважаючи на введення технологій у банківському секторі, кожен день бажаючих взяти сегмент банківських технологій збільшується. Можна зробити висновок, що послуги, що надаються банками через Інтернет, щодня все більше і більше зацікавлюють клієнтів, тому банки, які показуватися в першу чергу досягти своєї діяльності в Інтернеті займають лідируючі позиції на ринку банківських послуг України.

3.2 Самообслуговування як розширення клієнтських можливостей

Концепція самостійності часто викликає підозру або не бачення в якості крайнього засобу, коли ніякої іншої можливості обслуговування клієнтів немає. Але в останні роки, в основному у зв'язку з розвитком інформаційних технологій, веб-сервіси та нові телефонні функції, нарешті оцінені як ефективний спосіб розширити канали комунікації з клієнтами, надаючи їм можливість взаємодіяти з компаніями, в будь-який час і в в будь-якому місці.

Поняття самостійності часто пов'язують з індустрією швидкого харчування, а й в інших областях ці технології були в експлуатації протягом десятиліть. Так, всі магазини повністю заснований на самостійний вибір себе при купівлі продуктів. Без саме було б неможливо забезпечити такий широкий спектр продуктів. Цікавим фактом є те, що супермаркети в даний час також розширити самообслуговування, наприклад, за рахунок використання веб-технологій клієнт вибирає потрібні товари і формує свої вимоги, і забезпечує доставку супермаркету.

Самостійне онлайн самообслуговування зробило справжню революцію, особливо в банківській сфері. Воно стало вельми зручним для пошуку і вибору відповідної системи обслуговування клієнтів на банківських сайтах. Оплати (або інший переказ) також можна виконувати по мережі. Крім того, багато банків тепер мають можливість надавати своїм клієнтам можливість самоперевірки. Це велика перевага для клієнта, тому що він прискорює обслуговування і розширення спектру послуг

Дослідження показало, що близько 35% людей використовують Інтернет, щоб зберегти свій час, використовуючи веб-сайтах банків для розрахунку різних видів операцій при використанні цього телефону тільки для 20% респондентів. У той час як прямий контакт як і раніше дуже важливий канал комунікації в банківській справі, у здійсненні звичайної діяльності клієнта насправді не потребують спілкування з представниками для оплати будь-яких

послуг.

Об'єднання каналів зв'язку дозволяє компанії (банку) завжди буде "обличчям для клієнта", і таким чином вносити, шляхом самостійного нові канали комунікації, які забезпечують швидкість і гнучкість обслуговування. Революція в самообслуговування, в основному, і був причиною таких пропозицій на березі, де весь робочий процес заснований на самообслуговуванні.

Частка використання автоматизованих пристроїв для роботи з споживачами зростає, підвищуються і вимоги банків до спектру наданих ними послуг. На щорічному міжнародному форумі Wincor World в Падерборне один зі світових вендорів, що розробляють пристрої самообслуговування, представив лінійку нових рішень

Питання захисту від шахрайства завжди актуальний для банків. Крім фінансових втрат від подібного роду атак, банки повинні ще протистояти їх наслідків з точки зору загрози для свого іміджу і довіри клієнтів. Щорічний приріст числа випадків шахрайства з банкоматами перевищує 7%, при цьому вони стають все більш витонченими. Досвід показує, що найбільш ефективний метод боротьби - запобігання атак, а не боротьба з їх наслідками. Одним з таких рішень став Dynamic Fraud Management, представлений компанією Wincor Nixdorf. На виставці Wincor World компанія продемонструвала, як можна пов'язати між собою різні системи і генеруються ними дані, події і сигнали. Робота модуля Anti-Skimming II, біометричних рішень, системи аналізу зображень та рішення для фарбування банкнот була показана на реальних прикладах з життя.

Поряд з рішеннями для динамічного запобігання шахрайства були показані можливості інтелектуальної передачі інформації. Особливу увагу компанія Wincor Nixdorf приділила системі розпізнавання ознак атаки, в основі якої лежать поведінкові моделі, і можливостям успішного запобігання атак.

Рішення Cash Cycle Management Solution Base оптимізує процеси управління готівкою у відділеннях банків

Був продемонстрований портфель рішень ProTect, що включає в себе

консалтинг, обладнання, програмне забезпечення та сервіси. Нещодавно він розширився за рахунок рішень для динамічного запобігання шахрайства, при цьому був збережений трирівневий підхід до забезпечення захисту банків. На першому етапі проводиться експертний аналіз ймовірних загроз для банку з докладним дослідженням бізнес-процесів конкретної організації, структури інформації та комунікацій, а також робочого середовища. На основі отриманих даних індивідуально визначається необхідний для банку рівень захисту і формулюються основні вимоги до захисних заходів. Другий етап включає в себе впровадження спеціально налаштованих під потреби банку рішень щодо забезпечення безпеки. І, нарешті, на третьому етапі кредитна організація може передати Wincor Nixdorf управління інфраструктурою забезпечення безпеки.

Рішення Cash Cycle Management Solution Base (CCMS Base) допомагає контролювати і оптимізувати процеси управління готівкою у відділеннях банків. CCMS Base консолідує інформацію, отриману від різних систем (банкоматів, систем замкнутого циклу обороту готівки в банках, POS-терміналів у магазинах роздрібної торгівлі, логістичних та розрахунково-касових центрів) і обробляє отримані дані, забезпечуючи контроль процесу управління готівкою. Програмне забезпечення створено на основі сучасної архітектури і має модульну структуру. Основні компоненти системи - рішення, призначені для відстеження касет для зберігання готівки, моніторингу замовлень, розподілу готівкових та контролю над запасом готівки.

Модуль відстеження касет з готівкою надає інформацію, що надходить від окремих систем, а також докладні дані про кількість касет з готівкою у дорозі, кількості банкнот в кожній з них і обсязі готівки в розрахунково-касовому центрі в конкретний момент.

За запасами грошей стежить модуль моніторингу рівня готівки, який також виробляє деталізацію щодо окремих систем і містить дані про готівки на всьому шляху їх переміщення. Модуль моніторингу замовлень відстежує логістичний ланцюжок і забезпечує безперервне документування всіх переміщень готівки.

Комунікаційний центр, який об'єднує відділення банку, формує модуль розподілу готівки. Паралельно він здійснює моніторинг запасів готівки у

відділеннях роздрібної торгівлі.

Основні вимоги, пропоновані банками до зовнішніх постачальникам послуг, полягають у зниженні витрат і підвищенні якості готовності систем. Як постачальник комплексних рішень, Wincor Nixdorf крім обладнання та програмного забезпечення, зарекомендував себе у всьому світі, пропонує своїм клієнтам повний спектр послуг - від класичної технічної підтримки та ремонту до управління системами самообслуговування, IT-інфраструктурою та додатками до повного контролю процесів обробки готівки і платежів . Крім цього, компанія може взяти на себе всі обов'язки з ведення контрактів, надання конкретних послуг і підтримки рівня обслуговування. Дані послуги Wincor Nixdorf може надавати також клієнтам, які користуються пристрої інших постачальників.

