НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ
Українська академія банківської справи

НАУКОВО – ДОСЛІДНА РАБОТА

“ СУЧАСНІ ТЕХНОЛОГІЇ ФІНАНСОВО-БАНКІВСЬКОЇ ДІЯЛЬНОСТІ НА УКРАЇНІ ”

Державний реєстраційний номер 0102U006965

Тема: Вдосконалення системи боротьби з шахрайством з використанням Інтернету та застосування інших високих технологій.

Суми – 2003

Керівник теми: к.е.н., доц. кафедри банківської справи
Подоляка Олег Іванович

Виконавці:

1. Вахнюк Сергій Валерійович - асистент кафедри економічної кібернетики
2. Терехов Євгеній Миколайович - провідний інженер
3. Колдовський В’ячеслав Васильович - асистент кафедри управління і зовнішньої діяльності
4. Рижкін Дмитро Володимирович – зав. лабораторією кафедри банківської справи

ЗМІСТ.

ВСТУП

За останній час, як свідчать повідомлення інформаційних агенств, збільшилась кількість випадків шахрайства у світовому банківському середовищі при сдійсненні едектронних бізнес процесів. Сучасні комерційні банки, що застосовують у своїй діялності новітні технологічні рішення перебувають під постійною увагою інформаційних злочинців. Цілком очевидно, що вдалі випадки електроних злочинів можуть мати катастрофічні наслідки для електронного банкінгу, які полягають у безпосередніх фінансових втратах, виведення з ладу високотехнологічного обладнання, набуття негативної репутаціїї. В сучасних умовах фінансового ринку, банківським установам особливо важливо загострити увагу на питаннях інформаційної і фінансової безпеки, що у випадку електронного банкінгу набувають особливого значення.

Використання нетрадиційних каналів доступу до клієнтських рахунків приводить до того, що до звичайних ризиків, які вже були випробовувані банком, додаються нові, котрі мають специфічну природу[3].

Зазначена небезпека полягає в імовірності утворення збитків та недоодержання прибутків внаслідок збоїв у виконанні щоденних, рутинних банківських операцій, що здійснюються із застосуванням сучасних інформаційних технологій. Мова йде про, можливі порушення в процесах електронного збереження, передачі й обробки інформації. До них відносяться: перекручування, знищення, перехоплення даних або зловживання ними в результаті злочинних дій зловмисників.

Але, незважаючи на небезпеку проведення електроного банковського обслуговування клієнтів, фінансові інвститути прагнуть його впровадження у своїй діяльності. Це зумовлено значними перевагами, котрі має електронний банкінг перед традиційним – філіальним способом банківського сервісу. Насамперед необхідно підкреслити, що електронні банківські послуги, або

електронний банкінг, зовсім не екзотичний фінансовий інструмент і не додатковий напрямок банківської діяльності. Це новий спосіб здійснення банківських бізнесів-процесів, суть якого складається в проведенні транзакцій за допомогою електронних мереж. У зазначеному розумінні електронні банківські послуги є важливою частиною електронного бізнесу. Електронний банкінг містить у собі такі напрямки, як інформаційне обслуговування в режимі реального часу, емісія цифрових грошей, електронні платежі і розрахунки, а також депозитно-позикові, валютні і фондові операції, здійснені електронним способом.

З іншого боку, процес впровідження електронного банкінгу стимулюється посиленням конкуренціїї на фінансовому ринку з боку появі на ньому нових нетрадиційних учасників. В останній час до надання електронного фінансового сервісу, поряд із фінансово-кредитними установами, все більше вдаються інші господарські суб'єкти, різного напрямку діяльності та форми власності, підвищуючи тим самим конкурентний пресинг. Переділ нового ринку фінансових послуг наприкінці 20 - го і першого років 21 - го століття відрізнявся достатньою кількістю учасників, щоб звести зазначений вид банківського сервісу в розряд обов'язкових.

Поєднання переваг електронного банкінгу із значним конкурентним тиском у цій сфері діяльності вказує на те, що сучасний банк, незважаючи на підвищену небезпеку, повинен надавати своїм клієнтам повний набір віддалених фінансових послуг, інакше він ризикує позбавитися значної їхньої частини. Проблема підвищння рівня базпеки систем банківського обслуговування, побудованих на основі новітніх інформаційних технологій, являє собою обєкт досліджень даної науково дослідної роботи.

Метою цієї роботи є: на основі систематизації відомих способів шахрайства в інформаційному фінансовому середовищі та всебічного аналізу існуючих засобів та мірроприємств по запобіганню електронних

злочинів, сформулювати рекомендації по вдосконаленню систем безпеки фінансового обслуговування клієнтів сучаними банківсьними установами.

РОЗДІЛ І. ОСНОВНІ НАПРЯМКИ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ У СФЕРІ ЕЛЕКТРОННИХ БАНКІВСЬКИХ ПОСЛУГ.

1.1 Загальні характеристики зловмисних дій з використанням сучасних інформаційних технологій.

Послуги електронного банкінгу простираються від найпростіших інформаційних сервисів, типу отримання інформації про залишок на рахунку, до таких складних форм обслуговування, як одержання кредиту в режимі віддаленого доступу або розміщення заявок брокеру на фондовому або валютному ринку. Обслуговування різних сегментів ринку вимагає від банків використання різних технологій, пристроїв і каналів доступу. Канали доступу, тобто засоби комунікації, що використовує клієнт для керування рахунками, можуть бути самими різними — банкомат, телефон, мобільний телефон з підтримкою протоколу WAP або протоколу обміну короткими повідомленнями SMS, Інтернет, сервіс-центр (Call-центр), Personal Digital Assistant, електронна пошта, факс, спеціалізовані інтерфейси до сервіс-провайдерів типу Visa Interactive, Integrion. Фінансові організації, що надають своїм клієнтам повний набір сервісів електронного банківського обслуговування, тим самим стають телекомунікаційно-фінансовим центром, до якого по різних каналах надходять розпорядження клієнтів[3]. Саме такі телекомунікаційно-фінансовим центри стоють метою злочинних зазіхань. Треба зазначити, що разом із розвитком електронного банкінгу, та систем платежів через Інтернет, отримує свій розвиток інструментарій аферистів та інформаційних злочинців. Найчастіше в їхньому арсеналі присутні наступні злочинні дії:

• проникнення в систему через зовнішній (наприклад, телефонний) канал зв'язку з присвоєнням повноважень одного з легальних користувачів з метою

підробки, копіювання або знищення даних про платежі. Реалізується шляхом угадування або підбору паролів, виявлення паролів та протоколів через агентуру в банку, перехопленням паролів при теємному підключенні до каналу під час сеансу зв'язку, дистанційним перехопленням паролів у результаті прийому електромагнітного випромінювання;

• проникнення в систему через телефонну мережу при перекомутації каналу на модем зловмисника після входження легального користувача в зв'язок і пред'явлення їм своїх повноважень з метою присвоєння прав цього користувача на доступ до даних;

• копіювання фінансової інформації і паролів при таємному пасивному підключенні до кабелю локальної мережі або при прийомі електромагнітного випромінювання мережного адаптера;

• виявлення паролів легальних користувачів при таємному активному підключенні до комунікаційної мережі при імітації запиту мережної операційної системи;

• аналіз трафика при пасивному підключенні до каналу зв'язку або при перехопленні електромагнітного випромінювання апаратури для виявлення протоколів обміну;

• підключення до каналу зв'язку як активний ретранслятор для фальсифікації платіжних документів, зміни їхнього змісту, порядку проходження, повторної передачі, доставки з затримкою або попередженням;

• блокування каналу зв'язку власними повідомленнями, що викликає відмовлення в обслуговуванні легальних користувачів;

• відмовлення абонента від факту прийому (передачі) платіжних документів або формування помилкових зведень про час прийому (передачі) повідомлень для зняття із себе відповідальності за виконання цих операцій;

• формування помилкових тверджень про отримані (передані) платіжні документи;

• прихована несанкціонована передача конфіденційної інформації у складі легального повідомлення для виявлення паролів, ключів і протоколів доступу;

• незаконне оголошення користувачем себе іншим користувачем (маскування) для порушення адресації повідомлень або виникнення відмовлення в законному обслуговуванні;

• збір і аналіз використаних роздруківок, документації й інших матеріалів для копіювання інформації або виявлення паролів, ідентифікаторів, процедур доступу і ключів;

• візуальне перехоплення інформації, виведеної на екран дисплеїв або паролів, що вводиться з клавіатури для виявлення, ідентифікаторів і процедур доступу;

• таємна переробка устаткування або програмного забезпечення на фірмі-виготовлювачі, фірмі-постачальнику, у місці складування або в шляху проходження до замовника з метою впровадження засобів несанкціонованого доступу до інформації ззовні (програм-перехоплювачів і «троянських коней», апаратури висновку інформації і т.п.), а також знищення інформації або устаткування (наприклад, за допомогою програм-вірусів, ліквідаторів з дистанційним керуванням або уповільненою дією і т. п.);

• руйнування інформації або створення збоїв у комп'ютерній системі за допомогою вірусів для дезорганізації діяльності банку. Реалізується завантаженням вірусів у систему в неробочий час, підміною ігрових програм, використовуваних співробітниками банку в робочих приміщеннях, або врученням співробітникові банку «подарунка» у виді нової комп'ютерної гри або іншої цікавої програми;

• викрадення устаткування, у тому числі окремих плат, дисководів, дорогих мікросхем, кабелів, дисків, стрічок, з метою продажу, що спричиняє втрату працездатності системи, а іноді і знищення даних;

• викрадення магнітних носіїв з метою одержання доступу до даних і програм;

• руйнування устаткування, магнітних носіїв або дистанційне стирання інформації (наприклад, за допомогою магнітів);

• зчитування інформації з твердих і гнучких дисків (у тому числі і залишків «стертих» файлів), магнітних стрічок при копіюванні даних з устаткування на робочих місцях у неробочий час, при копіюванні даних з використанням терміналів, залишених без догляду в робочий час;

• копіювання даних з магнітних носіїв, залишених на столах або в комп'ютерах; копіювання даних з устаткування і магнітних носіїв, прибраних у спеціальні сховища, при їхньому розкритті або зломі;

• внесення змін у дані і програми для підробки і фальсифікації фінансових документів при включенні комп'ютерної системи під час таємного відвідування в неробочий час;

• використання залишеного без догляду устаткування в робочий час;

• внесення змін у дані, записані на залишених без догляду магнітних носіях;

• установка схованих передавачів для висновку паролів з метою копіювання даних або доступу до них по легальних каналах зв'язку з комп'ютерною системою в результаті таємного відвідування в неробочий час, відвідування з метою ремонту, настроювання, профілактики устаткування або налагодження програмного забезпечення, схованої підміни елементів устаткування при залишенні їх без догляду в робочий час;

• установка ліквідаторів уповільненої дії або з дистанційним керуванням (програмним, апаратним або апаратно-програмних з виконавчим механізмом вибухової, хімічної, електричної або вірусної дії) з метою знищення інформації або устаткування;

• несанкціонована зміна своїх повноважень на доступ або повноважень інших користувачів в обхід механізмів безпеки;

• внесення змін у базу даних або в окремі файли в межах виділених повноважень для підробки або знищення фінансової інформації.

1.2 Аналіз і класифікація способів злочинних посягань із використанням пластикових платіжних засобів.

На основі міжнародної практики протидії злочинним посяганням на платіжні системи визначено 12 основних способів скоєння злочинів, пов’язаних з пластиковими платіжними засобами:

1. Операції з підробленими картами.

2. Операції з украденими/загубленими картами.

3. Багаторазова оплата послуг і товарів.

4. Шахрайство з поштовими/телефонними замовленнями.

5. Багаторазове зняття з рахунку.

6. Злочинні посягання з використанням підроблених, а також украдених (загублених) документів.

7. Злочинні посягання з використанням підроблених сліпів.

8. Отримання авторизації від міжнародної платіжної системи за STIP (Stand In Processing) при збоях або відсутності зв'язку.

