УДК 336.71

Тетяна Сергіївна ПЕРЕДЕРІЙ,
студентка 2 курсу групи Ф-6-КБзб-17-2М факультету № 6
Харківського національного університету внутрішніх справ;
Оксана Сергіївна МАКОВОЗ,
доктор економічних наук, доцент,
завідувач кафедри економіки та фінансів факультету № 6
Харківського національного університету внутрішніх справ

СИСТЕМА FRAUD-МОНІТОРИНГУ В ЗАПОБІГАННІ ТА ВИЯВЛЕННІ ШАХРАЙСТВ З ПЛАТІЖНИМИ КАРТКАМИ

Сучасні умови господарювання вимагають прагнення до скорочення трансакційних витрат при здійсненні банківських операцій. Водночас з зазначеним особливої гостроти набувають питання захисту персональних даних контрагентів від посягання шахраїв. Зняти кошти з банківського рахунку вже можливо практично в будь-якій точці світу, а електронні сервіси допомагають проводити більшість платежів без застосування готівки, проте паралельно зі сферою нових фінансових послуг зростають і ризики використання платіжних карток.

За даними НБУ, у 2017 році тільки обсяг безготівкових операцій з використанням платіжних карток склав 835,0 млрд грн, що на 46,1% більше у порівнянні з 2016 роком, а кількість таких операцій становила 2,3 млрд шт., що на 27,7% більше ніж в 2016 році [1].

Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (далі - Закон) зобов'язує суб'єктів первинного фінансового моніторингу, якими в тому числі є банки, здійснювати ідентифікацію, верифікацію клієнта (представника клієнта), вивчення клієнта та уточнення інформації про клієнта у випадках, встановлених законом, забезпечувати у своїй діяльності управління ризиками та розробляти критерії ризиків, проводити аналіз відповідності фінансових операцій, що проводяться клієнтом, наявній інформації про зміст його діяльності та фінансовий стан з метою виявлення фінансових операцій, що підлягають фінансовому моніторингу, підтверджувати під час проведення верифікації відповідність ідентифікаційних даних особи клієнта (представника клієнта) відомостям, зазначеним в отриманих від нього офіційних документах [2].

На сьогодні одним із ризиків у використанні платіжних карток є «фрод», термін якого походить від англійського слова «fraud», що в перекладі означає «шахрайство». У широкому значенні фрод - це несанкціоновані дії і неправомірне користування ресурсами в сфері ІТ. Існує безліч типів фроду, при цьому ошуканими можуть виявитися користувачі, продавці, та банки. У більшості випадків об'єктом фроду

стають дані платіжних інструментів - банківських карт, електронних гаманців, мобільних засобів, хоча фродом можна назвати будь-який витік персональних даних, що веде до збагачення зловмисника [3].

Для попередження фроду на організаційно-адміністративному рівні, тобто без застосування спеціального ПЗ в організаціях зазвичай вживаються такі заходи: внутрішній аудит; навчання співробітників (anti-fraud awareness program); управління фізичним і логічним доступом; виявлення і контроль конфлікту інтересів; процедури узгодження і авторизації дій. Однак, коли всі бізнес-процеси, які обробляються в інформаційних системах знаходяться в сфері ризику, то одних адміністративних заходів стає недостатньо і в такому випадку застосовують антифрод системи [4].

Фрод-моніторинг – це обов'язкова складова превентивних заходів по боротьбі з шахрайствами, причому як із зовнішньої сторони (клієнти, зловмисники), так і всередині банку. Це моніторинг вхідної та вихідної інформації на предмет виявлення шахрайських дій [5].

Загальна схема роботи практично будь-якого механізму фрод-моніторингу виглядає таким чином: в момент здійснення оплати за допомогою банківської карти досліджується кілька показників (у кожної антифрод системи різні) - починаючи від IP адреси комп'ютера і закінчуючи статистикою оплат картою. Кількість фільтрів може перевищувати сотню (наприклад, у системи електронних платежів PayOnline фільтрів більше 120). Система має набір правил, тобто лімітів фільтрів безпеки, кожен з яких перевіряє користувача, а саме: його персональні і карткові дані. Мета системи - це переконатися в тому, що користувач є реальним власником карти, який здійснює купівлю на сайті. У разі виявлення підозрілої активності, тобто перевищення будь-якого значення параметра, фільтр автоматично блокує можливість здійснення платежу за цією карткою [6].