Один з головних елементів портфеля аутсорсингових послуг Wincor Nixdorf - постійний дистанційний моніторинг всіх банківських систем самообслуговування, що звільняє банки від тягаря управління власними пристроями, що в підсумку призводить до оптимізації бізнес-процесів і істотного зниження витрат.

Клієнти спілкуються зі своїм банком, використовуючи різні канали комунікацій. Незалежно від обраного каналу важливий єдиний інтерфейс і високу якість обслуговування. Пропоноване Wincor Nixdorf рішення PC / E Suite допомагає банкам вибудовувати стратегію продажів, що дозволяє проводити маркетингові кампанії, використовуючи всі канали комунікацій.

Продукт PC / E Suite допомагає банкам вибудовувати стратегію продажів, що дозволяє проводити маркетингові кампанії, використовуючи всі канали комунікацій

Відвідувачі виставки Wincor World побачили приклад багатоканального маркетингу. Спочатку у віртуальному банківському вікні з'являється рекламне повідомлення, що викликає інтерес клієнта. Користувачі смартфонів отримують додаткову інформацію про пропоновані продукти за допомогою інтегрованого QR-коду (двомірного штрих-коду, що містить закодований URL). Коли зацікавлений клієнт заходить під своїм логіном у термінал самообслуговування,

на екрані відображається пропозиція. Використовуючи функцію відповіді, клієнти можуть домовитися про особисту зустріч з фахівцями відділення банку. Консультант у відділенні вже знає про майбутній відвідуванні клієнта і може заздалегідь ознайомитися з інформацією про нього.

Таким чином, інструмент прямого маркетингу PC / E Direct Marketing дозволяє вибудувати цілісний процес комунікації від першого звернення до клієнта до укладення договору. PC / E Direct Marketing контролює систему управління всією маркетинговою кампанією банку по всіх каналах комунікацій. У підсумку разом з використанням CRM-систем банку це призводить до того, що клієнт отримує найбільш відповідні для нього рекомендації по продукту.

Програмне забезпечення, пропоноване Wincor Nixdorf в рамках пакету Enterprise Management Solutions, полегшує централізоване управління каналами і адміністрування цієї роботи в роздрібних банках. Кредитна організація може запровадити у себе дані рішення і експлуатувати їх самостійно або віддати всю роботу, пов'язану з інфраструктурою самообслуговування, на аутсорсинг.

3.3 Підвищення надійності Інтернет-систем та забезпечення безпеки надання фінансових послуг завдяки прогресу в сфері IP-технологій

Використання системи «Інтернет-банкінг» стає більш безпечним. Інформаційна безпека удосконалюється з урахуванням постійно змінюється інфраструктури, а також у зв'язку з постійним розвитком інформаційних технологій. Безпечне використання «Інтернет-банкінгу» забезпечується завдяки таким механізмам:

Аутентифікація сервера «Інтернет-банкінгу» Для того, щоби забезпечити захист від хакерських атак, спрямованих на підміну банківського Web-сервера і модифікації його контенту під час передачі, застосовуєть протокол SSL (Secure Sockets Layer) і сертифікат відкритого ключа, виданий одним з авторитетних Інтернет центрів сертифікації ключів (Certificate Authority) - VeriSign.

Аутентифікація користувачів «Інтернет-банкінгу» В «Інтернет-банкінгу» застосовується технологія двофакторної аутентифікації користувачів для організації безпечнішого доступу до системи. Технологія базується на двох чинниках: наявності у користувача дійсного особистого (таємного) криптографічного ключа, який зберігається у файловому контейнері або на токені, а також знання пароля (PIN-коду) доступу до цього ключа.

Конфіденційність переданих даних

З метою забезпечення конфіденційності даних, якими обмінюються користувачі з банком по каналах «Інтернет-банкінгу», ці дані шифруються. Таким чином, виключається можливість перехоплення та несанкціонованого читання платіжної та іншої інформації.

Авторизація платіжних документів З метою забезпечення автентичності (підтвердження авторства), неспростовності від авторства і цілісності електронних платіжних документів, які формуються клієнтами і передаються в банк, застосовується механізм електронного цифрового підпису. Дійсність електронного цифрового підпису перевіряється перед будь-якою операцією з обробки документа.

Засоби криптографічного захисту, інтегровані в систему «Інтернет-банкінг» для операцій формування та перевірки електронного цифрового підпису, сертифіковані відповідно до вимог законодавства України.

На рахунок рекомендацій щодо безпечної роботи в системі «Інтернет-банкінг» Для того, щоб убезпечити роботу в системі «Інтернет-банкінг», ознайомтесь з рекомендаціями фахівців інформаційної безпеки, які дозволять значно знизити ризики шахрайських дій з рахунками, доступ до яких здійснюється каналами «Інтернет-банкінгу».

1. Потрібно встановити на робочу станцію, з якої здійснюється доступ в систему «Інтернет-банкінг» ліцензійне антивірусне програмне забезпечення. Підтримувати оновлення версій, регулярно і своєчасно оновлювати антивірусні бази даних. Рекомендуємо використовувати антивірусне програмне забезпечення, яке поставляється російськими компаніями, наприклад Антивірус Касперського, Антивірус Dr.Web.

2. Встановити на робочу станцію, з якої здійснюється доступ в систему «Інтернет-банкінг»:

- Ліцензійне «антішпіонское» програмне забезпечення (antispyware);

- Програмний персональний мережевий екран (файервол, брендмауери) *.

На ринку присутній ряд програмних комплексів, які об'єднують в собі функції антивіруса, мережевого екрану, антишпигунського та іншого програмного забезпечення, призначеного для захисту робочих станцій.

Мережевий екран необхідно налаштувати таким чином, щоб максимально обмежити вихідний і вхідний мережевий трафік. Рекомендується дозволити тільки доступ до ресурсів системи «Інтернет-банкінг» і до інших мінімально необхідних ресурсів, наприклад, для оновлення баз вірусних сигнатур, антивірусних програмних засобів, операційної системи та іншого програмного забезпечення.

Антивірусне і антішпіонское програмне забезпечення рекомендується налаштувати для моніторингу всіх подій, а також періодичного сканування даних, які зберігаються на жорсткому диску робочої станції, з якої здійснюється доступ в систему «Інтернет-банкінг».

3. Необхідно регулярно і своєчасно оновлювати системне програмне забезпечення робочої станції, з якої здійснюється доступ в систему «Інтернет-банкінг», особливо, операційної системи, web-браузера, Java-машини. Рекомендується активувати можливість автоматичного оновлення програмного забезпечення.

4. Не рекомендується встановлювати на робочі станції, через які здійснюється доступ в систему «Інтернет-банкінг» програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо). Не рекомендовано здійснювати доступ з таких робочих станцій до ненадійних (незнайомим) інтернет-ресурсів.

5. Під час доступу в систему «Інтернет-банкінг» строго не рекомендується працювати в операційній системі під обліковим записом користувача, який має розширені права в операційній системі, наприклад, «Адміністратор».

