Інформаційна система з перешкоджання несанкціонованих дій з банківськими картками

Андрій Касянчук, аспірант кафедри ІТ. Світлана Цюцюра, д.т.н., професор, завідувач кафедри ІТ, Ілля Саченко, к.т.н., доцент кафедри ІТ, Владислав Гоц, к.т.н., доцент кафедри ІТ

[1] *Київський національний університет будівництва і архітектури, Київ, Україна*

АНОТАЦІЯ

В даній роботі розглянуті питання аналізу діючої системи управління процесами карткових рахунків, формування вимог до ефективної інформаційної технології системи захисту БПК у мережі АТМ з боку користувача та розробника, формування цілей процесінгових центрів, як основного рубежу захисту БПК у мережі АТМ , дослідження ІТ цілодобового моніторингу АТМ транзакцій як основи ІТ захисту БПК у мережі АТМ.

Ключові слова: БПК, мережа АТМ, процесінговий центр, транзакції, моніторинг.

1. ВСТУП

Наша країна давно стала раєм для карткових шахраїв в очах закордонних банкірів. МВС і Нацбанк стверджують, що це не так, і рівень втрат від крадіжки з карткових рахунків не відрізняється від середньоєвропейського. Дійсна ситуація відома лише комерційним банкам – саме вони бажають не афішувати випадки шахрайства з картками їхніх клієнтів і намагаються не псувати офіційну статистику.

2. МЕТА РОБОТИ

Створення інформаційної технології для захисту банківських карт від несанкціонованих дій.

3. ТЕОРЕТИЧНІ ВІДОМОСТІ

Стійкий тривалий інтерес з боку банківських організацій, а також цілеспрямований рух організацій-одержувачів платежів по шляху автоматизації операцій формування і оплати рахунків, дозволяють говорити про те, що ринок платіжних систем самообслуговування сформувався об'єктивно і суб'єктивно. І одержувачі, і платники готові сьогодні перейти на пряме спілкування, виключивши проміжні ланки – існуючі паперові технології. У той же час, банки можуть зайняти адекватне місце в новій технології, виконуючи властиву їм фінансову частину процедури, причому в самій передовій формі – електронній[1].

3D Secure – це сучасна технологія, розроблена для забезпечення безпеки карткових платежів в мережі Інтернет, що дозволяє ідентифікувати особу, яка здійснює операцію і максимально знизити ризик шахрайства по ній. Підвищення безпеки при здійсненні інтернет-платежів на сайтах, що підтримують технологію 3D Secure, відбувається за рахунок проведення додаткової ідентифікації власника платіжної картки шляхом обов'язкового введення власником картки одноразового пароля, який в ході операції автоматично направляється банком в SMS-повідомленні на номер мобільного телефону держателя [2].

Основна функція пластикової картки - забезпечення ідентифікації особи, що її використовує як суб'єкта платіжної системи. Для цього на пластикову картку наносяться логотипи банка-емітента і платіжної системи, що обслуговує картку, ім'я власника картки, номер його рахунку, строк дії картки.

Основним аргументом для впровадження «пластикових грошей» була зручність користувача. З появою електронних кошт реєстрації і збору інформації з'явилася можливість заносити і зчитувати інформацію на картку за допомогою кодування сигналу.

Система виконує роздільний моніторинг domestic- і international- транзакцій з контролем ризику по різних критеріях для обох типів операцій. Система формує базу даних про одного разу оброблених картах і відстежує їх подальшу АТМ – історію, розраховуючи статистичні характеристики контрольованих параметрів для кожної карти. Процес обчислення статистичних моментів оптимізований з метою забезпечення високої швидкодії системи.

У разі досягнення умов, при яких проводиться перевірка критеріїв ризику для даної карти, система автоматично розраховує їх порогові значення, що оновлюються у міру поповнення історії карти. Реакція системи передбачає як відсилання в Банк онлайнових повідомлень про карти, що входять в зону високого ризику, так і блокування, по розпорядженню Емітента, подальшого звернення карти за допомогою внесення її в стоп - список[3].

