JEL Classification: E42

Деркач Юлія Борисівна
к.е.н, доцент кафедри банківської справи
Сушарник Микола Олегович
студент факультету менеджменту,
обліку та інформаційних технологій
Одеського національного економічного університету

РИЗИКИ ШАХРАЙСТВА З ПЛАТІЖНИМИ КАРТКАМИ ТА МЕТОДИ ЇХ ЗНИЖЕННЯ

Тези присвячено ризикам шахрайства з платіжними картками у банківській сфері. Розглянуто основні види шахрайства, умови виникнення та запропоновано методи щодо їх зниження.

Ключові слова: *платіжні картки, ризики шахрайства, банківська сфера, скімінг, фішинг.*

В даний час, в умовах прискореного розвитку національних платіжних систем останніми роками збільшується важливість розробки та прийняття законодавства, що регулює безготівкові роздрібні платежі. Існування спеціального регулювання стає необхідною умовою модернізації платіжної інфраструктури з підвищенням інформаційної безпеки.

Окремі аспекти цієї теми є головним напрямком наукових досліджень про сучасне бачення проблеми багатьох вітчизняних та зарубіжних вчених. В умовах сьогодення, банківські картки є одним із ключових компонентів безготівкових розрахунків, які активно витісняють готівку. Головною особливістю є те, що карта включає певну інформацію, яка необхідна для доступу до банківського рахунку, здійснення розрахунків за товари та послуги, а також зняття готівки, саме це дозволяє їй служити простим та сучасним засобом безготівкових розрахунків та одночасно бути привабливим об'єктом для шахраїв.

За даними Української міжбанківської асоціації членів платіжних систем ЕМА за 2020 рік шахраям із застосуванням платіжних карток вдалося викрасти щонайменше 271,4 мільйонів гривень. Середня сума шахрайської операції в Інтернеті у 2020 році склала 198 гривень, завдяки методам соціальної інженерії українці втрачали в середньому 2400 гривень, а ось викрадення SIM-картки могло обернутися втратою близько 12 500 гривень з платіжної картки [1].

Процес безготівкових платежів по суті досить складний та здійснює миттєвий доступ до платіжної системи, який може стати предметом маніпуляції правопорушників з метою шахрайських дій. В цьому зв'язку важливо встановити, яка саме ланка в ланцюжку учасників платіжної системи відповідає за заподіяння збитку клієнту у разі неправомірних списань. Особливу актуальність, таким чином, набуває проблема розподілу відповідальності у разі здійснення несанкціонованих операцій, здійснених з використанням платіжних

карток. Від успішності вирішення цього завдання насамперед залежить рівень довіри громадян до існуючої платіжної інфраструктури [1, с. 92].

Платіжна банківська картка – це персоніфікований платіжний інструмент, що надає особі, можливість безготівкової оплати товарів або послуг, а також отримання готівки у відділеннях банків та банківських автоматах. Прийом картки до оплати та видача готівки за нею здійснюються на підприємствах торгівлі, сервісу та банках, що входять до платіжної системи, яка здійснює обслуговування картки.

Виділяється два основних види платіжних карток: кредитні картки; дебетові картки, що прив'язані до окремого депозиту. Також, можна відмітити передплачені картки – анонімні, доступні для загального використання картки, де вартість зберігається на окремому для кожної картки депозиті, або прив'язані до закритої системи (наприклад, подарункові картки певних рітейлерів). Дебетові та передплачені карти часто мають можливість застосування ПІН-коду для перевірки автентичності користувача, а кредитних картах для цих цілей в основному використовується магнітна смуга. Платіжні картки через об'єктивні фактори сприйнятливі до різноманітних шахрайських атак. Шахрайство в сфері платіжних карток може бути визначено як будь-яка діяльність, яка використовує приватну конфіденційну інформацію для незаконних цілей, включаючи ініціацію протизаконних транзакцій без авторизації платника [2].

Методами захисту банківських карток є збереження конфіденційності певної інформації про карту, верифікаційний код та PIN - код. Відповідно до цього прийоми, які застосовують шахраї, орієнтовані на добування цієї інформації або отримання доступу до коштів на карті в обхід неї. До способів шахрайства з банківськими картами, які стали класичними, можна віднести:

1. Фішинг – вид шахрайства, що полягає в підробці правопорушниками сайтів, подібних до офіційних сторінок кредитних організацій, на яких пропонують залишити клієнтам конфіденційну інформацію про себе. Інший варіант - поширення поштою або за допомогою фальшивих SMS - повідомлень від банків із проханням надати номер картки. Прийнявши надану інформацію, крадуть кошти з карток.

2. Скімінг – крадіжка даних картки за допомогою спеціального приладу, що зчитує інформацію. Скімер - невеликий пристрій, що встановлюється в карт-датчик банкомату і зчитує дані з магнітної смуги банківської картки (номер картки, ім'я, прізвище, термін дії, верифікаційний код, навіть в окремих випадках PIN - код). Стати жертвою скімінгу можливо не лише знімаючи готівку, а й оплачуючи товари.