6. При підключенні до веб-сайту системи «Інтернет-банкінг» (https://ibank.aval.ua/) переконайтеся в коректній аутентифікації веб-сервера системи «Інтернет-банкінг» за протоколом SSL. Уникайте підключень до веб-сайту системи по баннерним посиланнях або за посиланнями, що містяться в електронній пошті. Рекомендується ввести адресу веб-сайту системи самостійно і додати його в закладки браузера. При доступі до веб-сайту звертайте увагу на адресне поле браузера. Враховуючи, що веб-сайт системи «Інтернет-банкінг» має справжній і дійсний сертифікат від світової Інтернет центру сертифікації VeriSign, при вході в адресне поле браузера, повинні відображатися перші символи адреси https://, а не http:// (у вікні браузера може з'явиться повідомлення про те, що починається перегляд сторінки через безпечне з'єднання).

Сертифікат веб-сайту можливо переглянути за допомогою браузера. Для цього необхідно натиснути на значок «замочок» в полі статусу (цей значок розміщений в різних місцях залежно від браузера). На екрані з'явиться інформація про сертифікат безпеки веб-сайту ibank.aval.ua.

Значок закритого замочка, який відображається при безпечному підключенні до системи, є доказом того, що веб-сайт справжній.

7. Не рекомендовано здійснювати доступ в систему «Інтернет-банкінг" через посилання, отримані по електронній пошті, а також з неконтрольованих і ненадійних робочих станцій, розміщених в інтернет-кафе, готелях, офісах і т.д.

8. З метою заволодіння даними аутентифікації користувачів системи «Інтернет-банкінг» (особистий ключ та пароль доступу до нього) для подальшого незаконного використання, зловмисники скоюють атаки на робочі станції користувачів.

Основними методами заволодіння ключової інформації є:

- Поширення підроблених електронних листів, які містять посилання на адресу веб-сайту, замаскований під банківський;

- Поширення через електронні листи або веб-сайти програмного забезпечення, що містить шкідливий код і приховано передавального зловмисникові дані аутентифікації користувача;

- Несанкціоноване дистанційне керування персональним комп'ютером користувача шляхом віддаленого доступу.

Для попередження подібних ситуацій слід пам'ятати, що банк ніколи і не за яких обставин не здійснює розсилку електронних листів з проханням передати ключ, пароль, перейти за вказаним посиланням, а також не поширює по електронній пошті програми та їх оновлення. Відповідальність за зберігання особистих ключів та паролів возлогается на користувача.

У разі отримання подібних листів, програм або інших повідомлень електронною поштою необхідно терміново поінформувати про це банк листом або за телефоном, вказаним на сайті банку. Рекомендується видаляти підозрілі електронні листи не відкриваючи їх, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *. Exe, *. Pif, *. Vbs або інші файли.

9. Якщо настройку та обслуговування робочої станції, з якої здійснюється доступ в систему «Інтернет-банкінг», виконує сторонній фахівець, рекомендується контролювати його дії.

10. Рекомендації щодо безпеки поводження з даними аутентифікації (особистим ключем та паролем доступу):

- Особистий ключ та пароль доступу до нього є особливо критичними даними з точки зору безпечної роботи в системі «Інтернет-банкінг». Особистий ключ генерується з ініціативи користувача - його власника під особистим контролем. Банк ніколи не має доступу до особистих ключам користувачів. Для надійного зберігання та використання особистих ключів рекомендується застосовувати апаратні пристрої формування підписів (токени), які поставляються банком. Апаратний пристрій формування підпису (токен) - це засіб криптографічного захисту інформації, технічна реалізація якого забезпечує зберігання особистого ключа в захищеній пам'яті та виконання криптографічних операцій таким чином, щоб унеможливити копіювання особистого ключа або його знаходження за межами захищеної пам'яті пристрою.

Якщо користувач вибирає метод зберігання ключа у файловому контейнері, особистий ключ повинен зберігатися виключно на змінному носії інформації, наприклад на дискеті, CD-диску, USB-флеш пам'яті. Не допускається навіть тимчасове зберігання ключів на жорсткому диску робочої станції (комп'ютерів).

- Носій ключової інформації, який містить дійсний ключ (змінний носій інформації, токен) повинен постійно бути під особистим контролем користувача, таким чином, щоб не допустити доступ до нього інших осіб. Ні за яких обставин не допускається передача носія ключової інформації (токену) та / або розкриття пароля до нього іншим особам, у тому числі співробітникам банку.

- Носій ключової інформації, який містить дійсний ключ (знімний носій інформації, токен) повинен використовуватися тільки під час роботи в системі «Інтернет-банкінг». Не допускається залишення носія ключової інформації, підключеним до персонального комп'ютера, якщо робота у системі припинена або не проводиться, персональний комп'ютер використовується в інших цілях або в неробочі час.

- Пароль доступу (PIN-код) до особистого ключа не повинен зберігатися у відкритому вигляді (наприклад, бути записаним на папері) і використовуватися для інших систем і сервісів. Персональна відповідальність за зберігання пароля доступу (PIN-коду) і недопущення можливості його використання іншою особою повністю покладається на користувача.

- Рекомендується періодично змінювати пароль доступу до ключа (не рідше одного разу на місяць). Пароль повинен містити цифри, букви верхнього і нижнього регістра, а також спеціальні символи. При виборі пароля строго не рекомендується використання комбінацій, які легко встановлюються, наприклад, імена, дати народження, телефонні номери і т.д;

- У разі звільнення користувача або переведення його на посаду, яка не передбачає роботу в системі «Інтернет-банкінг», необхідно негайно звернеться в банк для блокування його ключа.

- У випадку компрометації або підозри в компрометації ключа (втрати, пошкодження носія ключової інформації, розголошення пароля або інших подій та / або дій, що призвели або можуть призвести до несанкціонованого використання ключа), необхідно терміново звернеться в банк з офіційним листом або по телефону для блокування ключа, при цьому обов'язково назвати блокувальний слово або.

11. У разі, якщо доступ в «Інтернет-банкінг» здійснюється зі статичного IP-адреси або діапазону адрес, рекомендується звернутися в банк для встановлення обмеження переліку IP-адрес і / або IP-підмереж, з яких можливий доступ до системи «Інтернет-банкінг» . У цьому випадку всі спроби підключення до системи «Інтернет-банкінг» з IP-адрес і / або IP-підсистем, які не включені в заявлений перелік блокуватимуться.

12. Рекомендується щодня аналізувати всі повідомлення про пропущені та отримані банком електронних розрахункових документів, а також негайно інформувати банк про випадки несанкціонованого зарахування (перерахування) коштів.

На думку експертів, основна і найважливіша загроза підстерігає будь-якого користувача Інтернет-банкінгу - це ризик шахрайського пошкодження та

несанкціонованого доступу до вашого рахунку. "Єдиний значний ризик, що можуть підстерігати користувачів цих систем є ризик протиправного привласнення коштів зловмисниками з використанням можливостей" Інтернет-банкінг ", проте, як і будь-який інший тип дистанційного обслуговування», - говорить Єгор Ізотов, начальник безпеки інформаційних технологій ПІВДЕНКОМБАНК. Саме тому банки намагаються використовувати різні системи і механізми, що забезпечують якщо ні, то принаймні підвищити безпеку використання онлайн-банкінгу.

Майже всі банки, що надають онлайн-банкінг, застосовуєть SSL-шифрування даних, переданих з комп'ютера користувача в банк і назад. Цей захід безпеки усуває раніше поширений вид шахрайства. "У минулому часто використовувалася схема« людина посередині. Платіжна інформація перехоплена на етапі, коли вони відправлені від клієнта, але ще не дійшли до банку шахрай змінює дані і тільки після цього відправляє їх у банк ", - розповідає Борис Косяков, начальник інформаційної безпеки Астра Банк.

Щоб скористатися всіма перевагами безпечних даних, слід дотримуватися основних вимог безпеки в Інтернеті - не відповідайте на підозрілі повідомлення (отримані нібито від вашого банку) і не проходять по невідомих посиланнях.

Одноразові паролі, отримані від банкомату. У рамках цієї системи захисту, ніж звичайні ім'я користувача і пароль, щоб увійти і підтвердження операцій користувач повинен ввести одноразовий пароль, список яких він може отримати в банкоматі банку. Така система має вагому перевагу - здійснювати операції по картковому рахунку через інтернет-банкінг, людина повинна мати принаймні, у присутності саму карточку, а також знати PIN код, щоб отримати список паролів в банкоматі.

Але, слід відзначити недоліки такої системи захисту. По-перше, список паролів, надрукована у вигляді отримання в банкоматі, вам доведеться подати для підтвердження майбутніх операцій. Це означає, що якщо ви випадково втратите або відмовитися від перевірки (або просто використовувати всі паролі), ви повинні піти на нову. Часто ви можете отримати список паролів не в

кожному банкоматі банку, і цілком імовірно, що вам доведеться слідувати за ним в інший кінець міста. Крім того, список може заволодіти злочинці.

Якщо у вашій системі онлайн-банкінгу включає в себе використання список одноразових паролів, намагайтеся дотримуватися простих правил. По-перше, не викидайте список можливих паролів і спробувати не втратити. По-друге, не зберігайте список одноразових паролів, а також логін і пароль до облікового запису. Останній не рекомендується писати, легше запам'ятати.

Одноразові паролі SMS. Цей спосіб аутентифікації користувача в системі онлайн банківській, є найбільш поширеним в пропозиціях українських банків. Згідно з цією системою, кожної операції, які ви виконуєте використанні онлайн-банкінгу, повинна бути підтверджена одноразовим паролем, який ви отримаєте в SMS повідомлення на Ваш мобільний телефон. У цьому випадку ваш мобільний номер повинен бути «прив'язаний» до номера рахунку. Ця система має ряд переваг. По-перше, це досить проста у використанні - вам не потрібно спеціального устаткування, а також порядок підтвердження операції займає всього пару хвилин. По-друге, вона дозволяє захистити ваш аккаунт від використання хакерами - навіть якщо шахраї дізнаються ваше ім'я користувача та пароль для входу в систему, вони не мають доступу до ваших грошей, і ви дізнаєтеся про спробу провести несанкціоновану робота повідомленнями SMS. Крім того, вам не потрібно, щоб зберегти список одноразових паролів, яка означає, що ви не можете втратити його, і ти не кради. Дійсно, нападники важко охопити одноразовий пароль, який триває протягом короткого часу. Якщо вони не володіють вашого мобільного телефону. І це марно системи було б у випадку, якщо ви використовуєте онлайн-банкінгу з мобільного телефону і зберігати паролі в браузері. Потім, ви вкрав телефон, шахрай будете отримувати свій рахунок у повному розпорядженні.

Якщо ваш банк використовує аутентифікацію користувачів за допомогою SMS, потрібно дотримуватися наступних правил:

не використовувати інтернет-банкінг за допомогою мобільного телефону;

не зберігати пароль на облік в браузері;

У разі втрати або крадіжки мобільного телефону - негайно зверніться в банк, щоб заблокувати ваш рахунок для онлайн-банкінгу.

Електронний цифровий підпис (ЕЦП)

Цей механізм часто використовується для підтримки банку компанії, але іноді він пропонується і для індивідуальних клієнтів. Плюс ЕЦП в тому, що він дає змогу однозначно і ідентифікувати користувача. Недоліком є те, що цифровий підпис також може бути уразливий для шахрайства. Зловмисники можуть дістатися до ключа цифрового підпису, щоб заразити комп'ютер шкідливими програмами. "Є" троянів ", які здатні знайти і вкрасти заражені інформаційної безпеки комп'ютера (ідентифікатори, паролі і навіть ключі ЕЦП) користувачів для доступу до різних послуг (включаючи віддалені сервери та клієнтські служби)", - говорить Борис косяки.

Якщо підтвердження від ваших фінансових операцій через інтернет ви використовуєте цифровий підпис, не забувайте використовувати антивірусне програмне забезпечення і регулярно сканувати комп'ютер на наявність зараження комп'ютерними вірусами. Експерти також радять не залишати ключ підпису підключений до комп'ютера, якщо ви не використовуєте його.

Інші банки пропонують для інтернет-користувачів купити спеціальний пристрій - одноразовий пароль генератора. Генератор підключений до комп'ютера через USB-порт і не вимагає спеціального програмного забезпечення. Ще інші установи пропонують зовнішній електронний ключ, який створюється при першому підключенні до системи Інтернет-банкінг, записується на носій, а потім використовувалася в операціях в системі.

Такі системи, по суті, це спрощена версія ЕЦП. Серед недоліків вони можуть виділити те, що ви не можете увійти в свій аккаунт, не маючи на руках "ключ", і завжди носити його з собою може бути не дуже зручно і безпечно.

Крім перерахованих вище, банки часто застосовують додаткові заходи щодо забезпечення безпечного використання інтернет-банкінгу:

обмеження використання особистого сертифіката - система дозволяє деяким банкам використовувати електронний ключ (цифровий сертифікат)

тільки на тому комп'ютері, на якому він був створений. Таким чином, для здійснення платежів через інтернет-банкінг, ви можете тільки з персонального комп'ютера (хоча заяви Перегляд акаунт може бути на інших пристроях);

віртуальна клавіатура - призначена для шахраїв не могли "вірити" ваші реєстраційні дані при введенні їх із звичайної клавіатури за допомогою комп'ютерних вірусів («троянські»);

обмежують тривалість сесії - у разі бездіяльності користувача, сесія в системі Інтернет-банкінгу через певний час (зазвичай 10-15 хвилин) буде закрито. Після цього для поновлення необхідності повторно пройти аутентифікацію;

Історія - За допомогою цієї функції, користувач інтернет-банкінгу буде знати, якщо хтось інший, ніж вона була підключена до системи, і бути в змозі відслідковувати всі несанкціоновані операції, якщо вони були зроблені.

Експерти відзначають, що найчастіше причиною шахрайського доступу до рахунку з Інтернет-банкінг, безтурботність і недбалість користувача. Тому, щоб уникнути можливих проблем, власнику рахунку повинні бути захищені доступу до даних. По-перше, експерти радять періодично змінювати паролі для доступу в систему, бажано робити це раз на місяць і не використовують інтернет-банкінг на ненадійних комп'ютерів (наприклад, інтернет-кафе).