9. Створення і використання фіктивних підприємств обслуговування за пластиковими картами.

10. Шахрайське використання банкоматів при видачі готівки.

11. Підключення електронного записуючого пристрою, до POS-термінала/банкомата ("Skimming").

12. Інші види злочинних посягань.

Звертаємо увагу на те, що класифікація видів шахрайства, запропонована нами вище, сформульована за функціональними ознаками і відрізняється від стандартної статистичної класифікації.

Якщо ж ґрунтуватися на міжнародній класифікації шахрайства за видами правопорушень, то картина виходить така [2, с.72]:

1) шахрайство з втраченими і викраденими картками складає 72,2 %;

2) шахрайство з підробленими картками - 20,5 %;

3) шахрайство з картками, не отриманими законним держателем - 2,8 %;

4) шахрайство з використанням рахунку - 1,4 %;

5) інші форми шахрайства - 3,1 %.

Якщо проаналізувати співвідношення шахрайства за сервісними підприємствами [2, с.72], то з'ясовується, що найчастіше відбувається шахрайство через ресторани - 26,4 %, готелі (мотелі) - 25 %, магазини - 20,7 %, бари - 10,6 %, телефонні послуги - 7,4%, тобто підприємства комерційної мережі, які обслуговують пластикові картки.

Для зручності характеристики окремих способів злочинних посягань доцільно розглянути їх, виходячи з класифікації за суб'єктами, що була запропонована вище.

1. *Операції з підробленими картами*. На цей вид злочинних посягань припадає найбільша частка втрат платіжних систем. Як правило, для підробки використовують викрадені заготовки карт, на які наносяться реквізити банку і клієнта. Маючи високу технічну оснащеність, злочинці можуть навіть наносити інформацію на магнітну смугу карти або копіювати її, тобто виконувати підробки на високому рівні.

Виконавцями подібних акцій є, як правило, організовані злочинні угруповання, що іноді вступають у змову із співробітниками банків-емітентів, які мають доступ до інформації про рахунки клієнтів, процедури проведення транзакцій. Відзначимо, що підроблені карти в Україні з'явилися практично одночасно з початком розвитку цього сектора банківського ринку.

Механізм шахрайства може бути різноманітним: шахрай одержує в банку звичайну картку в законному порядку, вносить на спеціальний картковий рахунок мінімально необхідну суму. Після цього (або до цього) він добуває необхідну інформацію про держателя пластикової картки цієї ж компанії, але з більш солідним рахунком, і вносить отримані в такий спосіб нові дані у свою картку. Для реалізації такого способу шахрайства злочинець повинен добути інформацію про кодові номери, прізвища, ім‘я та по батькові власника картки, про зразок підпису і т.д.

Здійснити таку підробку можна по-різному:

а) змінивши інформацію, яка є на магнітному носії;

б) змінивши інформацію, ембосовану (витиснуту) на лицевій стороні;

в) проробивши і те, і інше;

г) підробивши підпис законного держателя картки. При підробці підпису використовується декілька варіантів, але при цьому враховується те, що стерти зразок підпису не можна, тому що при спробі це зробити у полі підпису проступить слово VOID – "недійсна". Тому її часто просто зафарбовують білою фарбою. Буває, що поле підпису взагалі змінюють на нове з використанням смужки клейкого паперу.

Нанести добуту інформацію про власника на магнітну смугу і раніше не було великою проблемою у технічному плані. Дані просто вводилися за принципом магнітофонного запису у відповідному форматі. Коли ж емітенти стали захищатися за допомогою кодування запису, народився скімінг – ретельне і повне копіювання усього вмісту магнітних треків (доріжок).

Голограми й емблеми, зроблені за технологією дифракційної решітки – не дуже ефективний захист, тому що під час рутинної процедури ідентифікації на них звичайно звертають менше уваги, ніж на підпис та інші персональні реквізити. Зміна ембосованої (витиснутої) на лицевій стороні інформації здійснюється різними шляхами.

Букви і цифри, ембосовані в площині картки, шахраї можуть зрізати і за допомогою клею заміняти на інші. Таким чином, на картці з'являються цілком нові номер і прізвище.

Як уже відзначалося, є багато шляхів одержання нових даних для внесення в картку (вони беруться з контрактів між фірмами, з рахунків, з листів копіювального паперу, їх отримують від службовців і т.д.). При цьому як інструменти звичайно використовують лезо, скальпель, збільшувач з лампочкою. Спосіб досить грубий, оскільки при уважному огляді пластикової карти під кутом до світла, звичайно можна помітити сліди клею і старого номера.

До того ж букви і цифри можуть бути наклеєні нерівно, що також можна помітити. Наявність інструментів, використовуваних при вчиненні даного способу шахрайства, варто мати на увазі при проведенні обшуку в осіб, підозрюваних у шахрайстві з пластиковими картками.

Іншим прийомом часткової підробки є "вигладжування" пластмаси. За рубежем такий спосіб називають "робота праскою", у нас – термопереробка. Він практикується з початку 80-х років і породжений здатністю матеріалу з якого виготовляються картки, ставати пружним під впливом тепла. Перед прогладжуванням фарба з опуклих букв зішкрібається. Для нагрівання використовують найрізноманітніші засоби: праску, свічку, гарячу воду, мікрохвильву піч і т.д.

Після розігріву картку вручну або за допомогою гідравлічного преса вирівнюють. Шахрай перед тепловою обробкою або пресуванням повинен видалити фарбу з опуклостей. Для цього він може скористатися звичайними чистячими засобами, які містять пемзу, і продаються в господарських магазинах. Якщо стара фарба видалена не повністю, то надалі буде видно контури справжнього шрифту. Для реалізації такого способу необхідно мати ще один прес – настільний, машина з набором букв і цифр. Деякі з них виготовлено таким чином, що нові цифри і букви можна витискати поверх старих.

Слід зазначити, що якщо картку піддали тепловій обробці, то швидше за все, на поверхні залишаться хвилеподібні сліди. Явною ознакою підробки також служить наявність вм'ятин на шрифті, зсув букв і цифр і т.п. Повністю підробленими є пластикові картки, у яких підроблено і пластмасу і друк.

Один із найбільш небезпечних прийомів підробки пластикових карток – виготовлення повністю фальшивих карток. Найбільше поширення метод повного копіювання отримав у деяких країнах Південно-Східної Азії. Такий спосіб найчастіше використовується організованими злочинними групами, до яких, як правило, входять працівники ресторанів і інших сервісних закладів. Останніх використовують для збору інформації про кредитні картки, що

потрапляють їм до рук при оплаті ресторанних та інших послуг, як це вже згадувалася вище, коли картка на якийсь час зникає з поля зору клієнта. А коли повертається, у злочинців на руках залишається її "брат-близнюк".

До цього ж методу відносять і спосіб "чистого пластика" (WPC). Підробка картки – дорога технологія, тому що ступенів зовнішнього захисту у справжніх карток (малюнки тонкими лініями, гільошированний прошарок, голограми, фотографії, ультрафіолетові картинки) з кожним роком стає усе більше. WPC – це використання шматка чистої пластмаси у формі звичайної картки, на який наносять справжні дані (номер реального рахунку, термін дії, прізвище і т.д.).

Далі картка використовується власником сервісної точки, що діє разом із злочинною групою. Власник магазина здійснює фіктивний оборот, відправляє емітенту картки рахунок для оплати, а прибуток ділить зі своїми співучасниками.

За допомогою "білих" карток, отримавши PIN-код, можна вчиняти крадіжки, знімаючи готівку через банкомати, які підпис не звіряють, фото й інші атрибути картки не перевіряють.

Кредитна інформація, яка використовується при виготовленні підроблених кредитних карток може збиратися в різноманітних країнах світу. Найчастіше використовуються дані з Канади, Сполучених Штатів Америки, країн Європи, а також з азіатського регіону. Злочинні групи, які працюють в різних регіонах обмінюються такою інформацією між собою.

2. *Операції з украденими/загубленими картами*. Злочинне використання украдених кредитних карток залишається найпоширенішим злочином. Методи протидії крадіжкам і злочинному використанню пластикових карток удосконалюються роками, проте в даний час компанії віддають перевагу випуску недорогих карток з метою зменшення суми можливих збитків від їхнього незаконного використання. Коли суми збитків різко зростають, компанії терміново вводять нові заходи безпеки.

Завдати значного збитку за вкраденою картою можна лише в тому випадку, якщо шахрай знає PIN-код клієнта. Тоді можна зняти значну суму з рахунку клієнта через мережу електронних касирів – банкоматів до того, як банк-емітент украденої карти встигне поставити її в електронний стоп-лист (список недійсних карт).

Для зазначеного способу характерно заволодіння пластиковим платіжним засобом шляхом викрадення його з квартири, в транспорті або в інших місцях, а також через втрату власником картки після її придбання в банку і підписання.

Картку викрадають в господаря звичайно разом із документами, гаманцем і іншими речами. Подія це частіше усього не залишається непоміченою. Одразу ж законний власник картки звертається в банк-емітент з проханням заблокувати рахунки, що дає можливість затримати злочинця або запобігти крадіжці коштів, якщо тільки викрадач картки не кинеться відразу робити покупки, не викликавши при цьому своєю поведінкою підозри з боку касира й ідеально підробивши підпис, або якщо викрадач не скористається нею в регіоні, не заявленому в "стоп-листі". Зазначимо, що мова йде про стандартні картки з магнітною смугою, а не про чіпові картки. Таким чином, злочинці використовують чужі картки, як правило, протягом того часу, поки "стоп-лист" ще не надійшов у сервісні точки, а крім того, користуються халатністю обслуговуючого персоналу, що не звіряє зі стоп-листами пред'явлені їм картки.

У випадку викрадення картки при пересилці її поштою, особливість злочинного посягання полягає в тому, що власник не знає про втрату картки, не здогадується, що картку в нього викрадено. Запобігти крадіжці при цьому способі шахрайства дуже складно. Такий спосіб у нас в Україні поки не має поширення. Справа в тому, що в США, наприклад, при зміні місця проживання, держатель кредитної картки може письмово звернутися до компанії-емітента із запитом на одержання копії картки за новою адресою.

Зловмисник підробляє повідомлення про переїзд власника банківського рахунку, і картку відсилають йому прямо в руки – поштою. Подальша доля викраденої таким способом картки може бути різною. Нею може скористатися сам викрадач, або він може перепродати її іншому зловмиснику. Це ще один із способів проникнення викрадених кредитних карток на територію країни.

Для викрадення пластикових карток можуть бути використані поштові скриньки в житлових будинках. Злочинці нерідко інформовані про час доставки нових кредитних карток. Йдучи за листоношею, злодій чекає, поки той опустить пошту до поштової скриньки і піде, після чого забирає її вміст. Слідчі називають цей тип крадіжки "повільним перехожим".

Через істотні втрати від поштових крадіжок багато організацій, що випускають картки, користуються для доставки рекомендованими листами. Як додатковий захід обережності може використовуватися попереднє повідомлення про майбутню доставку картки. Іноді разом із попереднім повідомленням використовується система, що одержала назву "подвійне датування". У цьому випадку картка починає діяти через місяць або більше після дати відправлення. У випадку неотримання картки, цього відрізка часу досить для повідомлення про пропажу і внесення картки в список попереджень. Деякі організації, що випускають картки, чекають від отримувача обов'язкового підтвердження того, що картку йому доставлено.

Якщо член злочинної групи має можливість проникнути в поштову організацію, то він отримує унікальні можливості для крадіжки карток, що пересилаються, які потім передає спільникам. Таким чином, удосконалювання засобів доставки кореспонденції разом з підвищеними заходами охорони пошти сприяють зменшенню крадіжок пластикових карток.