3. Вішінг – вид шахрайства, за допомогою якого зловмисник отримує інформацію про банківську картку жертви. Власнику карти дзвонить шахрай, прикидаючись співробітником банку, для цього також може бути використаний автоінформатор та під будь-яким переконливим приводом просить повідомити конфіденційні дані картки [2-3].

Останні тенденції на світовому платіжному ринку свідчать про те, що відбувається міграція шахрайства з «банкоматного сектора» до сектору інтернет-торгівлі. В табл. 1 наведено основні напрями запобігання шахрайства.

Таблиця 1

Напрями запобігання шахрайству з використанням платіжних карток

Механізм шахрайських дій	Характетистика напряму
Використання банківських платіжних карток для здійснення незаконних угод	Моніторинг «підозрілих операцій» та негайне повідомлення банку для перевірки законності угоди
	Консультації з працівниками банку для роз'яснення прав та обов'язків, пояснення співпраці при проведенні моніторингу
Використання незаконно скопійованої з банківської картки інформації для створення підроблених платіжних карток	Моніторинг «підозрілих операцій»
	Моніторинг банкоматів та терміналів з метою недопущення встановлення скімінг-пристроїв
	Консультації з працівниками банку для роз'яснення прав та обов'язків

У разі здійснення шахрайства з карткою клієнта існує два напрями дій з боку банку: 1) визнання банком злочинна та повернення клієнту грошових коштів; 2) кваліфікація виконаної операції, як шахрайства з боку клієнта. Правом банку у такому разі є звернення у правоохоронні органи. Факт шахрайства має бути доведений у суді.

Також, можна виділити методи зниження ризиків шахрайства з платіжними картками зі сторони банківських установ, а саме:

1. Порівнювати операції проведенні з платіжними картками. Операції порівнюються з операціями у торговій точці за обумовлений період. Операція не зіставлена за деяким алгоритмом, вона відкладається з обробки до закінчення розслідування. Звичайно, немає сенсу розслідувати всі випадки підозрілих операцій. Розумним є застосування порогових лімітів: сума операції, сума операцій протягом дня, тижня. Усі події перевищення лімітів можна посилати на розслідування та за результатами процесування операцій.

2. Використовувати технології SMS-повідомлення власників платіжних карток про авторизаційні запити на проведення операцій за їх картками. Метод дуже ефективний, оскільки клієнт самостійно забезпечує моніторинг особистих коштів на карт-рахунку.

3. Надати клієнтам право додаткової автентифікації або двофакторної автентифікації, а також гарантію підтримки механізму електронно-цифрового підпису під час виконання різноманітних фінансових операцій.

4. Ввести особливий антискімміновий модуль безпеки, який ставиться на банкомат. Цей модуль обладнаний спеціальними датчиками для контролю ділянки карто приймача, який дозволяє виявляти установку на банкомат будь-яких сторонніх пристроїв. У разі виявлення несанкціонованого доступу до

банкомату негайно надсилається попередження у відповідні служби. При цьому банкомат блокується для проведення операцій, а камера фіксує особу шахрая.

5. Надати доступ до мобільного банку для того, щоб клієнт у режимі онлайн міг контролювати стан свого рахунку.

Крім цього безпосередньо клієнт банку повинен дотримуватися правил користування та зберігання картки, не зберігати карту та пін-код разом. При розрахунку різних покупок через Інтернет, необхідно завести нову карту, яка буде призначена лише для таких операцій. Не слід тримати велику суму на ній, тому що відомо багато випадків, коли продавці різних Інтернет-магазинів дізнаються всі необхідні дані, нібито для переказу грошей за будь-який товар, знімають певну суму, але товар надалі потерпілому не відправляється. Також, не слід повідомляти пін-код та інші дані третім особам, навіть якщо телефонують та представляються працівником банку [4-5].

Таким чином можна зробити висновок, що шахрайські схеми та маніпуляції в банківську сферу з кожним роком все більше вдосконалюються, тим самим підриваючи стійкість та економічну безпеку країни. Шахрайство з банкоматами та банківськими платіжними картками тягнуть за собою негативні наслідки в вигляді гальмування поширення безготівкової форми оплати, яка є запорукою формування глобальної фінансової системи. Підвищена кримінальність безготівкового проведення розрахунків, обумовлена як соціально економічними, так і іншими об'єктивними та суб'єктивними факторами, зокрема: швидке та неконтрольоване використання платіжних систем та відсутність ефективних засобів охорони, що забезпечують повну безпеку банківських карток.

Список використаних джерел

1. ЕМА: веб-сайт. URL: https://www.ema.com.ua/ (дата звернення: 16.05.2022)

2. Олійничук О. Банківські картки як об’єкт шахрайства: стан і протидія явищу. Актуальні проблеми правознавства. 2017. №1. С. 91–94.

3. Домінова І. В. Ризик шахрайства в умовах функціонування електронного банкінгу. Науково-виробничий журнал «Бізнес-навігатор». 2017. №4. С. 92–98.

4. Коцан-Олинець Ю. Я. Види шахрайства з банківськими картками та способи протидії їх проявам. Вісник Львівського торговельно-економічного університету. 2019. №8. С. 95–100.

5. Портал Національного Банку України. Офіційний сайт Національного банку України. URL: https://promo.bank.gov.ua/stopfraud/#section-3 (дата звернення: 21.04.2022).