Передусім при здійсненні транзакції (фінансова операція) відбувається первинний аналіз на підставі факторів, які описані вище, а потім їй присвоюється «мітка», що характеризує спосіб обробки транзакції. Існують три типи міток: «зелена» відмічає транзакції з низькою ймовірністю виникнення шахрайської операції; «жовта» мітка - транзакції, в яких шанс виникнення шахрайської операції вище середнього, і для проведення платежу буде потрібно додаткової уваги; «червона» - транзакції, які з найбільшою ймовірністю можуть виявитися шахрайськими, і при їх проведенні потрібно документальне підтвердження автентичності власника карти. Таким чином використовуються найпростіші налаштування захисту: захист від підбору CVV і номера карт; аналіз параметрів карти банку, власника, типу продукту, країні випуску і географії використання; ідентифікація покупця з історії покупок; ретроспективний аналіз покупок; виявлення підозрілих транзакцій за відбитками використовуваного обладнання; перевірка домену та IP адреси [4].

Основними параметри виявлення шахрайських операцій, що застосовуються системами моніторингу є:

1. Оплата однією картою відбувається з різних пристроїв, що ідентифікованих різними IP адресами.

2. З одного і того пристрою (IP адреси) проводяться операції за допомогою великої кількості платіжних карт.

3. З однієї карти відбувається кілька невдалих спроб здійснити оплату (ймовірно, користувач не має можливості пройти процедуру підтвердження).

4. Один клієнт реєструється під декількома акаунтами, використовуючи різні адреси електронної пошти, і платить з однієї карти.

5. Ім'я платника, що вказане на платіжній формі, відрізняється від імені держателя карти.

6. Різні країни реєстрації інтернет-магазину, банку-емітента картки і покупця [3].

Основними перевагами системи моніторингу шахрайських операцій є автоматичне відхилення сумнівних транзакцій, захист суб'єктів господарювання і, звичайно ж, мінімізація репутаційних і фінансових ризиків. Водночас, як і у будь-якого сервісу, у системи фрод-моніторингу є свої недоліки: відхилення платежів може призвести до втрати клієнтів, а значить, й прибутку; без належного налаштування фільтри можуть не пропускати важливі транзакції; захист даних користувачів, як персональних, так і платіжних [6].

У Європі понад половину провідних банків передають цю функцію на аутсорсинг. Для оцінки клієнтських запитів на предмет шахрайств прийнято звертатися до спеціалізованих компаній. По-перше, подібні організації, як правило, консолідують інформацію в декількох банках, що дозволяє захистити від загрози тих, на кого атака ще не почалася. По-друге, спеціалізовані організації мають в своєму штаті висококваліфікованих аналітиків, які за результатами аналізу даних вчиненого шахрайства роблять прогнози щодо розвитку схем атак і пропонують конкретні заходи протидії. Однак при цьому виникають різні ризики,а саме: неякісний сервіс може призвести до негативних наслідків навіть перерв в роботі. Також проблема банківської таємниці є не менш актуальною, як показує практика, подібний підхід є ефективним [7].

Дослідники Масачусетського технологічного інституту розробили «автоматизовану функцію інжинірингу» підхід, якої виділяє понад 200 детальних особливостей для кожної окремої угоди - наприклад, якщо користувач був присутній під час покупок, а середня сума, витрачена в

конкретні дні в певних постачальників, то таким чином, вищезазначена функція краще визначає, коли витрати власника карт відхиляються від норми. Протестувавши набір даних в 1,8 мільйона транзакцій з банку, модель зменшила помилкові позитивні прогнози на 54 відсотки в порівнянні з традиційними моделями, які, за оцінками дослідників, могли врятувати банк в розмірі 190 000 євро (близько 220 000 доларів США) у разі втрати прибутку [8].