Крім того, слід дотримуватися обережності при роботі в Інтернеті. "Шахраї широко використовують методи" соціальної інженерії "для того, щоб заманити дані аутентифікації (ім'я користувача, пароль і т.д.) клієнтів старий метод -." Фішинг "повідомлення електронної пошти, які заохочують одержувачам відправляти свої дані аутентифікації для хакерів або пропонують пройти по посиланню на шахрайський веб-сайт. Із зростанням популярності соціальних мереж («Однокласники», Twitter, Facebook) шахраї відразу ж почали використовувати для "фішинг" повідомлення соціальних мереж. Крім того, хакери створюють шахрайські копій веб-сайтів для онлайн-банкінгу з іменами, дуже схожими на справжні ", - каже Борис косяки І якщо ви входите на цьому сайті дані свого облікового запису, вони тут же потрапляють до рук шахраїв ..

Якщо у вас є побоювання, що шахраї мають доступ до вашого рахунку через інтернет-банкінг, експерти радять зробити наступні кроки:

- ✓ відключити комп'ютер від мережі Інтернет;
- ✓ зверніться в операторський центр (а при необхідності - в офісі) вашого банку, поясніть проблему і попросити заблокувати Ваш рахунок;
- ✓ перевірити комп'ютер на наявність зараження шкідливим програмним забезпеченням;
- ✓ для відновлення роботи з онлайн-банкінгу тільки тоді, коли ви впевнені, що немає ніякої загрози;
- ✓ змінити пароль на аккаунт.

Якщо ваші підозри виправдалися, і рахунок був знятий з рахунку несанкціонованих платежів ви повинні зробити заяву про те, що трапилося в банк і поліцію. У цьому випадку, рекомендується не вживати ніяких дій на комп'ютері (встановлення або видалення програмного забезпечення тощо) до прибуття співробітників правоохоронних органів або експертів банку, оскільки будь-які зміни можуть вплинути на розслідування інциденту.

Крім ризику шахрайського злому, інтернет-банкінг користувач піддається і іншим загрозам. Наприклад, небажані дебетові, через Інтернет-банкінг може статися, якщо користувач неправильно введені дані для відправки грошей.

"Якщо клієнт при відправці платежу через Інтернет-банкінг допустив помилку в номер рахунку, повернення такої процедури оплати така ж, як якщо платіж був відправлений при відвідуванні відділення банку. Бачачи, що платежі в Інтернеті банківської системи помилково поставляється, клієнт повинен повідомити ваш банк », - говорить Юлія Морозова, директор департаменту карткового бізнесу VAB Банку.

Таблиця 3.3.1

Системи безпеки Інтернет-банкінгу, використовувані найбільшими українськими банками (банки в таблиці розташовані за розміром активів

Банк	Яка система безпеки використовується	Додатково
ПриватБанк	Одноразові смс-паролі	віртуальна клавіатура, обмеження тривалості сесії
Укрексімбанк	Одноразові паролі (використовується USB-генератор) ЕЦП	ЕЦП
УкрСиббанк	Одноразові смс-паролі	особистий ключ, віртуальна клавіатура
Укрсоцбанк	Одноразові паролі (виходять в банкоматі банку)	код PIN2, видається одночасно з картою
Альфа-Банк	Одноразові смс-паролі	віртуальна клавіатура, обмеження тривалості сесії
ОТП Банк	Одноразові паролі (використовується USB-генератор)	
Фінанси та Кредит	Одноразові смс-паролі	ЕЦП
Перший Український Міжнародний Банк	Одноразові смс-паролі	
Форум	Одноразові смс-паролі	історія підключень, обмеження тривалості сесії
Дельта-Банк	Одноразові смс-паролі	
Сведбанк	Одноразові смс-паролі	віртуальна клавіатура
Південний	Зовнішній електронний ключ	ЕЦП
Сбербанк Росії	Одноразові смс-паролі	ЕЦП
Universal Bank	Особистий цифровий сертифікат	можна замовити смарт-карту для зберігання особистого сертифіката

		За даними компанії "Простобанк Консалтинг"

За даними "Простобанк Консалтинг"

Експерти в банку відзначають, що успіх виправлення помилки, в першу чергу залежить від швидкості реакції на його жертви. Якщо ваші кошти ще не були відправлені до банку одержувача, то ви повернете їх майже відразу. Якщо оплата вже пішов в інший банк - вам доведеться трохи почекати. "Якби ці гроші були відправлені в інший банк на рахунок юридичної особи, у зв'язку з тим, що інші деталі не відповідають усім вимогам, гроші будуть повернені протягом трьох днів, а на підставі заяви", - каже Ростислав Божко, провідний спеціаліст альтернативної БАНК розподілу Марфін. Тим не менш, повернення може бути відкладено на більш тривалий період часу. "Точні терміни повернення в даному випадку буде залежати від банку одержувача Тобто, як тільки банк-одержувач поверне кошти банку-відправнику, кошти будуть зараховані на клієнтів,.", - Розповідає Юлія Морозова.

Найскладніше справа йде в тому випадку, якщо гроші були відправлені на рахунки приватних осіб і в даний час на їх рахунку. «Якщо гроші були зараховані на рахунок одержувача, відповідно до р.1.7. І 1.19. Інструкції НБУ« Про безготівкових платежів у національній валюті в Україні »№ 22 від 21.01.04g. розпорядника коштів є власником рахунку. Відповідно, лист з проханням повернути помилково зараховані кошти на рахунок клієнта повинні бути спрямовані одержувачем коштів », -. Каже Єгор Ізотов У цьому випадку, отримати свої гроші назад, ви можете або за згодою одержувач, або за рішенням суду.

Тим не менш, інтернет-банкінг є безпечним та інших ризиків, виникнення яких люди не беруть участь. Наприклад, якщо під час операції існує технічна несправність. Експерти стверджують, що цей ризик не є великою загрозою для власника рахунку. "Системи інтернет-банкінгу, як і будь-який інший сучасний обробки даних системи були розроблені таким чином, щоб у разі технічних або програмного збою під час транзакції документ просто не буде прийнятий банком», - каже Єгор Ізотов. Але навіть якщо неправильні діяльність ще

утримувала - слід негайно звернутися в банк, щоб виправити помилку. "Якщо ви робите трансляція невдала в транзакції, то ця невдача досить інформувати банк і кошти будуть повернуті на рахунок в найкоротші терміни», - каже Ростислав Божко.

У той же час, користувачі інтернет-банкінгу може зіткнутися з набагато більше неприємної ситуації. Так, за повідомленнями ЗМІ, клієнт одного з банків Росії на початку 2009 року, потрапив у неприємну історію, коли одноразові паролі для підтвердження платежів в Інтернеті банківської системи були спрямовані не до нього, а номер мобільного телефону суперника. У результаті шахраї були списані з рахунку великі суми грошей. Жертвою переконаний, що інцидент був пов'язаний із співробітниками банку, як тільки вони просто не міг дозволити нападаючим реєстраційні дані (ім'я користувача і пароль від рахунку), але і відправити їх одноразовими паролями.

Досвід жертвою в цій ситуації показує, що довести щось у таких умовах важко. Швидше за все, доведеться звертатися до суду, і його рішення буде залежати від змісту договору, підписаного з банком. Тим не менш, експерти відзначають, що цей вид шахрайства не має прямого відношення до використання інтернет-банкінгу, так як у присутності співробітника нечесні махінації з таким же успіхом зробити підроблені платіжного доручення.

Для надання якісних послуг для своїх клієнтів, банки в даний час пропонують найвищий рівень захисту даних. Використання веб-сервіс з сертифікатом безпеки https://, є вимоги до паролю для входу в систему. Для підтвердження кожної транзакції з проханням введення одноразового пароля. Система реалізована генерація ключа цифрового підпису. З кількох невдалих спроб увійти в обліковий запис автоматично блокується.

Для виключення перехоплення конфіденційних даних вірусними програмами запропонувати використовувати віртуальну клавіатуру при введенні імені користувача та пароля.

Якщо рахунок зламали, перш за все, вам необхідно відключити зламаний (інфіковані) комп'ютер від мережі і повідомити про це в банк, щоб заблокувати рахунок клієнта, щоб запобігти шахрайству. Забезпечити безпеку всіх

необхідних даних для подальшого розслідування - не змінювати на зламаному (інфіковані) комп'ютера. Для дослідження залучення кваліфікованих фахівців (з банку або спеціалізованих фірм). Тільки кваліфіковані розслідування і з'ясування причини допоможе уникнути подібних інцидентів в майбутньому.

Практика показала, що зловмисники часто не намагаються проникнути в комп'ютерні мережі банків, і захопити контроль над клієнтськими комп'ютерами, і отримувати доступ до ключів електронного цифрового підпису та пароль, здійснювати платежі від їх імені. Отож, досить надійна схема безпеки повинна охоплювати наступні мінімальний набір завдань:

- створення безпечного, довіреної середовищі і продовжувати функціонування віддаленої служби на стороні клієнта банку. Ніякі зміни у виробничому середовищі коду і його параметрів, що виникають у роботі системи, не повинні бути збережені при виключенні системи. У цьому випадку, навіть якщо зловмисник якимось чином отримати і віддаленого доступу до середовища в процесі його експлуатації, він не буде володіти нею на постійній основі;
- створення захищеного від несанкціонованого доступу до інформації каналу між клієнтом і банком;
- забезпечення умов, які не дозволяють крадіжки ключів і паролів, що використовуються для роботи в віддаленої служби.

Відповідає цим критеріям спеціальних комп'ютерних віртуальних отримані шляхом завантаження із спеціального носія системи незмінні, або "нормальної", але в кожному разі - вузькоспеціалізований, тільки вирішальні одну задачу: забезпечити системі дистанційного обслуговування. Ці рішення, в розробці якої взяли участь фахівці нашого банку вже існують, на жаль - не в Україні.

Банки докладають всі зусилля, щоб гарантувати, що технічні засоби інтернет банківська система захищена грошових коштів і користувачів фінансової інформації від зловмисників. Звичайно, всі ці складні і дорогі системи найбільш ефективно працювати разом з відповідальними та уважне ставлення до своїх користувачем паролів, ключів, цифрових підписів та інших засобів захисту, пропонованих банками. Рекомендовано дотримуватися

декількох простих правил безпеки, які забезпечать конфіденційність особистих даних і збереження грошей свого клієнта:

НЕ повідомляйте свій пароль. Співробітники банку ніколи, ні за яких обставин, просять паролі;

НЕ зберігати ключ цифрового підпису на комп'ютери інших людей;

Уникнути платежів або змінювати пароль з комп'ютерів, на яких багато людей мають доступ (комп'ютери в інтернет-клуби, зали очікування на вокзалах, аеропортах і т.д.);

Якщо користувач враження, що хтось шпигував свій пароль, ви повинні негайно повідомити про це банк і блокувати доступ до системи;

Якщо клієнт як і раніше не в змозі забезпечити конфіденційність своїх даних, перше, що він повинен зробити - це повідомити банку про цей інцидент. Банк буде блокувати доступ користувача до системи і рахунок клієнта, щоб уникнути фінансових втрат. Клієнтові потрібно буде зробити заяву, в якій він розповідає обставини події. Розслідування цих подій проводить служба безпеки банку з правоохоронними органами.

Висновки до розділу 3

Банки в усі часи були центром передових технологій, майданчиком для впровадження інновацій. Сьогодні це високоорганізована система, з оперативним і компактним керуючим центром. Якісна організація і управління структурами кредитної установи з багатопрофільними відділами та диверсифікованим двостороннім взаємодією з клієнтами досягаються, в першу чергу, впровадженням новітнього обладнання та програмних комплексів.

Саме в цій площині лежить ключ до успіху і ефективним банківським технологіям. З часів появи перших банків основними складнощами розвитку цього бізнесу були: надійність, асортимент послуг, що надаються, територіальна доступність і безпеку.

Ці ж питання ставилися в першу чергу і перед розробниками нових банківських технологій сьогоднішнього дня. Головне досягнення кінця 20-го століття це можливість створити для клієнта віртуальний банк.

Немає тепер тотальної необхідності витрачати дорогий час, у що стали незручними мегаполісах, на тяжке переміщення свого тлінного тіла в банк. Стало можливим перенести в нього лише свій активний і динамічний розум - інтернет з'явився для нас тим чарами, про який твердили старі казки.

Тепер ми можемо переміщатися в просторі зі швидкістю світла, залишаючись при цьому вдома в затишному кріслі.

Вчасно розпізнавши в глобальній мережі підмога, банківські технології дали нам можливість керувати своїми рахунками віддалено: через персональний комп'ютер, портативний смартфон або за допомогою мобільного зв'язку, за допомогою голосових або тональних команд.

Другим кроком став вихід зі скрути в плані територіальної доступності - завдяки банкоматам! Для банку це можливість знизити операційні витрати, зайняти персонал чимось більш корисним, а то й зовсім скоротити його надлишки. Нарешті, замість боротьби з профспілками - ефективно заробляти двадцять чотири години на день, сім днів на тиждень.

Те ж саме стосується платіжних терміналів, які беруть на себе більшу частину функцій старих банків. А поважні будівлі з колонами й левами, в який став старим «новому імперському» стилі, банки тепер перетворили просто в депозитарні сховища або сакральні декорації для реклами і проведення виставок експресіоністів.

Банк завтрашнього дня це сторінка в мережі або взагалі, незабаром, просто блог, з можливістю брати і давати кредити під «лайки», фічі і кількість переглядів!

ВИСНОВКИ

Сучасні форми дистанційного банківського обслуговування, що виникли останнім часом з появою персональних комп'ютерів, телекомунікацій і нових засобів масової інформації та багато інших технологій. У побутовому сенсі дистанційне обслуговування відноситься до банківських операцій без відвідування клієнтом банку (на основі замовлень посилаються за допомогою дистанційних засобів передавання інформації).

Обслуговування різних сегментів ринку вимагає, щоб банки використовують оптимальні технології, пристрої та канали доступу. Канал доступу, тобто повідомлення, яке використовує управління клієнтського рахунку, і вони можуть бути найрізноманітнішими - банкомат, телефон, мобільний телефон, що підтримує WAP протокол або протокол обміну короткими повідомленнями SMS, Інтернет-центр (Call-центр), персональний цифровий помічник електронною поштою, факсом, спеціалізовані інтерфейси для постачальників послуг, таких як Visa Interactive, Integrion, CheckFree.

У розвинених країнах вже давно інтернет-банкінг необхідною частиною життя, а в нашій країні вони мають постійно доводити свою цінність для людей. У більшості розвинених країн, заробітна плата нараховується на банківський рахунок, і левова частина оплати проводиться за безготівковим розрахунком. Цілі комерційних банків в Україні сьогодні - стати таким же необхідним елементом життя для українця. Це може бути зроблено тільки на основі впровадження необхідних сервісів. Іінтернет-банкінг - це та область, яка може допомогти комерційним банкам в їх просуванні і удосконаленні роздрібних послуг.

Виходячи з вище сказаного , сьогодні ми можемо зробити висновок, що український ринок онлайн-банкінгу, хоча знаходиться в майже початковому етапі , але збільшуватиме темпи розвитку, в тому числі можливість використання інтеграція та розвиток онлайн покупок послуг, які доповнюють один одного і взаємостимулюють. У загальному, українські споживачі тепер

мають можливість порівнювати, і користуватися послугами інтернет-банкінгу.

СПИСОК ДЖЕРЕЛ ПОСИЛАНЬ

1. Ачкасов А.И. Активные операции коммерческих банков. - М., Косалтбанкир, 2004р..
2. Баласинович Б. Стан та перспективи розвитку ІКТ-індустрії в Україні // Банківська справа.- 2004.- № 5/6.- С. 39-48.
3. Бережной О. А. Інформаційно-аналітичне забезпечення прийняття ефективних управлінських рішень // Актуальні проблеми економіки.- 2004.- № 9.- С. 26-29.
4. Березина М.П. Деньги и современноеобщество. / М.П. Березина – М.: ФЕНИКС, 2006. – 435 с.
5. Бэлоглазова Г. Н.. Аудит банків // Г. Н. Бэлоглазова, Л. П. Кролівецька, Е. А. Лебедева / –М.: Фінанси і статистика, 2002. – 352 с
6. Васюренко О.В. Банківський менеджмент: Посібник. – К.: “Академія”, 2001. – 320 с.
7. Вересюк А. Малый электронный банковский бизнес // Банковская практика за рубежом.- 2005.- № 8.- С. 65-69.
8. Гриценко Р. Сучасні платіжні технології та їх використання у соціальній сфері // Вісник Національного банку України. – 2004. – №10. – с. 18-20.
9. Джоунс П. Реинжиниринг дебетовых карточных систем // Карт_Бланш. – 2005. – №5. – с.26-31.
10. Долин П.А. Справочник по технике безопасности. – М.: Энергоиздат, 2003. – 800 с.
11. ДЭффективные кредиты // Бизнес. – 2006. – № 1-2. – с. 32-34.
12. Єрьоміна Н.В. Банківські інформаційні системи: Навч. Посібник. – К.: КНЕУ, 2000. – 220с.
13. Завальнюк Є. Розвиток прикладної банківської системи з урахуванням вимог міжнародних стандартів: інструментальний аспект // Вісник Національного банку України. – 2005. – №7. – с. 26-28.

14. Закон України “Про банки і банківську діяльність”. (Відомості Верховної Ради, 2001 р., N 5-6, ст.30), редакція закону від 22.06.2004 р. чинна З 15.07.2004 р.
15. Закон України “Про електронні документи та електронний документообіг”. (Відомості Верховної Ради, 2003, N 36, ст.275)
16. Закон України “Про захист інформації в автоматизованих системах”. (Відомості Верховної Ради, 1994 р., N 31, ст.286), редакція закону від 11.05.2004 р. чинна з 09.06.2004 р.
17. Закон України “Про Національний банк України”. (Відомості Верховної Ради, 1999, N 29, ст. 238), редакція закону від 03.02.2004 р. чинна з 27.02.2004 р.
18. Закону України "Про охорону праці" (ухвала Верховної Ради України від 14 жовтня 1992 року № 2695-XII)
19. Запорожець З. Сучасні тенденції у сфері банківських інформаційних технологій // Вісник Національного банку України. – 2004. – №3. – с. 38-39.
20. Запорожець З. Управління банківськими ризиками в контексті інформаційних технологій // Вісник Національного банку України. – 2004. – №10. – с. 54-59.
21. Заруцька О. Проблеми розвитку банківського управлінського обліку // Вісник Національного банку України. – 2005. – №8. – с. 40-42.
22. Засадна Х.О. Про захист послуг Інтернет-банкінгу/ Х.О. Засадна // Вісник університету банківської справи національного банку України. – 2008. − № 3. − С. 225-229.
23. Интегрированный Front-Office как инструмент развития банка // Банкиръ. – 2005. – №3. – с. 38-40.
24. Івасів Б.С. Операції комерційних банків. - К., 1992.
25. Івченко І., Гуска І. Комплексна система антивірусного захисту інформаційної мережі НБУ // Вісник Національного банку України. – 2004. – №7. – с. 38-41.

26. Інструкція Національного банку України від 28.08.2001 р. "Про порядок регулювання діяльності банків в Україні" з наступними змінами і доповненнями.
27. Інструкція Правління НБУ “Про безготівкові розрахунки в господарчому обороті України” №135 від 25.04.2001 р.
28. Інструкція Правління НБУ “Про організацію роботи з готівкового обігу установ банків України” № 69 від 19.03.2001 р.
29. Інструкція про застосування плану рахунків бухгалтерського обліку комерційних банків України. Затверджено постановою Правління НБУ від 21.11.1997 р. № 388.
30. Інструкція про міжбанківський переказ грошей в Україні в національній валюті (від 17.03.2004 р.)
31. Інформаційні системи і технології в економіці: Посібник для студентів ВНЗ/ За ред. В.С.Пономаренка. – К.: Видавничий центр “Академія”, 2002. – 544 с.
32. Капий А. Интернет-платежи: второе дыхание // Карт_Бланш. – 2005. – №3 – с. 27-33.
33. Капралов Р. Рынок платежных систем: новые горизонты // Банкиръ. – 2005. – № 2. – с. 23.
34. Карпенко С.Г. Інформаційні системи і технології. Навчальний посібник. – К.:Кондор, 2004 р. – 192 с.
35. Коваль І., Гаврилюк В. Система електронних міжбанківських переказів НБУ // Вісник Національного банку України. – 2005. – №1. – с. 8-10.
36. Коломієць С. Інтернет-платежі за технологією НСМЕП // Вісник Національного банку України. – 2005. – №8. – с. 18-19.
37. Коломієць С. Перспективи розвитку Національної системи масових електронних платежів // Вісник Національного банку України. – 2005. – №4. – с. 33-34.
38. Коряк С.Ф., Самофалов Л.Д. Комп’ютерні системи обробки та передачі фінансової інформації. / Підручник для студентів вищих навчальних закладів. За ред. Самофалова Л.Д. – Харків: “Компанія СМІТ”, 2004. – 290 с.

39. Коцовська Р., Ричаківська В., Табачук Г., Гудзевич Я., Вознюк М.: Операції комерційних банків / 2-ге вид., доп. – Львів: ЛБІ НБУ, 2001. – 516 с.
40. Кравець В. Інтернет-комерція в Україні // Вісник Національного банку України. – 2004. – №3. – с. 9-12.
41. Кравець В. Інтернет-платежі в системі безготівкових розрахунків // Вісник Національного банку України. – 2005. – № 11. – с. 21-23.
42. Крыжановская Л. Банкоматы стали «умнее» // Банкиръ. – 2005. – №3. – с. 52-53.
43. Куклев К. Карточные продукты для банков // Банкиръ. – 2005. – № 2. – с. 56-57.
44. Лакосник Е. Новые IT для финансовых институтов // Банковская практика за рубежом.- 2004.- № 11.- С. 34-39.
45. Лессік Д., Івченко І. Інформаційна безпека банківської діяльності: вимоги міжнародних стандартів // Вісник Національного банку України. – 2004. – №9. – с. 25-27.
46. Лищишин М., Шаповалов С., Сажинець С. Інтернет - інструмент розвитку інформаційних технологій // Підприємництво, господарство і право.- 2004.- № 12.- С. 124-126.
47. Марченко В. Комментарии к Положению о порядке эмиссии платежных карт и осуществления операций с их применением // Карт_Бланш. – 2005. – №6-7. – с. 34-39.
48. Махаєва О. Електронні гроші в Європі та Україні // Вісник Національного банку України. – 2004. – №9. – с. 22-24.
49. Мирун Н.И., Герасимовыч А.М. Банковское обслуживание предприятий и населения. - К., 2004р.
50. Недилько А. Информационная эволюция // Банковская практика за рубежом.- 2004.- № 8.- С. 65-67.
51. Недилько А. Место информационных технологий в стратегии развития // Банковская практика за рубежом.- 2005.- № 2.- С. 56-58.

52. Нікіфорова А. О. Вітчизняний та зарубіжний Інтернет-банкінг – стан, проблеми та перспективи розвитку // А. О. Нікіфорова / Регіональна економіка. – 2010. – № 8. – С. 23-26. С 24

53. Облік та аудит в комерційних банках / А.М.Герасимович, Т.В.Кривов'яз, О.А. Мазур та ін. / За ред. д-ра екон. наук, проф. А.М.Герасимовича. – Львів: Фенікс, 2004. – 512 с.

54. Охоба О. М. Інформаційні технології в управлінні інвестиційними проектами // Актуальні проблеми економіки.- 2004.- № 9.- С. 115-117.

55. Панова Г.А. Банковское обслуживание частных лиц. - М., 2004р.

56. Політюк Л.Г., Маленька Е.Ю. Розвиток Інтернет-банкінгу як форми вдосконалення дистанційного керування в банківській системі / Л.Г. Політюк, Е.Ю. Маленька // Часопис економічних реформ. – 2011. − № 2. − С. 66-68.

57. Положення про ведення касових у національній валюті в Україні, №72 від 19.02.2001 р.

58. Положення про Ліцензійну палату України, затвердженим Указом Президента України від 16 липня 1997 року N 648/97, і у виконання ухвали Кабінету Міністрів України від 3 липня 1998 року N 1020 (1020-98-п)

59. Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженим Указом Президента України від 22 травня 1998 року N 505/98;

60. Положення про систему електронної пошти Національного банку України (від 29.12.2004 р.)

61. Примостка Л. Економічні ризики в діяльності банків // Банківська справа. – 2004. – № 3. – с. 16.

62. Развитие Интернет-банкинга Ffktura.ru // Карт_Бланш. – 2004. – №9-10. – с. 47-49.

63. Решетніков П. Досвід використання інформаційних технологій у банківській справі // Вісник Національного банку України. – 2004. – №4. – с. 40-43.

64. Рид Э., Коттер Р., Гилл Э. и др. Коммерческие банки /Пер. с англ. Под ред. В.М. Усоскина. - М.: СП "Космополис", 2003р.

65. Рогач І.Ф., Сендзюк М.А., Антонюк В.А. Інформаційні системи у фінансово-кредитних установах: Навч. посібник. – 2-ге видання, перероб. і доп. – К.: КНЕУ, 2004. – 239 с.
66. Рогач І.Ф., Сендзюк М.А., Антонюк В.А. Інформаційні системи у фінансово-кредитних установах: Навч. Посібник. – 2-ге вид., перероб, і доп. – К.: КНЕУ, 2001. – 239 с.
67. Рожков А.П. Пожарная безопасность на производстве. Учебное пособие. – Киев: Редакция журнала «Охрана труда», 2002р. – 219 с.
68. Савицкий Н.И.. Экономическая информатика. К.:Кондор, 2005 – 429 с.
69. Сибаров Ю.Г. и др. Охрана труда в вычислительных центрах. – М.: Машиностроение, 2004р. – 192с.
70. Ситник В.Ф. та ін. Основи інформаційних систем: навч. Посібник. – К.: КНЕУ, 1997. – 252 с.
71. Стельмах В.С., Єпіфанов А.О., Сало І.В. та ін. Економічна інформатика. – Суми. Видавництво “Слобожанщина”. 2000. – 260 с.
72. Страхарчук А.Я., Страхарчук В.П. Інформаційні технології в економіці: Навч. посібник. – К.: УКООП “Освіта”, 1999. – 355 с.
73. Усоскин В.М. Современный коммерческий банк: управление и операции. - М., 2003р.
74. Уткин В.Б., Балдин К.В. Информационные системы и технологии в экономике. Учебник для вузов. – М.: ЮНИТИ-ДАНА, 2003. – 335с.
75. Фурман В. Перспективи створення альянсів страхових компаній і банків України // Вісник Національного банку України. – 2005. – №4. – с. 20-22.
76. Харченко В. Нове у використанні платіжних карток // Вісник Національного банку України. – 2005. – №8. – с. 15-17.
77. Хит сезона: «Платежная карта 2005» // Карт_Бланш. – 2005. – №6-7. – с. 6-14.
78. Чуб О.О. Розвиток Інтернет-банкінгу в глобальному середовищі / О.О. Чуб // Вісник Української академії банківської справи. - 2009. - №1 (26). - С. 62-67.

79. Шквір В.Д., Загородній А.Г., Височан О.С. Інформаційні системи і технології в обліку – Львів: Видавництво Львівського національного університету “Львівська політехніка”, 2003. – 268 с.
80. Шпірко А., Прокопенко А. Запровадження та ефективне використання електронного документообігу й електронного підпису в Україні: проблеми, нові можливості, шляхи розвитку // Вісник Національного банку України. – 2005. – №3. – с. 36-41.
81. Яковенко С. І. Інформаційні технології й реінжиніринг у процесах організації, трансформації та управління корпораціями // Актуальні проблеми економіки.- 2005.- № 10.- С. 222-235.
82. Яковенко С. І. Реінжиніринг бізнес-процесів шляхом інформатизації управління на підприємствах України // Актуальні проблеми економіки.- 2004.- № 9.- С. 118-130.