4. ПРОЕКТУВАННЯ ПРОГРАМНОГО ПРОДУКТУ

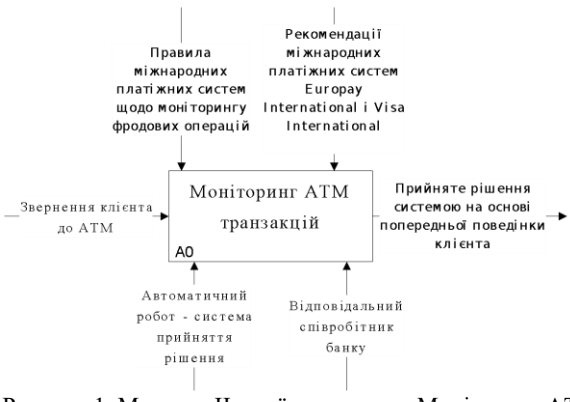

Рисунок 1. Модель «Чорної скриньки» «Моніторинг АТМ транзакцій»

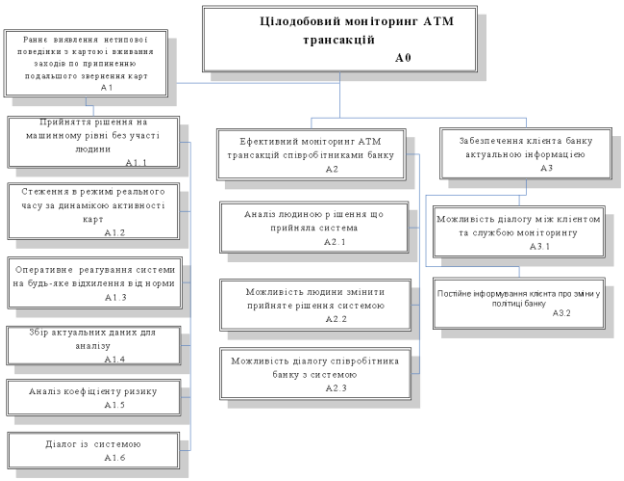

Рисунок 2. Дерево функцій «IT цілодобовий моніторинг АТМ транзакцій»

0. Цілодобовий моніторинг АТМ транзакцій – головна функція, що спонукала для створення IT.

1. Раннє виявлення нетипової поведінки з картою і вживання заходів по припиненню подальшого звернення карт до завершення авторизації повинно значно зменшити фінансові збитки банків від шахрайських операцій.

1.1 Прийняття рішення на машинному рівні без участі людини – головна функція яку ми будемо розглядати, для її виконання потрібно виконати наступні функції:

1.2 Стеження за активністю картки, в режимі реального часу, та динамікою активності картки.

1.3 Оперативне реагування системи на будь-яке відхилення від норми у поведінці клієнта до видачі коду авторизації.

1.4 Збір актуальних даних для аналізу, що буде проводити система.

1.5 Аналіз коефіцієнту ризику відбувається на машинному рівні і від нього залежить прийняте рішення системи.

1.6 Діалог із системою – для отримання актуального рішення потрібно перед початком роботи системи ввести необхідні параметри критеріїв ризику, які можна вирахувати для кожного з типів карт окремо и ввести в роботу також у режимі онлайн .

2. Ефективний моніторинг АТМ транзакцій співробітниками банку.

2.1 Аналіз людиною рішення що прийняла система вже не на стільки актуальний у часі, так як система сама обирає варіант відповіді і у разі шахрайства збитки зводяться до мінімуму.

2.2 Можливість людини змінити прийняте системою рішення.

2.3 Можливість діалогу співробітника банку із системою.

3. Забезпечення клієнта банку актуальною інформацією про стан рахунку, та операції що проводилися по платіжній картці.

3.1 Можливість діалогу між клієнтом та співробітником служби моніторингу.

3.2 Постійне інформування клієнта про зміни у політиці банку що до моніторингу потенційно фродових операцій шляхом Internet та SMS банкінгам.

5. ВИСНОВКИ

Вибір теми був зумовлений актуальними потребами такими, як стійкий тривалий інтерес з боку банківських організацій, а також цілеспрямований рух організацій-одержувачів платежів по шляху автоматизації операцій формування і безпечної оплати рахунків.

Створений комплекс є універсальним у користуванні будь-якими банківськими структурами, а також відповідає вимогам Держстандарту України щодо розробки програмного забезпечення.

Список джерел

[1] І.В. Смірнова, доц., канд. екон. наук, Я.В. Клименко, ст. гр. ОА 08-2 Кіровоградський національний технічний університет.Тенденції розвитку ринку платіжних карток у банківській сфері, 2012 с.57-58

[2] Офіційний сайт Національного Банку України URL:http://www.bank.gov.ua/.

[3] Васюренко О.В. Банківські операції: Навч. посіб. — К. : Знання, 2008. — С. 23-28.