Шахраїв цікавить усе: зразки підпису, банківські рахунки, фотографії, листування. Зібравши за 2-3 місяця інформацію, що їх цікавить, злочинці вибирають банк, кредитної картки якого клієнт не має, і пишуть його

керівництву лист від імені наміченої жертви з проханням видати пластикову картку. Фінансисти, отримавши подібну заяву, після короткої перевірки (саме ім'я клієнта багато про що говорить) зі спокійною душею висилають кредитну картку на його адресу. Проте вона туди не доходить: ще на шляху її перехоплює шахрай, що осів на пошті спеціально з цією метою. Тепер залишається підробити підпис жертви на кредитній картці й інтенсивно почати її використовувати.

В усьому світі використання картки, виданої на чуже ім'я, жорстко переслідується законом. Проте в неприємні історії, пов'язані з пластиковими картками, часто потрапляють солідні люди через елементарну безграмотність, яку уміло використовують шахраї [5, с.5]. Наприклад, іноземець, що приїхав в Україну, робить борги, а коли приходить час розплачуватися за рахунками, повідомляє своєму кредитору про необхідність від'їзду додому. Через відсутність готівки надходить пропозиція кредитору як компенсацію прийняти пластикову картку боржника. При цьому повідомляється, що на спеціальному картковому рахунку боржника є не менше 10 тисяч доларів. Кредитор-підприємець йде в банк з проханням обслужити його, пред'явивши пластикову картку боржника, у чому йому справедливо відмовляють. Більше того, "подаровану" картку працівники банку вилучають. І лише тоді кредитору стає зрозумілим, що напередодні закордонний боржник уже заявив у банк-емітент, який видав картку, про її втрату.

Компанії, що випускають картки, звичайно мають цілодобово працюючу службу для повідомлень про втрату карток. При одержанні повідомлення рахунок клієнта блокується і всяке подальше використання його картки тягне за собою проведення розслідування. Іноді незвичайна кількість транзакцій може викликати спрацювання комп'ютерної системи сигналізації ще до того, як буде відомо про крадіжку картки. Проведені нами дослідження показують, що повідомлення про втрату картки можуть надходити в компанію навіть через 3-4 дні після її зникнення, а у випадку

використання підробленої картки, шахрайство може виявитися навіть через 30-40 днів.

Компанії регулярно видають бюлетені з переліком номерів карток, що підлягають вилученню; розсилають продавцям так звані списки попереджень. У деяких торгових закладах стоїть спеціальна апаратура (point of sale) – комп'ютерні термінали, що дозволяють перевірити стан рахунку клієнта перед тим, як операцію буде здійснено. Проте можливість вчинення аналізованого способу шахрайства пов'язана з тим, що правоохоронні органи і торгові підприємства технічно поки ще дуже слабко оснащені, і немає єдиної картотеки викрадених кредитних карток, а також не завжди своєчасно надходять у торгові організації стоп-листи.

Злочинці проявляють велику винахідливість і зухвалість у спробах використовувати систему розрахунків кредитними картками у своїх особистих цілях. Проте крадіжка її в законного власника залишається найпоширенішим способом заволодіння карткою. Щомісяця з незаконного обороту тільки в Росії вилучається близько 200 пластикових карток [9].

Найважчий випадок для розслідування – наявність змови в продавців між собою або між продавцем і покупцем. Наприклад, два продавці можуть співробітничати, обмінюючись загубленими або вкраденими картками для проведення фіктивних транзакцій. Продавець може також оформити продаж речі шахраю, яка насправді залишається в нього, а сума, оплачена фінансовою установою ділиться між ними за домовленістю. Касиру звичайно пропонують 10-20 % від кожної операції, причому готівкою.

Іноді касири вступають у злочинну змову із шахраями через уявну безкарність. Адже єдиний фінансовий документ, що підтверджує операцію з пластиковою кредитною карткою – сліп, на якому після звичайного прокочування і залишаються реквізити пластикової картки.

Проте визначити "на око", зчитані вони були зі справжньої пластикової картки або ж просто із шматка пластика з набитими даними, практично неможливо. Цим і користуються шахраї.

Є ще один різновид шахрайства, що потребує наявності непорядного продавця, або іншої особи, що має номер телефону для проведення перевірки картки. Дзвінок дозволяє з'ясувати, чи є картка в списку викрадених. Якщо її там немає, несумлінний продавець може провести фіктивну оборудку на значну суму через свій заклад. Якщо картка значиться як викрадена, він може здійснити декілька транзакцій, які не виходять за межі встановленого для нього ліміту.

3. *Багаторазова оплата послуг і товарів* на суми, що не перевищують "floor limit" і не потребують проведення авторизації. Для проведення розрахунків злочинцю необхідно лише підробити підпис клієнта. Проте при даній схемі стає недоступним самий привабливий об'єкт зловживань – готівка. До цієї категорії можна віднести злочини з картами, викраденими під час їхньої пересилки банком-емітентом своїм клієнтам поштою.

Поширені за кордоном також крадіжки шляхом шахрайства за кредитними картками банків, що встановили значний ліміт граничної суми операції, здійснюваної без авторизації. Шахраї використовують граничний ліміт суми неодноразово протягом одного дня в різноманітних сервісних і торгових точках. Так, наприклад, деякі солідні лондонські банки встановлюють граничний ліміт у 200 фунтів і кількаразове використання такої суми принесе шахраю значну суму.

Для того, щоб визначити невикористану частину кредиту на картці, злочинці використовують простий метод. Вони телефонують у реєстраційний центр компанії і просять дозволити транзакцію, наприклад, на 3000 доларів США. У випадку відмови вони зменшують суму до тих пір, поки не дістануть згоду. Через якийсь час вони дзвонять знову і просять скасувати транзакцію. Завдяки цьому в них на даній картці утворюється сума, вже заздалегідь дозволена до виплати. Одержати номера справжніх карток нескладно. Для цього використовують дані, отримані від персоналу готелів, ресторанів, за допомогою необережно викинутих рахунків, агентств з прокату автомобілів і т.д.

Різновидом даного способу вчинення шахрайства з пластиковими картками може стати використання картки із злочинною метою самим держателем, який, провівши великі операції за карткою (найчастіше банкоматом), може заявити, що картка було викрадено. У таких випадках можуть використовуватися і спільники, щоб уникнути можливості бути впізнаними.

4. *Шахрайство з поштовими/телефонними замовленнями*. Цей вид злочинів з'явився в зв'язку з розвитком сервісу доставки товарів і послуг за поштовим або телефонним замовленням клієнта. Знаючи номер кредитної карти своєї жертви, злочинець може вказати її в бланку замовлення і, отримавши замовлення за адресою тимчасового місця проживання, зникнути. За допомогою подібного способу звичайно добувають дорогі предмети, такі як комп'ютерне обладнання, електронне обладнання і т.п. Цей вид шахрайства в області телемаркетингу звичайно називається "inbound". Номери карток можна дізнатися в персоналу магазинів і ресторанів, з комп'ютерних бюлетенів і т.д.

Шахрайське використання номерів кредитних карток включає широкий набір способів, таких як шахрайство за допомогою системи телемаркетинга і телекомунікації. Оскільки для того, щоб зробити замовлення поштою або по телефону, не потрібно пред'являти картку, а потрібно лише повідомити її номер, число варіантів способів шахрайства є нескінченним і все зростає. Зловживання в області телемаркетинга відносяться до неавторизованих операцій, здійснених телемаркетерами-шахраями, а також злочинцями, що мають справу з справжніми телемаркетерами і підприємствами, які приймають замовлення поштою.

У вчиненні шахрайств в області телемаркетинга типу "outbound" беруть участь шахраї-телемаркетери. Ці злочинці різними способами дізнаються про справжні номери карток і використовують їх при виписуванні шахрайських рахунків за замовлення, оплата за якими зараховується на банківський рахунок телемаркетера щодня. Оскільки більшість банків установили для

рахунків за замовлення такий же режим, як і для готівки, телемаркетер має можливість негайно переводити ці кошти на інший рахунок або просто щодня знімати гроші з рахунку. Коли злочин розкрито, телемаркетер-шахрай звичайно зникає разом із грошима.

Новим різновидом такого виду шахрайства є використання комп'ютерної мережі Internet для електронної системи замовлень на різноманітні товари. Але вже сьогодні нараховується близько 30 видів незаконних операцій із пластиковими картами через Internet:

- оплата неіснуючими картками;
- створення фальшивих віртуальних магазинів;
- "електронні" крадіжки;
- фальшиві оплати в ігорних закладах і т.д. [10, с.67].

5. *Багаторазове зняття з рахунку*. Ці злочини, як правило, вчиняються працівниками торгових і сервісних точок, що приймають платежі від клієнтів за товари і послуги за кредитними картами, і здійснюються шляхом оформлення кількох платіжних чеків за одним фактом оплати. На підставі пред'явлених чеків на рахунок підприємства надходить більше грошей, ніж коштує проданий товар або зроблена послуга. Проте після проведення ряду операцій злочинець змушений закрити або залишити підприємство.

Зазначений спосіб характеризується участю в шахрайських діях обслуговуючого персоналу таких сервісних точок як ресторани, кафе, бари, мотелі і т.ін. Працівники таких підприємств, користуючись неуважністю клієнта, або зумисне відволікаючи його, роблять кілька додаткових відтисків пластикових карток (сліпов), які потім використовують для присвоєння матеріальних цінностей і грошей.

Ключовим моментом у цьому способі є те, що, на відміну від магазину, де при розрахунку дії з карткою відбуваються на очах у власника, у ресторані офіціанти відносять її на якийсь час, а потім повертають разом із рахунком. При цьому держатель картки не здогадується, що пред'явлений йому рахунок або разом з ним сліп (відтиск із картки) – тільки один із декількох, зроблених

спритним касиром або офіціантом. Від інших відтисків його відрізняє лише присутність дати. Протягом наступних декількох днів готівку, отриману з інших клієнтів, касир, поділившись з офіціантом, може привласнювати, а рахунки з реквізитами держателя картки благополучно прилучати до звітності і направляти для оплати фірмі-емітенту (банку або платіжній системі). При цьому керівництво закладу може не знати про шахрайство. Для запобігання подібних дій користувачам карти рекомендується уважніше ставитися до документів, які підписуються при здійсненні угод навіть на незначні суми.

6. *Шахрайство з використанням підроблених документів, а також украдених (загублених) документів законних власників*. Характерним у даному способі є те, що особа, отримавши незаконним шляхом кредитну картку, що належить, наприклад, іноземному громадянину, видає себе за цього іноземця – держателя кредитної картки, пред'являючи при цьому підроблений паспорт або інший документ на ім'я власника кредитної карти.

Документи можуть бути підроблені цілком або частково. У цьому випадку шахрай тренується в підробці підпису, після чого в підприємствах по торгівлі на валюту купує той чи інший товар, за який розплачується наявною в нього кредитною карткою і розписується за держателя кредитної картки в рахунках, або використовує картку в інших сервісних точках.

Різновидом зазначеного способу шахрайства є операції з картками, виданими на чужі імена. Наприклад, в банк звернувся громадянин із законним проханням – видати йому міжнародну картку Visa. При цьому відкрив у банку рахунок і поклав на нього 1000 доларів США. Зрозуміло, пред'явив при цьому паспорт, але украдений, в котрий акуратно було вклеєно листок з фотографією шахрая. Отримавши пластикову картку, він відразу ж вилетів у Європу, де усього за тиждень привласнив за нею 50000 доларів США, здійснюючи операції на долімітні суми – по 100-200 доларів. Рахунок у результаті прийшов на ім'я справжнього власника паспорта, який відразу відмовився від нібито зроблених ним покупок [12].

Використання вигаданих даних (несправжнього імені, зміненої адреси) при одержанні пластикової картки – дуже поширений спосіб незаконного одержання кредитної картки.

Справжній власник картки і продавець звичайно не несуть відповідальності у випадку шахрайських дій; збиток, як правило, лягає на компанію, що випускає картки, або може бути розділений відповідно до домовленості між фінансовими установами, що випустили і реалізували картку згідно з існуючими між ними угодами.

7. *Шахрайство з використанням підроблених сліпів*. Даний спосіб отримав значне поширення при співучасті касирів магазинів. Суть цього способу зводиться до використання явно підроблених сліпів, виготовлених шляхом застосування підроблених кліше, або за допомогою набірних друкарських форм, з використанням даних із справжніх пластикових карток. У цьому випадку картка частіше всього використовується без відома її законного держателя, який після виявлення факту шахрайства не визнає зафіксованих витрат.

Касир одержує від співучасників злочину заздалегідь виготовлений сліп, прокочений в одну сторону (тобто такий, що має дані про номер картки, ім‘я її держателя і термін дії) і дооформляє цей сліп, прокочуючи його в іншу сторону, тобто проставляються дані про сервісну точку, через яку сліп оформляється. Після того як у касу надійшла оплата за якийсь товар готівкою, у підробленому сліпі вказується як оплата та сума, що була отримана готівкою. Сліп прилучається до звіту, гроші вилучаються і присвоюються шахраями.

8. *Одержання авторизації від міжнародної платіжної системи за STIP (Stand In Processing) при збоях або відсутності зв'язку*. Суть вказаного способу шахрайства полягає в навмисному виведенні з ладу системи зв'язку між торговою точкою й авторизаційним центром з тим, щоб в момент проведення операції неможливо було провести авторизацію.

9. *Створення і використання фіктивних підприємств обслуговування за пластиковими картами*. Цей спосіб шахрайства є дуже поширеним і може завдати великої економічної шкоди учасникам платіжної системи. На жаль, подібних фактів шахрайства на основі використання пластикової платіжної системи в Україні надзвичайно багато, про що докладно написано в ряді спеціальних видань [3,7,8].

10. *Шахрайське використання банкоматів при видачі готівки.* Розглянемо використання карток при одержанні готівки з автоматичних касових машин (ATMs - Automated Teller Machines).

Тільки в Канаді в експлуатації знаходиться більш 2000 банкоматів і їх кількість усе збільшується. Деякі фінансові установи випускають спеціальні картки для користування автоматичними касовими машинами, у той час як деякі види цих машин можуть використовувати закодовані банківські картки типу Visa і MasterCard. У будь-якому випадку картка використовується разом із персональним ідентифікаційним номером (PIN-кодом) для доступу до АТМ.

PIN-код відомий тільки власнику картки, якому рекомендується запам'ятовувати свій номер, і ні в якому разі не записувати його на картці. Інакше при крадіжці картки в руки злочинця потрапляє також і особистий код, що значно полегшує вчинення злочину.

Головною вигодою від впровадження автоматичних касових апаратів є їхня велика надійність і продуктивність у порівнянні з живим касиром, що робить їх більш зручними і безпечними для широкого надання послуг населенню. Незважаючи на це, злочинці успішно нападають на автоматичні касові машини, застосовуючи як чисто силові методи (крадіжка зі зломом, повне руйнування і т.д.), так і шахрайські дії. У більшості випадків використовується справжня картка і справжній персональний код, отримані злочинцями в результаті крадіжки в законного власника, або оманним шляхом від фінансової установи. Відомі випадки, коли шахраї дзвонять особі, що загубила картку, і відрекомендовуються інспектором банку. Нібито

з метою перевірки реєстрації картки, вони просять повідомити їм персональний ідентифікаційний номер, після чого рахунок стає доступним для крадіжки за допомогою касових автоматів. Досить часто при цьому способі реалізуються прийоми вчинення шахрайства, пов'язані з використанням банківських службовців із метою одержання від них інформації про грошові внески, про держателів пластикових карток із великими внесками за хабар.

Відповідальність законного власника картки за збиток, нанесений у випадку неправомірного використання його картки й особистого коду, не обмежена, але звичайно не перевищує 50 доларів США. Фінансові компанії звичайно підкреслюють ту обставину, що їхні клієнти несуть певну відповідальність за цілість персонального ідентифікаційного номера.

Донедавна одержання грошей через банкомат було одним із найбільше надійних і безпечних способів використання пластикових карток, оскільки наявність PIN-коду, відомого тільки користувачу, гарантує ідентифікацію власника картки і конфіденційність доступу клієнта до рахунку. Проте міжнародна практика вже зафіксувала крупні шахрайства через банкомати. Так, в Угорщині злочинці через банкомати, розташовані в різних районах Будапешта, протягом декількох хвилин, використовуючи близько 1,5 тисяч підроблених карток, зняли з рахунків приблизно 1,5 млн. форинтів. За даними Інтерполу, в операції брали участь до 150 чоловік [9]. У Англії мав місце факт використання шахраями фальшивого банкомата, що зовні був оформлений так, ніби належав одній з відомих фірм. При обслуговуванні фальшивий банкомат видавав правильне повідомлення, тому не викликав у держателів карток сумнівів у його істинності. Користувачі банкоматом залишали всі дані про свій рахунок. Потім шахраї, використовуючи отриману інформацію, виготовляли фальшиві картки з білого пластика, наносили справжню інформацію, кодували магнітну смугу, а потім одержували готівку з чужих рахунків через справжні банкомати.

11. *Підключення електронного записуючого пристрою, до POS-термінала/*банкомата ("Skimming"). Цей вид шахрайства, з'явився недавно. Даний вид шахрайства характеризується повним копіюванням усього вмісту магнітної смуги пластикової картки.

Мабуть, основним чинником для зменшення збитків залишається обмеження на грошову суму (кілька сотень доларів), яка може бути видана з одного автомата протягом дня.

Іншим заходом запобігання крадіжки є спеціальні комп'ютерні програми, що управляють автоматичною касою. Вся інформація, якою автоматична касова машина обмінюється з центральним комп'ютером, шифрується, щоб запобігти можливості підключення і перехоплення інформації [4, с. 25-26]. Підозріло часта видача грошей протягом короткого періоду часу або неправильно вказаний персональний номер можуть призвести до "проковтування" картки автоматом.

12. *Інші види шахрайства*. До інших видів шахрайства, на наш погляд, можна віднести різноманітні комбінації розглянутих нами вище способів шахрайства або види шахрайства, які щойно з‘явилися і ще не вивчені.

РОЗДІЛ ІІ. СУЧАСНІ МЕТОДИ ЗАПОБІГАННЯ СПРОБАМ ШАХРАЙСТВА ПРИ ЗДІЙСНЕННІ ЕЛЕКТРОННИХ ФІНАНСОВИХ ОПЕРАЦІЙ .

2.1 Загальні принципи організації безпеки систем електроного обслуговування клієнтів банкавських установ.

З метою систаматизації та вдосконалення існуючих методів протидії інфрмаційним злочинам у банківській сфері, розглянемо досвід передових банків США та країн Євросоюзу і їх придатність до застосуванні на вітчизняному фінансовому ринку. Федеральна Резервна система США, Федеральний резервний банк Нью-Йорка та відділ контролю Казначейства США у вересні 2000 року, випустили спільний прес-реліз, який містить основні поради інвесторам та користувачам Інтернет, що регулярно користуються послугами переведення коштів через Інтернет. Це була перша спроба розробити комплекс заходів по підвищенню безпеки по розрахункам через Інтернет. Наведемо кілька змістовних порад, які допоможуть вітчизняним користувачам уникнути проблем із з'ясування стосунків із закордонними Інтернет-брокерами та компаніями, що ведуть торгівлю через Інтернет[8].

По-перше, потрібно перевірити, чи справді існує фізично Он-лайн банк або компанія, яка пропонує свої послуги. Обов'язково сайти таких установ повинні містити розділи, які надають інформацію про місце знаходження офісу компанії, чи адресу. Особливу підозру у Вас повинні викликати посилання на абонентські скриньки. За повідомленням FATF, близько 60% злочинів у Інтернет відбувається саме таким чином, коли нікому невідома компанія відкриває сайт, розпочинає рекламну компанію, отримує номери кредитних карт, чеки, поштові грошові перекази, а потім через тиждень зникає. Схема стандартна, як правило, сама компанія, якщо вона насправді існує, має сумнівні Панамські чи Тюркські коріння. Знайти потім, де насправді опинились Ваші гроші неможливо, оскільки із рахунку у солідному банку, гроші потрапляють у банки Східної Європи, Панами, Африки, Півден ної Америки, а вже потім на кодовані анонімні ра-

хунки фізичних осіб. Парадокс, але такі можливості для злочинців відкриває саме Інтернет-банкінг, який дозволяє миттєво провести трансферт не тільки зручно, але і майже анонімно. В Україні, на перший погляд таких проблем виникати не повинно, особливо із банками, які жорстко контролюються НБУ, один запит в який може розвіяти фіктивні банки в Інтернеті. Але все це тільки на перший погляд. Об'єктом аферизму можуть стати і українські підприємці та громадяни. Сутність операції, може стати тією ж, що і в США, але, звісно, передмова буде іншою. Вже найближчим часом можна передрікати проблеми у цій галузі банківської справи в Україні. Не дивно, якщо у мережі з'являться сайти-фантоми добре відомих банків, які насправді не будуть мати ніякого відношення до банку, а скоріше будуть створені на кілька тижнів із великою рекламною компанією у мережі та із номерами рахунків померлих фізичних осіб, чи компаній з оффшорних зон.

Чи готові вітчизняні банки до появи таких фантомів? Звісно ж, тільки ті, що мають вже власну сторінку у Інтернет. Розрізнити сайт двійник можливо за кількома ознаками:

• по номеру рахунку, на який пропонується здійснити трансакцію. В Україні рахунок фізичної особи, як правило, розпочинається із 2620. Цікаво, що при пропозиції двійника вести розрахунки за допомогою пластикової картки просто не можливо буде відстежити, кому переведені кошти з Вашого рахун ку;

• підозріло низькі ціни та добрі умови обслуговування. Здебільшого комп'ютерні пірати є люди без економічної освіти, тому на сайтах такого типу можна зустріти парадоксальні речі, наприклад маржа між кредитними та депозитними ставками на стільки низька, що "банк" виходить на від'ємне сальдо після врахування обов'язкових резервів.

Звісно ж, потрібно бути дуже уважними, наприклад, при наборі назви сайту справжнього он-лайн банку у віконці браузера. У США вже були випадки, коли кілька років разом із сайтом банку паралельно функціонували сайти фантоми за адресами, які відрізнялись від банку тільки однією буквою у назві. Ідея створення таких сайтів злочинцями проста, всі, хто невірно друкує назву сайту банку у

віконці Інтер-нет-браузеру потрапляли на сайт фантом, там вводили пароль та номер рахунку, після чого власноруч відправляли їм все це по електронній пошті. Звісно ж, з рахунку таких неуважних клієнтів зникали кошти, а оскільки таких клієнтів було небагато, служба банківської безпеки не приділяла значної уваги розслідуванням.

По-друге, періодично виникають проблеми у клієнта із самими банками, які відносяться безвідповідально до власної безпеки, а потів тягар перекладають на клієнта. Як правило, при використанні для розрахунків у Інтернет пластикових карт банк пропонує підписати клієнту договір, за яким банк відмовляється від відповідальності за несанкціоноване зняття грошей із клієнтського рахунку. Такі умови приховуються за іншими пунктами і більшість клієнтів бачить вказаний пункт тільки після підписання, а частіше - після випадку шахрайства. Звісно ж, банк нездатен захистити клієнта від шахраїв на сто відсотків, і саме це зменшує перспективи подальшого розвитку електронного банкінгу, але аналіз ситуацій, пов'язаних із шахрайськими випадками за кордоном, свідчить, що найбільші в історії шахрайства стались з вини банківської безпеки, яка залишила можливість шахраям скористатись недосконалістю системи інформаційної безпеки.

Базельський комітет з банківського нагляду при Банку міжнародних розрахунків сформулював 14 принципів керування ризиками в сфері електронних банківських послуг. Звід цих правил не є обов'язковою для виконання директивою, однак де-факто всі солідні банки в розвитих країнах дотримують дані вимоги[3].

Принципи керування ризиками ДБО згруповані в три великі категорії.

Перша категорія – це нагляд з боку вищого керівництва банку , до неї відносячи принципи з першого по третій. Перш ніж банк почне надавати клієнтам електронні послуги, рада директорів і правління повинні прийняти чітко сформульоване стратегічне рішення по цьому питанню. Варто погодити плани розвитку даного напрямку з загалькорпоративними стратегічними задачами, провести аналіз ризиків і розробити заходи щодо їх

моніторингу і зниження, а також розробити принципи безперервної оцінки ефективності веб-сервісу.

Принцип перший - створення ефективної системи спостереження за операціями, що здійснюються електронним способом. Нові проекти в сфері електронного банкінгу, які можуть вплинути на конфігурацію банківського ризику і реалізацію прийнятої стратегії, повинні розглядатися на засіданнях ради директорів і правління і піддаватися глибокому стратегічному аналізові і детальній оцінці з погляду співвідношення очікуваних витрат і результатів. Після завершення проектів варто проводити їхній ретроспективний аналіз. Керівництво банку не має права приступати до електронного обслуговування клієнтів, не забезпечивши необхідного рівня кваліфікації менеджерів і персоналу в сфері нових технологій, у тому числі й у тих випадках, коли для проведення тих або інших операцій залучаються сторонні організації. Управлінський нагляд повинний бути максимально динамічним і здатним негайно й ефективно реагувати на будь-які проблеми. Для цього необхідно створити систему оповіщення керівних органів про виникнення інцидентів у розглянутій області. Рада директорів і правління зобов'язані домогтися інтеграції процесу керування ризиками в сфері онлайнових послуг у загальний механізм керування банківськими ризиками. Комплекс питань, зв'язаних з електронним виходом за кордон, вимагає особливої уваги керівництва.

Принцип другий - впровадження всебічної процедури контролю над підтримкою необхідного рівня інформаційно - технологічної безпеки. Збереження банківських активів — один з найважливіших обов'язків, покладених на директорів і топ-менеджерів. Для виконання цієї задачі потрібно зосередити зусилля на наступних ключових напрямках. Призначити конкретних осіб (інших, ніж аудитори), що несуть відповідальність за стан справ у даній області. Сформулювати тверді правила, що дозволяють стежити за спробами вторгнення в комунікаційні мережі і запобігати несанкціонованому доступу (як фізичному, так і в рамках реєстрації входу)

до комп'ютерної техніки, програмному забезпеченню для веб-транзакцій і базам даних. Регулярно переглядати заходи для забезпечення безпеки з метою впровадження новітніх технологічних досягнень і своєчасної модернізації використовуваних програм.

Принцип третій - організація режиму ретельного спостереження за взаємодією з партнерами, які залучені до надання окремих видів електронних банківських послуг. Керівним органам банку варто здійснювати постійну оцінку і переоцінку рівня співробітництва зі спеціалізованими сервіс-провайдерами. При цьому члени ради директорів і правління повинні чітко усвідомлювати пов'язані з аутсорсингом ризики; в обов'язковому порядку проводити попередній аналіз ступеня професіоналізму і фінансового становища передбачуваних контрагентів; точно формулювати межі відповідальності обох сторін при підписанню контрактів (особливо по порядку надання інформації); установити практику проведення періодичних аудиторських перевірок у відношенні переданих на сторону систем і операцій та включити їх у діючу систему керування ризиками; розробити план заходів на випадок виникнення надзвичайних ситуацій у притягнутих до надання електронного сервісу партнерів.

Друга категорія включає принципи, що спрямовані на забезпечення безпеки в сфері інформаційних технологій. Якщо вище керівництво банку визначає загальну політику в області інформаційно-технологічної безпеки, то безпосередньою побудовою відповідних систем займаються фахівці середньої ланки, чия увага зосереджена на реалізації наступних принципів.

Принцип четвертий - аутентифікація клієнтів, що користуються електронними каналами обслуговування. Аутентифікація означає ідентифікацію клієнта (установлення дійсності особи, що робить онлайнову транзакцію) у сполученні з авторизацією (установлення легітимності доступу даної особи до банківського рахунку або наявності в нього права на проведення операцій по рахунку). Вона здійснюється за допомогою персональних ідентифікаційних номерів (ПІНів), паролів, смарт-карточок,

біометрики (сканування лиця та райдужної оболонки ока, відбитків пальців, аналізу голосових даних і т.п.) і сертифікатів цифрового підпису на базі інфраструктури відкритого ключа. Багатофакторна аутентифікація (з використанням декількох методів) забезпечує більш високий рівень захисту, що особливо важливо при поширенні електронних банківських послуг на іноземних клієнтів. Аутентифікаційні бази даних необхідно захищати від підробок, замін і розкрадань, а спроби подібних дій — обов'язково документувати. Будь-які зміни в цих базах варто робити винятково з санкції відповідного джерела. Підключення до систем ДБО повинне ретельно контролюватися (щоб запобігти заміщення клієнтів, що пройшли аутентифікацію третіми особами), а у випадку зриву веб-сеансу потрібно проводити повторну аутентифікацію.

Принцип п'ятий - недопущення відмовлення від зобов'язань по онлайновим транзакціям і сувора відповідальність за їхнє проведення. В даний час найбільш надійним способом уникнути несумлінного сторнування електронних угод є використання сертифікатів цифрового підпису на базі інфраструктури відкритого ключа, у рамках якої кожен контрагент має свою пару ключів (шифрів). За допомогою секретного ключа генерується цифровий підпис і зашифровується текст, а за допомогою відкритого ключа (парного до секретного) здійснюється розшифровка і перевірка дійсності документа. Банк може сам стати центром, що засвідчує випуск сертифікатів або удатися до послуг незалежних центрів (в останньому випадку необхідно вибирати такі установи, що забезпечують однаковий рівень аутентифікації, що і банк).

Принцип шостий - розмежування функцій, що виконуються банківськими службовцями при роботі в системах ДБО, з базами даних і додатками. Не можна надавати одній особі або сервіс-партнерові права на ініціювання, авторизацію і завершення транзакції. Різні співробітники повинні займатися підготовкою інформації (наприклад, змісту веб-сайту) і перевіркою її цілісності, а також розробкою й адмініструванням систем

електронного сервісу, причому варто забезпечити неможливість обійти принцип розмежування функцій у цих системах.

Принцип сьомий - ефективний контроль за процедурами авторизації і одержання доступу в системи ДБО, бази даних і прикладні програми. Головне в організації такого контролю — гарантувати збереження баз даних, у яких зберігається інформація про права на авторизацію і доступ до проведення тих або інших операцій. Для цього використовуються ті ж методи, що і при захисті аутентифікаційних баз даних.

Принцип восьмий - забезпечення цілісності даних по операціям і записам у сфері онлайнових послуг. Усі здійснювані в рамках банківського Інтернет-сервісу процеси повинні бути налаштовані таким чином, щоб досягти підвищену стійкість транзакцій і записів до розкрадань та перекручувань і була практично повна гарантія того, що будь-які несанкціоновані зміни не залишаться непоміченими. Цілісність даних необхідно контролювати особливо ретельно в періоди модернізації використовуваних у банку комп'ютерних систем і програм.

Принцип дев'ятий - точний облік транзакцій, що відбуваються електронним способом. Критично важливим представляється облік у наступних областях: відкриття, зміна і закриття клієнтського рахунка; проведення операції, що відбивається на стані банківського балансу; дозвіл перевищити раніше обговорений із клієнтом ліміт; надання, модифікація або анулювання права на доступ у систему ДБО.

Принцип десятий - збереження конфіденційності ключової банківської інформації. Усі конфіденційні дані і записи повинні бути захищені під час передачі по відкритих, закритих і банківських телекомунікаційних мережах і доступні тільки особам, агентам і системам, що мають відповідні повноваження і пройшло процедуру аутентифікації. Використовувані банком стандарти по забезпеченню конфіденційності варто поширити і на сторонні організації, залучені до надання електронних послуг. Усі випадки

доступу до такого роду даних необхідно реєструвати, а реєстраційним файлам потрібно додати підвищену стійкість до розкрадань і замін.

До третьої категорії відносяться принципи керування правовим і репутаційним ризиком.

Принцип одинадцятий - розкриття необхідної інформації щодо використання електронного банківського сервісу на веб-сайті банку. На веб-сайті банку потрібно вказати наступну інформацію: назва банку і місцезнаходження його штаб-квартири і філій; назва наглядового органа, що контролює діяльність головного офісу; контактна інформація щодо банківського центра по обслуговуванню клієнтів; порядок подачі скарг; порядок одержання інформації про страхування депозитів; інші необхідні данні (наприклад, перелік країн, у яких надається електронний сервіс).

Принцип дванадцятий - запобігання несанкціонованого доступу до клієнтської інформації. Стандарти використання інформації про клієнтів, що накопичується банком у процесі надання онлайнових послуг, повинні відповідати всім вимогам законодавства тих держав, на які поширюється веб-обслуговування. Сервіс-провайдерам, з якими співпрацює банк, також варто дотримувати цих стандартів. Банк зобов'язаний дати своїм вкладникам і позичальникам право заборонити передачу інформацію про себе третім особам, що бажають використовувати їх в маркетингових цілях.

Принцип тринадцятий - підтримка систем ДБО в постійній експлуатаційній готовності. Потрібно забезпечити необхідні потужності для електронного сервісу і його безперервне функціонування, а також розробити комплекс мір на випадок виникнення надзвичайного стану. На критично важливих напрямках розвитку онлайнових послуг повинні проводитися постійні оцінки і переоцінки наявних потужностей і розроблятися прогнози їхньої динаміки в майбутньому. Системи варто періодично випробувати на стійкість до стресових ситуацій.

Принцип чотирнадцятий - створення ефективного механізму реагування на несподівані інциденти у формі зовнішніх і внутрішніх атак на системи

ДБО. Для залагоджування тих або інших подій у банку повинні бути розроблені плани дій у наступних областях. Негайне виявлення кризової ситуації і визначення розмірів погрози. Відновлення електронних систем (у тому числі і тих, що передано зовнішнім виконавцям) відповідно до різних сценаріїв розвитку подій (включаючи оцінку імовірності різних варіантів). Взаємодія з учасниками ринку і засобами масової інформації. Повідомлення керівництва банку і державних регулювальних органів. Формування команд фахівців з особливими повноваженнями і порядку підпорядкованості співробітників, задіяних у ліквідаціях проблем. Своєчасне постачання всіх зацікавлених сторін необхідними зведеннями в продовження всього інциденту. Збір і збереження даних для аналізу кризи після його завершення і покарання винних.

Таким чином, основна увага в документі Базельського комітету з банківського нагляду приділяється забезпеченню інформаційно-технологічної безпеки електронних послуг. Фахівці з цих питань стають визнаними членами елітарного клубу в службовій ієрархії і нарівні з вищим фінансовим керівництвом беруть участь у формуванні банківської стратегії. У деяких країнах наглядові органи вважають потрібним перевести правила інформаційного захисту з розряду рекомендаційних у розряд обов'язкових.

2.2 Механізм попередження злочинів з використанням пластикових платіжних засобів.

Розрахунки із застосуванням пластикових платіжних засобів лишають "паперовий слід" (див. Табл. 1) за яким з метою забезпечення контролю, виключення фактів шахрайства можна простежити рух коштів держателя будь-якої картки.

Таблиця 2.1

Дія	"Паперовий слід"
Введення в оборот пластикової картки	Договір (контракт) між банком-емітентом і держателем пластикової картки
Початок розрахунків із застосуванням пластикової карточки в сервісному або торговому центрі	Договір (контракт) між банком-емітентом і сервісним або торговим центром
Розрахунок у сервісному або торговому центрі з застосуванням пластикової картки	Рахунок (сліп) сервісного або торгового центру (має підпис держателя пластикової картки), який направляється в банк-емітент пластикової картки

При вчиненні шахрайства з пластиковими картками злочинці можуть діяти, зовні не порушуючи традиційної процедури користування карткою. Це відбувається, коли використовуються способи, у яких не приймає участі персонал сервісних точок.

Підробленими вважаються пластикові картки, виготовлені виробниками, що не мають на це спеціального дозволу. Вони виготовляються з використанням подібних методів друку, а іноді і тих же самих засобів захисту, які використовуються для справжніх кредитних карток.

Кредити по підроблених картках звичайно використовуються повністю (практикується придбання дорогих товарів), потім картка знищується.

Пластикові картки, викрадені у їх держателів в одній країні, можуть бути використані в іншій. Злочинці пред'являють для оплати товарів і послуг ці пластикові картки, видаючи себе за їхніх законних держателів, розписуючись від їхнього імені в рахунках, які оформляються, і пред'являючи підроблені посвідчення особи зі своєю фотографією.

Як уже згадувалося вище, із метою профілактики злочинів банки-емітенти періодично інформують мережу організацій, що приймають картки до оплати, про номери карток, визнаних недійсними: украдених, загублених, повністю підроблених, фальшивих. Така інформація доводиться у вигляді списку номерів недійсних карток, який називають "стоп-лист". Платежі за недійсними картками не повинні проводитися, тому співробітникам підприємств необхідно регулярно (не рідше одного разу на тиждень) одержувати "стоп-листи" із переліком недійсних карток.

Підготовка і вчинення злочинних посягань з використанням пластикових платіжних засобів потребує певних знань в області: механізму використання пластикових карток, їхніх функціональних характеристик, видів, технічних вимог до оформлення, системи захисту пластикових карток, застосування спеціальних прийомів і засобів друку, розпізнавальних ознак, застосування високотехнологічних захисних ознак (у тому числі магнітного контролю).

Набір знань диктується обраним зловмисниками способом учинення посягання або навпаки - наявний набір знань диктує вибір способу. Одній особі досить складно вирішити весь комплекс проблем, що виникають. Тому нерідко, на етапі підготовки до вчинення злочину і на етапі його реалізації діють різні особи. Так, крадіжки пластикових платіжних засобів вчинюють проститутки, кишенькові злодії, квартирні злодії, обслуговуючий персонал готелів. Ці особи частіше усього збувають викрадені картки, не ризикуючи безпосередньо заволодіти матеріальними цінностями або просто не маючи достатніх знань для закінчення шахрайської операції.

Без створення угрупувань злочинні посягання можуть здійснювати самі власники карток або працівники банків, що заявили про втрату картки, яка належить їм або знаходиться в їхньому веденні.

Серед учасників викрадання карток можуть бути працівники поштових установ, злочинні групи вантажників в аеропортах, які діють за завданнями

організованих злочинних угрупувань і вилучають картки з поштових відправлень [6].

Таким чином, класифікація суб'єктів шахрайства з використанням пластикових платіжних засобів, може бути розглянута за такою схемою:

- персонал обслуговуючих сервісних точок;

- особи, що займаються викраденням карток;

- особи, що використовують загублені картки;

- банківські службовці;

- особи, що займаються виготовленням підроблених пластикових карток;

- особи, що є законними держателями пластикових карток.

Основним механізмом попередження і профілактики злочинних посягань з використанням пластикових платіжних засобів є побудова і реалізація комплексної, багатофункціональної системи безпеки пластикових платіжних засобів. У даному підрозділі зупинимося на аналізі деяких причин, що сприяють можливості здійснення протиправних дій.

Основними причинами, які сприяють шахрайству з використанням пластикових платіжних засобів, є по перше: а) нерозумна економія на засобах захисту пластикових платіжних засобів і по друге: б) невчасне і не всеохоплююче використання "стоп-листів" з метою припинення шахрайства з картками.

З метою профілактики злочинів із застосуванням пластикових карток їхні емітенти періодично інформують мережу організацій, що приймають картки, про номери карток, визнаних недійсними: украдених, загублених, підроблених, фальшивих. Така інформація, як уже говорилося, доводиться у вигляді списку номерів недійсних карток ("стоп-листа").

Платежі за недійсними картками не проводяться, тому співробітникам торгових підприємств і сервісних точок необхідно в усіх випадках робити звіряння, особливо якщо виникають підозри в правомірності використання пластикової картки якоюсь особою. "Стоп-листи" формуються по регіонах:

Європа, Африка, Північна Америка, Росія і т.д. розміщення картки в "стоп-листі" обходиться компаніям (банкам) у значні суми, тому з метою економії в окремих випадках вони направляють картки не у всі регіони, а в регіони найімовірнішого кримінального використання.

Умовою, що сприяє злочинним посяганням, є також недостатня взаємодія банківських структур і правоохоронних органів. Банки зацікавлені в залученні клієнтів, оскільки, використовуючи їхні кошти, вони отримують прибуток. Мабуть, з цими і низкою інших обставин пов'язано те, що окремі банки не завжди вимагають ретельної перевірки кандидатів на придбання пластикових платіжних засобів і, часто, з метою збереження іміджу, приховують факти шахрайства з пластиковими платіжними засобами, розраховуючись з потерпілими власними коштами.

Прояви настороженості з боку працівників окремих банків, небажання розголошувати свою неспроможність, окремі провали в роботі заважають правоохоронним органам здійснювати профілактичні заходи і опосередковано додають впевненості у безкарності особам, що вчинюють ці злочини.

Але слід зазначити, що в правоохоронних органах має місце недооцінка суспільної небезпеки даного виду злочинного посягання, яка призводить до того, що викрадені картки не вносяться в списки номерних викрадених речей і тому не завжди потрапляють у поле зору працівників міліції при обшуку осіб, затриманих за інші правопорушення.

Злочинним посяганням з використанням пластикових карт сприяє також халатне ставлення окремих службовців банку до збереження службової інформації або недбале збереження пластикових платіжних засобів, не говорячи вже про те, якого збитку банку може завдати умисне співробітництво банківських службовців із злочинцями.

Сприяє вчиненню злочинного посягання і те, що бланки, які використовують для оформлення сліпів, не в усіх банках є бланками суворої звітності, що полегшує доступ до них шахраїв.

Важливим фактором, що сприяє злочинним посяганням є недоліки в діяльності торгових і сервісних організацій, де обслуговуються держателі пластикових платіжних засобів. Зокрема, допускаються численні факти грубих порушень порядку обслуговування держателів пластикових карток, зокрема, ведення касових операцій.

Для кожної разової операції з картками конкретного емітента встановлюється максимальний ліміт суми операції. Це означає, що власник картки може протягом одного дня використовувати свою картку в різноманітних пунктах обслуговування (готель, ресторан, бар, бюро прокату автомобілів і т.д.), і в кожному пункті сума проданих товарів або зроблених послуг не повинна перевищувати встановленого ліміту.

Розмір ліміту має строго конфіденційний характер і повідомляється кожному підприємству окремо. Емітенти можуть періодично змінювати ліміти суми операції. У випадку, коли сума вартості одноразово проданого товару або зроблених послуг перевищує встановлений ліміт, підприємствам забороняється розбивати цю суму на декілька рахунків. Підприємство повинно запросити через авторизаційні центри спеціальний дозвіл - код підтвердження.

Касири, замість того, щоб через авторизаційні центри запросити код підтвердження на пред'явлену до оплати кредитну картку і тим самим перевірити, заявлено її як втрачену чи ні, розбивають цю суму на кілька частин. Крім того, касири допускають факти, коли пред'явник пластикової картки розписується в рахунку (сліпі) не в його присутності або присутності працівника підприємства обслуговування. Це дає можливість підробити підпис. Такі дії можуть бути як результатом низької кваліфікації працівника сервісного підприємства, так і результатом його змови зі злочинцями.

При прийомі пластикових карток до оплати необхідно перевірити її відповідність встановленій формі за всіма параметрами, згідно інструкціям. При огляді пластикової картки, що викликає сумнів, доцільно порівняти її зі справжньою карткою. На підробку картки можуть вказати такі деталі:

- вм'ятини або зсув кольорів на друку;

- нерівномірна відстань між буквами, цифрами, знаками, зсув їх у ряду;

- хвилеподібні зміни на поверхні картки (як можливий результат теплової обробки);

- сліди змін (стирання, виправлення, перефарбування) на полі підпису (поле можуть зафарбувати білою фарбою або змінити на нове за допомогою клейкого паперу).

У випадку, коли виникає підозра про зміну номера картки, необхідно зіставити номера на її лицевій і зворотній сторонах.

Якщо картки випускаються фінансовими установами, то будь-які збитки від шахрайських дій, що пов'язані з використанням цих карток, несе організація, що випустила їх, у тому випадку, якщо буде встановлено, що продавець повністю виконав свої обов'язки, передбачені укладеним із ним договором. Якщо ж буде доведено, що продавець через недбалість або умисно не виконав усіх необхідних вимог, то на нього може бути покладене відшкодування збитку.

Такого ж порядку дотримуються і для карток для подорожей, туризму і відпочинку. Виняток складають фірмові картки (відомчі), де продавець і кредитор – одна і та ж юридична особа.

При видачі картки в договорі вказується, що у випадку неправомірного використання або неповідомлення про втрату власник картки може бути оштрафований на суму до 50 доларів США. Компанії вважають цю умову важливою, щоб підкреслити цінність картки і необхідність уважного ставлення до її захисту від злочинних зазіхань.

Необхідно відзначити, що за кордоном, як правило, продавці не вимагають у клієнтів документи, що засвідчують особу. Це пов’язано з тим, що, отримавши дозвіл на основі номеру картки на здійснення угоди, продавець у будь-якому випадку одержує від компанії оплату і встановлення особи клієнта його не цікавить.

Використання чіпових карток, оснащених мікросхемою, у великій мірі ускладнюють здійснення злочинних посягань. Справа в тому, що точне копіювання чіпової картки практично неможливе, з огляду на високу технологічність процесу її виготовлення. Нечисленні фірми-розробники тримають будову кристала в найсуворішому секреті. Полем бою стають комп'ютерні комунікації, а зброєю - програми, алгоритми обслуговування, глобальні системи захисту [11].

У міру того, як сучасні електронні грабіжники придумують нові хитрощі, емітенти удосконалюють системи захисту на комп'ютерному рівні. До подібних заходів можна віднести використання прихованих ключів-паролів [13]. Наприклад, зловмисник якимось чином одержав доступ до вихідної точки – електронного термінала. Він має інформацію про чужий рахунок і хоче рахунок змінити. Але його дії можуть бути заблоковані, оскільки кожна ланка ланцюга, по якому проходить транзакція, захищена ключами, якими управляє адміністратор даної ділянки [1].

РОЗДІЛ ІІІ. РОЗРОБКА НОВІТНІХ ЗАХОДІВ ТА ТЕХНОЛОГІЙ, З МЕТОЮ МІНІМІЗАЦІЇ ВТРАТ В НАСЛІДОК ІНФОРМАЦІЙНОГО ШАХРАЙСТВА.

3.1. Розробка заходів щодо створення Національного кредитного бюро.

Значну роль в запобіганні шахрайства в розвинених країнах відіграють кредитні бюро, які акумулюють кредитні історії, здійснюють облік, обробку, оновлення, зберігання, отримання та надання інформації щодо них.

Необхідність в таких організаціях вже давно назріла в Україні. Створення такої системи дозволить не лише запобігти втратам та мінімізувати ризики при наданні кредитів малому бізнесу та фізичним особам а й активізувати роботу банків в цьому напрямку.

Розглянемо базові організаційні та технічні засади створення такої системи в Україні.

Кредитне бюро має виконувати такі функції:

- ведення кредитних історій;
- впровадження та розповсюдження спеціалізованого програмного забезпечення, що використовується для автоматизації діяльності учасників системи кредитного бюро;
- надання консультаційних послуг, зв'язаних з інформаційним забезпеченням учасників системи кредитного бюро;
- здійснення маркетингових і статистичних досліджень;

Кредитна історія формується за допомогою передачі в кредитне бюро постачальниками інформації, а також за допомогою дій кредитного бюро по її одержанню, аналізу, систематизації й обліку.

Формування кредитних історій має здійснюватись з урахуванням наступних принципів:

- повноти й об'єктивності інформації;
- рівності всіх суб'єктів кредитних історій у захисті їхніх законних прав і інтересів і забезпечення такого захисту;

- послідовності і незмінності інформації, що надходить
- систематичності, регулярності і безперервності надходження інформації;
- цільового використання інформації;
- невтручання в особисте життя громадян і інтереси юридичних осіб і держави;
- конфіденційності інформації;
- відповідальності осіб, винних у перекручуванні і розголошенні інформації.

Учасниками системи кредитного бюро є:

1) кредитне бюро;
2) постачальники інформації;
3) одержувач кредитних звітів;
4) суб'єкти кредитних історій;
5) органи державного контролю.

Постачальниками інформації мають бути:

- комерційні банки;
- організації, що здійснюють окремі види банківських операцій;
- страхові організації, що здійснюють обов'язкові види страхування;
- податкова інспекція;
- органи, що здійснюють реєстрацію населення;
- державний орган, що здійснює контроль за проведенням процедур банкрутства;
- інші фізичні і юридичні особи на підставі укладених договорів.

Одержувачами кредитних звітів мають бути:

- банки, організації, що здійснюють окремі види банківських операцій;
- страхові організації, що здійснюють обов'язкові види страхування:
- юридичні особи, що реалізують товари і послуги в кредит;

- суб'єкти кредитних історій:
- органи попереднього слідства і дізнання по наявним у їхньому виробництві кримінальним справам;
- суди по наявним у їхньому виробництві справам;
- органи прокуратури на підставі постанови про здійснення перевірки в межах компетенції по матеріалах, що знаходяться в них на розгляді;
- митні органи у випадках надання відстрочки по митних платежах;
- органи податкової служби в зв'язку зі здійснюваними ними перевірками платників податків;
- органи виконавчої служби по справам, що знаходяться в їхньому виробництві.

Кредитне бюро має нести відповідальність за повноту, точність і своєчасність надання інформації, що міститься в кредитній історії. Кредитне бюро повинно вести облік запитів про надання кредитного звіту й облік наданих кредитних звітів. У звіті кредитного бюро, видаваного по запиту суб'єкта кредитної історії, повинні бути відбиті усі факти надання кредитних звітів по кредитній історії даного суб'єкта, раніше з зазначенням дати видачі і реквізитів одержувачів. Надання кредитного звіту комерційним структурам має відбуватись тільки при наявності згоди суб'єкта кредитної історії.

Першочергове значення для роботи кредитного бюро має автоматизована система підтримки. Розглянемо базову функціональність автоматизованої системи „Кредитне бюро". Така система має вирішувати такі завдання: формування і ведення централізованої бази даних про позичальників, забезпечення можливостей віддаленого доступу до неї, реалізацію інтерфейсів з іншими системами автоматизації, набір додаткових сервісних функцій і звітності для учасників системи, функції запобігання шахрайства, реалізацію маркетингових функцій, можливості тарифікації, взаємодія з БД інформаційних систем органів державної і виконавчої влади і т.д.

Перелік функцій:

- Пошук кредитних історій по 30-40 параметрам;
- Розширений пошук;
- Реєстрація нових кредитних історій;
- Облік придбання і погашення заборгованостей з урахуванням фактів прострочення і пролонгації;
- Ведення історії зміни реквізитів позичальників;
- Облік гарантів по кредитах;
- Взаємодія з абонентами в захищеному режимі;
- Шифрування даних;
- Розсилання аналітичних звітів абонентам;
- Видача по запиту абонента кредитної історії;
- Імпорт даних із систем автоматизації кредитних союзів;
- Розрахунок загальної заборгованості і заборгованості в розрізі груп і окремих позичальників;
- Розрахунок кредитного рейтингу позичальника;
- Взаємодія з базами даних систем автоматизації банків та інших фінансових установ одержання для даних про позичальників;
- Взаємодія із системою ініційована користувачами;
- Фіксація усіх фактів звертання до кредитних історій;
- Формування звітності по звертаннях до кредитних історій;
- Формування довідки для позичальника;
- Аналітика (не складна) з можливістю проектування аналітичних показників;
- Розсилання аналітичних даних абонентам;
- Формування звітності з можливістю розсилання абонентам;
- Формування стоп-аркушів несумлінних позичальників з можливістю розсилання;
- Розподіл прав доступу до даних;

- Імпорт/експорт даних
- Автоматична архівація даних;
- Ведення протоколу роботи користувачів із системою.
- Тарифікація звертань;
- Формування рахунків за користування системою;
- Складні запити;
- Фільтри і бізнесу-правила для контролю надмірної заборгованості з можливістю автоматичного оповіщення учасників системи;
- Процедури фіксації і врегулювання претензій;
- Маркетингові функції;
- Робота із шаблонами запитів;
- Реєстрація користувачів і постачальників інформації;
- Звітність по користувачах і постачальникам даних;
- Можливість тимчасового блокування будь-якого об'єкта або елемента даних у системі;
- Функції звірки даних;
- Облік заявок на надання кредитів і корегування з урахуванням цього рейтингу позичальників;
- Можливість моделювання процедур корегування даних, усунення претензій, і т.д на. основі технології бізнесів-процесів.
- Механізми контролю за цільовим використанням наданої інформації (зіставлення числа запитів з числом виданих кредитів);
- Механізми анулювання і вилучення кредитних історій;
- Взаємодія з базами даних інформаційних систем органів державної і виконавчої влади
- Статистика роботи системи;
- Ведення довідників (різноманітних для користувачів);
- Взаємодія з аналогічними системами;
- Додаткові бази даних (банкрутства, судові рішення, майно в заставі);

- Підтримка додаткової позитивної і негативної інформації.

Функції запобігання шахрайства;

- Моніторинг;
- Розрахунок середніх значень і встановлення контрольних орієнтирів;
- Аналіз відхилень і пошук потенційних-недостовірних даних;
- Робота з графікою (фотографії позичальників з метою недопущення шахрайства);
- Оцінка ризиків кредитування позичальника і видача рекомендацій;
- Рейтинги безпеки і рекомендації для користувачів по забезпеченню безпеки в договорах;
- Дослідження поведінки позичальників.

Особливості реалізації:

- Робота в діалоговому режимі;
- Робота в реальному масштабі часу;
- Робота через Web- інтерфейс;
- Забезпечення одночасної роботи із системою декількох користувачів;
- Підтримка механізмів файлового обміну даними;
- Механізми гарантії доставки повідомлень;
- Робота з ЭЦП;
- Доступ системи по декількох каналах.

3.2. Розробка вимог до системи автоматизації моніторингу.

Для активного попередження випадків шахрайства поряд з створенням системи кредитного бюро винятково важливе значення має впровадження систем моніторингу трансакцій та оперативної діяльності структурних

підрозділів. В умовах України з недостатньо розвиненою інфраструктурою проблеми шахрайства найближчим часом не можуть бути вирішені централізовано. Тому значну роль мають відігравати заходи на місцях. Випадки злочинних дій організованих за допомогою персоналу фінансово-кредитних установ робить актуальною задачу контролю операції структурних підрозділів. Необхідно зазначити, що моніторинг може бути ефективним лише в умовах масового впровадження та використання.

Базові засади організації системи моніторингу на рівні локальних об'єктів:

- Моніторинг має виконуватись на рівні максимально можливого числа об'єктів;
- Результати моніторингу мають консолідуватись на рівні головних установ;
- Необхідно забезпечити можливість математичної та статистичної обробки великих масивів даних про трансакції на рівні локальних об'єктів;
- Система підтримки має забезпечувати можливість нарощування новими моделями та методами контролю;
- Прозорість методичного забезпечення для користувачів та можливість вдосконалення методичного апарату з використанням стандартних інструментальних засобів;
- Система моніторингу має бути відокремленою від систем, що контролюються нею;
- Робота системи моніторингу не повинна заважати роботі підконтрольної системи автоматизації (в першу чергу ще стосується продуктивності);

Слід зазначити що система моніторингу має працювати в умовах коли:

- набір вхідних і вихідних даних не визначений цілком, вірніше, може змінюватися;

- вона розрахована на рішення проблеми моніторингу для широкого кола фінансово-економічних і управлінських задач;
- функції й алгоритми перетворення вхідних даних у вихідні можуть змінитися в ході проектування й експлуатації;
- у процесі роботи системи набір розв'язуваних задач, вхідних і вихідних даних може істотно змінюватись;
- Іншою важливою вимогою є доступність системи для широкого кола потенційних користувачів за ціновими характеристиками.

Серед стратегічних вимог до автоматизованої системи моніторингу необхідно визначити такі:

- реалізація у вигляді конструктора;
- мінімальна вартість ліцензії;
- мінімальна вартість володіння;
- максимальна прикладна функціональність;
- простота реалізації;
- інтеграція з існуючими системами автоматизації;
- простота впровадження, супроводу і навчання;
- незалежність прикладних функцій системи одна від іншої;
- можливість поступового нарощування функціональності;
- можливість часткової і поетапної реалізації системи;
- відкритість;
- мінімальні зміни вихідного коду при настроюванні і впровадженні системи;
- використання стандартних засобів розробки;
- великий термін ефективного використання системи;
- розвиті засоби адміністрування й ін.
- можливість доробки стандартними (без вбудованих компіляторів і інтерпретаторів) засобами;

Розглянемо необхідну функціональність системи моніторингу на прикладі підсистеми „Моніторинг” ІС БізнесПроцесор 5.х. розробки компанії МетаСистеми www.metasystems.sumy.ua.

Базова версія цієї системи, передбачає рішення наступних блоків задач:

- організація збору, надійного збереження і використання внутрішньої і зовнішньої корпоративної інформації;
- рішення задачі проектування, створення, управління, обробки бізнес-процесів;
- оперативне управління об'єктами і бізнес- процесами;
- облік;
- моніторинг бізнес- процесів, показників і ресурсів компанії;
- розрахунок техніко-економічних показників;
- формування звітності;
- сервісних і адміністративних задач та ін.

Модуль «Моніторинг» призначений для контролю та обчислення статистичних параметрів різних процесів, для яких ведеться відстеження в часі чисельних характеристик функціонування.

Обчислення параметрів і формування звітності може вироблятися в ручному, або цілком автоматичному режимі, модуль підтримує обчислення параметрів з урахуванням консолідації даних по різних об'єктах.

Модуль підтримує технологію Microsoft Scripting Host, усі параметри можуть бути змінені безпосередньо самим замовником, можуть бути додані нові параметри і форми звітів, підтримується технологія OLE DB для забезпечення доступу до даних, унаслідок чого модуль може бути інтегрований з існуючими статистичними пакетами, наприклад, SPSS for Windows або Microsoft Excel, для істотного розширення існуючої функціональності підтримується технологія бібліотек, що автоматично відвантажуються (Plug-Ins).

Працюючи в автономному режимі модуль, може обмінюватися результатами моніторингу та розрахунку показників з копіями модуля на

інших об'єктах через технологію SMTP/POP3, за рахунок чого реалізується автоматична консолідація даних по різних об'єктах.

Архітектура та склад модулю „Моніторинг”

Модуль обчислення параметрів

Здійснює безпосередній розрахунок параметрів, може працювати в автоматичному, або ручному режимі, забезпечує:

1. розрахунок статистичних параметрів вбудованими засобами з використанням MS Windows scripting host і стандартних компонентів Borland Delphi;
2. розрахунок вбудованих параметрів за допомогою статистичних пакетів, що підтримують технологію Active і ODBC/OLE DB доступ до даних (MS Excel, SPSS for Windows і т.д.)

Розрахунок значень показників здійснюється відповідно до параметрів, заданими в модулі настроювання параметрів, а результат зберігається в окремій базі даних.

Модуль настроювання параметрів моніторингу

Забезпечує конфігурування параметрів модуля «Статобработка»:

- задаються способи і методи обробки даних, а також їх параметри;
- підтримується аудит способів обробки даних і їхнє редагування;
- створення нових способів обробки даних вбудованими засобами (на основі SQL і MS Windows scripting host);
- підключення існуючих засобів (статистичних пакетів), що підтримують технологію Active і ODBC/OLE DB доступ до даних (MS Excel, SPSS for Windows і т.д.)

Доступ до модуля настроювання параметрів обмежений окремими групами користувачів і захищений паролем.

База даних

Забезпечує збереження різних типів даних: чисельних для представлення в табличній формі, звітів, діаграм, графіків, будь-яких результатів роботи додатків, що підтримують технологію Active.

База даних спроектована з урахуванням консолідації даних: підтримується перегляд результатів обробки даних по окремих структурних підрозділах, для тих параметрів, для яких це можливо, надається можливість побудови зведених звітів.

Модуль візуалізації результатів

Модуль забезпечує відображення, вивід на принтер і збереження у файли результатів обробки даних(звітів, таблиць, графіків і т.д.)

Модуль консолідації даних

Даний модуль забезпечує переміщення даних між окремими інсталяціями додатка „Моніторинг” з метою їх консолідації.

Модуль забезпечує автоматичне переміщення даних через e-mail по протоколах SMTP/POP3, або забезпечує завантаження/вивантаження даних для їхнього переміщення по інших каналах зв'язку.

Окреслимо переваги організації моніторингу на локальних об’єктах за такою схемою:

– відсутність необхідності ручного введення найменувань параметрів і складного настроювання – настроювання параметрів статистичної обробки зводиться до асоціації способів статистичної обробки даних з моделями, уже побудованими в системах обробки трансакцій;
– мінімальні витрати на ліцензування програмного забезпечення;
– підтримка роботи в цілком автономному режимі – користувач тільки переглядає результати без необхідності очікування перерахунку показників, можливість автоматичного пересилання результатів обробки даних через e-mail;

- можливість швидкого та простого розширення можливостей системи без втручання розробника; математичний апарат та алгоритми можуть буди змінені без втручання в базовий програмний код;
- можливості автоматичного сповіщення користувачів про настання певних подій, отримання значних відхилень в підконтрольних параметрах, ігнорування некоректних даних;
- можливість реалізації розрахунку параметрів обробки даних винятково внутрішніми засобами системи, усуваючи необхідність установки сторонніх пакетів, підвищуючи в такий спосіб стабільність і зменшуючи вартість кінцевого рішення;
- надійна система захисту від несанкціонованого доступу до модифікації алгоритмів і результатів розрахунку параметрів моніторингу.

Окрім спеціалізованого модулю базова поставка ” ІС БізнесПроцесор передбачає розширені можливості організації моніторингу за рахунок організації моніторингових бізнес-процесів на рівні бізнес-логіки. Такі процеси призначені для спостереженням за трансакціями, ходом вирішення завдань, критичними ситуаціями і режимами а також контролю відхилень. Такі процеси можуть існувати постійно або запускатись у відповідь на порушення нормального режиму роботи інформаційної системи.

Моніторингові процеси дозволяють в режимі читання отримати доступ до необхідних даних, а також перевірити їх на виконання певного набору умов. Процеси цього типу можуть містити набори керуючих команд та подій для виправлення ситуації (що генеруються в ручному або автоматичному режимах). Таким чином моніторингові процеси дозволяють побудувати досить складні контури зворотнього зв’язку та інтелектуального регулювання.

Моніторингові процеси можуть генерувати зовнішні події для управління іншими БізнесПроцесорами або зовнішніми інформаційними системами.

Зупинимось на перевагах організації моніторингу за такою схемою:

- За допомогою таких систем має здійснюватись моніторинг і інших сфер діяльності організації, що забезпечить базу для вдосконалення роботи структурних підрозділів;
- Незалежність функцій та методів моніторингу, дозволять постійно нарощувати функціональність і продуктивність системи.
- Система дозволяє вести паралельний облік у декількох площинах і розрізах. Це забезпечує підвищення ефективності роботи кінцевого користувача.
- Використання стандартних середовищ програмування робить можливою доробку системи без залучення розробника. Це робить незалежним від нього кінцевого користувача.
- Можливість забезпечити ефективну роботу у випадку неповноти вхідної інформації, за рахунок контрольних значень, що містять моделі процесів;
- Отримання стратегічних переваг перед конкурентами за рахунок ефективного контролю основних сфер діяльності;
- Можливість впровадження найсучасніших технологій управління;
- Якісне вирішення індивідуальних і досить складних задач з мінімальними витратами;
- Отримання унікальних споживчих властивостей та застосування для виришення практично будь яких фінансово економічних задач;
- Економію коштів на впровадженні, навчанні персоналу та супроводженні системи;

Перераховані можливості роблять ІС БизнесПроцессор зручною платформою для реалізації прикладних рішень в області моніторингу і управління бізнес-процесами банків та інших установ.

Таким чином масове використання систем моніторингу дозволить суттєво знизити втрати від шахрайства, більш оперативно ідентифікувати випадки та нові схеми шахрайства, консолідувати дані для колективного використання або централізованої розробки заходів щодо попередження шахрайства.

Висновки

Проблема шахрайства стає все більш актуальною в усьому світі. Збитки від нього ростуть швидкими темпами. Україна не є винятком з цієї тенденції.

В сучасних умовах України ефективними засобами боротьби з шахрайством мають стати:

- система централізованого контролю не зможе забезпечити оперативних захист та запобігання збитків від нових схем шахрайства, тому значна частина зусиль має бути зосередженою на рівні локальних об’єктів;
- створення Національного кредитного бюро або системи спеціалізованих кредитних бюро;
- масове впровадження та використання недорогих систем економічного моніторингу, які б забезпечили не тільки зменшення втрат від шахрайства але й загальне підвищення ефективності роботи установ;
- значну роль в поширенні нових технологій, методичних розробок та передового досвіду боротьби з шахрайством має відігравати Національний банк та інші державні установи;
- Значну роль в проблемі боротьби з шахрайством мають відігравати автоматизовані системи управління ризиками.

Список використаної літератури

1. Аглотков С.А. HP OpenView - як засіб адміністрування банківських систем // Перспективні банківські технології.- К.: Коміздат, 1997.- С.39.
2. Астапкина С.М., Максимов С.В. Криминальные расчеты: уголовно-правовая охрана инвестиций: Научно-практическое пособие.- М.: Учебно-консультационный центр ЮрИнфоР, 1995.- 128с.
3. Ванин А., Сумманен К., Введение в телебанкинг//Банковские технологии.-2000-№8.
4. Вересюк А. Мобильный банкинг: дорогостоящая игрушка или реальный источник прибыли? // Банковская практика за рубежом (рус.).- 2001.- № 4.- С.76-80.
5. Вертузаєв М.С., Голубєв В.О., Котляревський О.І., Юрченко О.М. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / Під ред. д.ю.н. О.П.Снігерьова. - Запоріжжя: ПВКФ "Павел", 1998.- 316 с.
6. Вертузаєв М.С., Хрипко С.Л. Шифрування як засіб захисту інформації // Інформаційні технології та захист інформації: Збірник наукових праць.- Запоріжжя: Юридичний ін-т МВС України, 1998.- Вип.2.- С.24-32.
7. Карточки для наивных американцев // Мир карточек, 1997.- № 21.- С.5-6.
8. Грачева М. В. Электронные банковские услуги // Банковские технологи.- 2002.-№6.
9. "Карточный" детектив: борьба с мошенничеством в сфере пластиковых карточек в России // Мир карточек, 1997.- № 17.-С.27-31.
10. Котляревский А.И. Международный опыт расследования мошенничеств с использованием кредитных карточек // Бюллетень по обмену опытом работы.- № 120, 1997.- С.73-81. Инв. № 1152.

11. Котляревський О.І. Шахрайства с використанням пластикових платіжних карток: Збірник наукових праць.- Запоріжжя: ЗЮІ МВС України, 1998.- № 1.- С.49.

12. Кредитные карты как инструмент совершения мошеннических операций и практика борьбы с данными преступлениями // Материалы V международной конференции "Бизнес и безопасность. Мировой опыт" (Москва, 20-21 мая 1998г.).- М.: Ассоциация международного сотрудничества "Безопасность предпринимательства и личности".- С.1-4.

13. Минина Т.И. Электронные банковские услуги // Банковские услуги.-2002.- №7.

14. Немчин О.В. Предупреждение и противодействие мошенничеству, корыстным злоупотреблениям при проведении валютных операций // Безпека бізнесу (рекомендації, поради, консультації спеціалістів).- К.: Українська економічна студія, 1998.- С.57-75.

15. Павлова Т. Интернет-банки в борьбе за выживание // Банковская практика за рубежом (рус.).- 2002.- № 1.- С.12-16.

16. Семенов А. Интернет-банкинг// Банковские технологи.- 2002.- №2.

17. Шапран В.С. Інтернет - банкінг: небезпека очевидна! // Фондовий ринок (укр.).- 2002.- № 4.- С.20-22.

18. Шеремет А.Д., Сайфулин Р.С. Финансы предприятий. Учеб. пособие. — М: ИНФРА-М — 1999.

19. Шимкович В. Конкуренция в виртуальном пространстве // Банковская практика за рубежом (рус.).- 2002.- № 3.- С.15-20.

20. Юрченко О.М. Зарубіжний досвід попередження шахрайств з використанням пластикових платіжних карток // Інформаційні технології та захист інформації: Збірник наукових праць.- Запоріжжя: Юридичний ін-т МВС України, 1998.- Вип.2.- С.41-53.

21. Юрченко О.М. Способи посягань на майно банків та їх вкладників із застосуванням пластикових платіжних засобів // Безпека

бізнесу (рекомендації, поради, консультації спеціалістів).- К.: Українська економічна студія, 1998.- С.76-112.

22. "Book of DS19xx Touch Memory Standards", Edition 2.0. - 1994.- Dallas Semiconductor Corporation, Dallas, Texas.

Додаток А

Перелік даних, що мають міститись в кредитній історії фізичної особи

По позичальниках і гарантам:

- Прізвище, Ім'я, По батькові;
- Унікальний код у рамках системи;
- Паспортні дані;
- Податковий код;
- Прописка;
- Місце фактичного проживання;
- Попереднє місце проживання;
- Дата народження;
- Місце народження;
- Родиний стан;
- Склад родини з даними про непрацездатних, дітей і т.д.;
- Освіта;
- Місце роботи, посада;
- Термін роботи на підприємстві;
- Судимість за корисливі злочини;
- Рішення суду про непрацездатність або обмежену працездатність;
- Інші документи (вид, ким і коли виданий, термін дії);
- Контактні телефони;
- Додаткова інформація;
- Дані про зміни;
- Поточний рейтинг;
- Зміна рейтингу за ...
- Захворювання;
- Чи є гарантом і поручителем третіх осіб;

- Чи є відповідачем по цивільній або кримінальній справі;

Поводження (дані за всю історію і за останні місяці)

- Загальна заборгованість по кредитах;
- Число порушень термінів виплат;
- Число заявок на кредит;
- Число виданих кредитів;
- Факти позитивного плану;
- Факти негативного плану;
- Депозити.

По кожному кредиту:

- Установа;
- Регіон, населений пункт;
- Дата договору;
- № договору;
- № рахунка;
- Тип рахунка;
- Валюта;
- %;
- Ціль кредиту;
- Дата видачі;
- Дата погашення;
- Термін кредитування;
- Дата останнього платежу;
- Графік погашення;
- Сума кредиту;
- Поточний залишок;

- Непогашена сума;
- Погашення %
- Кредитний ліміт (для карток);
- Спосіб оплати;
- Забезпечення кредиту;
- Гаранти (дані про гарантів);
- Застава (вид, вартість);
- Інші документи по кредиту;
- Додаткові відомості про позичальника;
- Додаткові умови за договором кредитування.

Дані про платоспроможність:

- Заробітна плата (середня за період);
- Інші доходи;
- Нерухоме майно (опис, вартість, страховка, співвласники);
- Рухоме майно (опис, вартість, страховка, співвласники);
- Інше майно (опис, вартість, страховка, співвласники);
- Майно в заставі.