Банки приділяють особливу увагу вдосконаленню системам забезпечення безпеки в сегменті захисту клієнтів від протиправних посягань, скоєних за допомогою банківських карт, термінального обладнання та інших засобів електронного бізнесу.

Висновок. Таким чином, система fraud-моніторингу та застосування комплексу організаційно-технічних заходів захисту від шахрайських посягань сприятимуть мінімізації ризиків у використанні платіжних карток. Застосування fraud-моніторингу є дієвим інструментом запобіганні та виявленні шахрайств з платіжними картками, що формується під впливом нових інформаційних технологій у ведені діяльності суб'єктів господарювання для внутрішніх і міжнародних банківських операціях.

Саме застосування вищезазначеного виду моніторингу сприятиме запобіганню злочинних посягань. Основними цілями з реалізації ефективної системи захисту інформації має стати побудова ефективної системи захисту банку і клієнтів від кіберзагроз, а також впровадження систем фрод-моніторингу в різних сегментах банківської діяльності.

Список бібліографічних посилань

1. Рекомендації для зниження ризику шахрайських операцій : лист НБУ від 04.07.2018 № 57-0009/36366 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/v3636500-18 (дата звернення: 31.10.2018).

2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 05.01.2017 №1702-VII // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/1702-18 (дата звернення: 31.10.2018).

3. На страже безопасности - система Fraud-мониторинга // Про грабли. 29 октября 2015. URL: https://prograbli.ru/upgrade/on-guard-security-fraud-monitoring/ (дата звернення: 31.10.2018).

4. Пискунов И. Антифрод системы и как они работают // SecurityLab.ru. 6 Февраля 2017. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/339929.php (дата звернення: 31.10.2018).

5. Носаль А. В., Олехнович Л. В. Фрод-мониторинг как средство защиты банковских технологий // Электронный научно-технический журнал

«Студенческий вестник». Октябрь 2017 г. URL: http://e.biblio.bru.by/bitstream/handle/1212121212/5145/Nosal.pdf?sequence=1 (дата звернення: 31.10.2018).

6. 9 секретов онлайн-платежей. Часть 7: система Fraud-мониторинга // HABR. 23 июня 2016 в 20:40. URL: https://habr.com/company/payonline/blog/303204 (дата звернення: 31.10.2018).

7. Митричев И. Фрод-мониторинг меняет процесс обслуживания клиентов в банке, к этому надо быть готовым // Bankir.Ru. 05.09.2012. URL: https://bankir.ru/publikacii/20120905/ilya-mitrichev-frod-monitoring-menyaet-protsess-obsluzhivaniya-klientov-v-banke-k-etomu-nado-byt-gotovym-10002191/ (дата звернення: 30.09.2018).

8. Matheson R. Reducing false positives in credit card fraud detection // MIT News. September 20, 2018 URL: http://news.mit.edu/2018/machine-learning-financial-credit-card-fraud-0920 (дата звернення: 31.10.2018).

Одержано 31.10.2018

УДК 004.056.5

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук,
доцент кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-3381-3350;
Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7755-3071

ПРОТОКОЛИ, МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ НА ТРАНСПОРТНОМУ РІВНІ

Вступ і постановка проблеми. В останнє десятиліття широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управлінні процесами призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах OSI (Open System Interconnection). Особливістю протоколів транспортного рівня таких систем, є відсутність перевірки джерел інформації, що сприяє таким загрозам, як перехоплення та підключення до відкритих портів протоколів транспортного рівня.

Захист від перехоплення потребує застосування додаткових протоколів, які підтримують шифрування даних та автентифікацію суб'єктів обміну даними. Для вирішення цієї задачі використовується протокол SSL/TLS (Secure Socket Layer / Transport Layer Security), який реалізує шифрування і автентифікацію між транспортними рівнями приймача і передавача.

Процедура роботи протоколу SSL/TLS включає в себе три основних фази: