

**Олександра Олійничук,**  
кандидат економічних наук, доцент  
кафедри економічної безпеки  
та фінансових розслідувань  
Тернопільського національного  
економічного університету

## **БАНКІВСЬКІ КАРТКИ ЯК ОБ'ЄКТ ШАХРАЙСТВА: СТАН І ПРОТИДІЯ ЯВИЩУ**

*Проаналізовано обсяги шахрайства із банківськими картками в Україні протягом останніх років. Відображено світові тенденції досліджуваного явища. Охарактеризовано основні способи карткового шахрайства. Висвітлено аспекти діяльності Української міжбанківської асоціації членів платіжних систем «ЕМА» у напрямі запобігання даному виду шахрайства. Окреслено шляхи протидії злочинам з банківськими картками.*

**Ключові слова:** банківська картка, шахрайство, способи шахрайства, злочин, відповідальність, кримінальне законодавство.

**Олійничук А.**

**Банковские карты как объект мошенничества: состояние и противодействие явлению**

*Проанализировано объемы мошенничества с банковскими картами в Украине в последние годы. Отражены мировые тенденции изучаемого явления. Охарактеризованы основные способы карточного мошенничества. Освещены аспекты деятельности Украинской межбанковской ассоциации членов платежных систем «ЕМА» в направлении предотвращения данного вида мошенничества. Определены пути противодействия преступлениям с банковскими карточками.*

**Ключевые слова:** банковская карточка, мошенничество, способы мошенничества, преступление, ответственность, уголовное законодательство.

**Oliynychuk O.**

**Bank cards as a fraud object: state and combating the phenomenon**

*The volume of card fraud in Ukraine in recent years was analyzed in the article. The world trends of the phenomenon were shown. The basic methods of card fraud were characterized. The aspects of the Ukrainian Interbank Association of Payment Systems Members «ЕМА» activity toward preventing the card fraud were highlighted. The ways of combating the card fraud were defined.*

**Keywords:** bankcard, fraud, methods of fraud, crime, responsibility, criminal law.

**Постановка проблеми.** Перехід на безготівкову оплату – мета розвитку багатьох фінансових систем світу. Безготівкові розрахунки з використанням банківських карток допомагають зробити сферу комерції максимально прозорою як для покупця, так і для продавця. Крім того, це спосіб уникнення багатьох видів фінансового шахрайства і захисту екології планети. Водночас із зростанням популярності розрахунків через банківські картки збільшується і кількість шахрайських спроб використання даних карткових користувачів для незаконного збагачення. Так, сума знятих кібершахраями коштів з електронних платіжних карток українців в 2016 р. порівняно з 2015 р. збільшилася в 4 рази – до 339,13 млн. грн. Крім того, сума втраг користувачів банківських карток від шахрайських операцій в Інтернеті за результатами 2016 р. збільшилася в 2 рази – до 63,68 млн. грн. [13]. Банківські установи також зазнають значної шкоди від таких дій, адже несуть певну відповідальність при здійсненні операцій за допомогою платіжної картки, якщо йдеться про операції, які, за твердженням користувачів, не були ними погоджені, про що вони повідомили банк-емітент. Тому дослідження питань шахрайства з банківськими картками та протидії цьому явищу є надзвичайно актуальним в умовах розвитку інформаційних технологій в банківському секторі та поширення їхнього використання.

**Аналіз останніх досліджень і публікацій.** Різні аспекти дослідження новітніх шахрайських дій з використанням сучасних програмно-технічних засобів, зокрема в банківському секторі, окреслено у багатьох працях останніх років. Так, Т. В. Романенко, С. В. Шапочка висвітлили питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет [10; 14]. С. В. Поперешняк розглянув основні ризики, що супроводжують карткові технології та методи захисту учасників карткових операцій [7]. С. В. Самойлов описав типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі Інтернет, відповідні їм слідчі версії та алгоритми їх перевірки [11]. Однак стрімкий розвиток шахрайських технологій актуалізують наукові пошуки засобів боротьби зі злочинністю у сфері використання банківських карток.

© Олександра Олійничук, 2017

**Цілями даної статті** є дослідження поточних обсягів і способів шахрайства із банківськими картками, а також окреслення шляхів протидії даному явищу.

**Виклад основного матеріалу дослідження.** Банківська платіжна картка – це персоналізована пластикова картка з магнітною смугою або чіп-модулем, яка є ключем доступу до управління банківським рахунком і надає її власнику можливість безготівкової оплати товарів або послуг в різних торгових і сервісних підприємствах, що приймають картки до оплати, одержувати готівку у відділеннях банків і в банкоматах, а також користуватися іншими додатковими послугами та певними перевагами. З'явившись в середині минулого століття, банківські картки набули поширення більш, як в 200 країнах світу і стали невід'ємним атрибутом цивілізованої людини [6, с. 43].

На даний час банківські картки є основним елементом електронних банківських систем, все більш активно витісняючи традиційні чекові книжки та готівку. Та особливість, що картка містить певну інформацію, яка потрібна для доступу до банківського рахунку, здійснення розрахунків за товари та послуги, а також зняття готівки, дозволяє їй слугувати простим і прогресивним засобом в організації безготівкових розрахунків і водночас бути привабливим об'єктом для шахрайських операцій з боку злочинців.

Останнім часом шахрайство з банківськими картками має зростаючу тенденцію не тільки у світі, але й в Україні. Як зазначає В. Некрасов з посиланням на дані консалтингової компанії Gemius, частота зіткнення із шахрайством з банківськими картками в Україні збільшилась (табл. 1) [3].

Таблиця 1

**Частота зіткнення із шахрайством з банківськими картками в Україні, %**

Категорії опитаних	2014 р.	2016 р.	Тенденція (+/-)
Особисто стикались	3	12	+
Стикались мої друзі, знайомі, родичі	12	37	+
Чули по ЗМІ, але я і мої друзі не стикались	76	47	-
Не чули про таке шахрайство	8	2	-
Важко сказати	1	2	+

Джерело:[3].

Отже, відповідно до результатів дослідження, проведеного компанією Gemius, протягом 2014–2016 рр. в Україні в 4 рази збільшилась кількість осіб-користувачів банківських карток, які особисто стикнулись із шахрайством. Водночас варто відзначити, що аналогічний показник в інших країнах світу є значно вищим (табл. 2).

Таблиця 2

**Кількість респондентів, які стикнулись із шахрайством з банківськими картками у світі, %**

№п/п	Країна	2016	Динаміка 2014–2016 рр.
1	Мексика	56	+23
2	Бразилія	49	+19
3	США	47	+6
4	Австралія	40	+9
5	Індія	37	+4
-//-	-//-	-//-	-//-
16	Нова Зеландія	20	+3
17	Німеччина	18	+2
18	Швеція	14	+4
19	Нідерланди	14	+1
20	Угорщина	9	н/д

Джерело:[3].

Як свідчать дані табл. 2, шахрайство із банківськими картками набирає обертів і стає поширеним видом діяльності зловмисників. Його найбільш популярними видами є фішинг, вішинг, скіммінг та шиммінг. За видами злочинів у банківській сфері вони відносяться до злочинів, що вчиняються в основному не банківськими працівниками, а іншими особами, які володіють відповідними знаннями і технічними навичками [4, с. 59].

Концепція фішингу (англ. fishing – риболовля) полягає у тому, що шахрай будь-якими можливими способами намагається витягнути з власника картки інформацію. Це може бути підроблений лист, наприклад, від банку або платіжної системи, клієнтом якої є власник, із проханням так чи інакше повідомити інформацію, за допомогою якої шахрай може одержати доступ до коштів – запит PIN-коду, логіна, пароля

тощо. Найпростіший спосіб фішингу – підробка листа. Користувач одержує листа з пропозицією перейти за посиланням, адреса якого схожа на адресу відомої користувачу компанії. Якщо користувач перейде за посиланням та вкаже дані доступу, які звичайно використовує для доступу до Інтернет-банкінгу або особистого кабінету, його персональні дані стануть доступними шахраям [1].

Вішинг (від англ. voice – «голос»; fishing – «риболовля») – вид шахрайства з банківськими картками, що значно поширився в Україні протягом останніх років. Це один з методів шахрайства з використанням соціальної інженерії. Він полягає в тому, що зловмисники, граючи роль співробітника банку або покупця, випитують по телефону у власника платіжної картки конфіденційну інформацію або провокують до здійснення певних дій зі своїм картковим рахунком. У 2016 р. шахраї за допомогою вішингу обікрали карткові рахунки українців на 275 млн. грн. Втрати від цього виду кібершахрайства ростуть небаченими темпами. За 2016 р. дохід шахраїв виріс більш, ніж в п'ять разів з 51 млн. грн. в 2015 р. Якщо тенденція збережеться, то в кінці 2017 р. кожен 30-й українець стане жертвою вішингу [3].

Одним із способів викрадення коштів з банківської картки є скіммінг (англ. skimming – «знімання вершків»). Скіммер – невелике пристосування для зчитування інформації з магнітної стрічки, яке вміщається в долоні і може вмістити в себе до 200 номерів карток. Зі скіммера дані перевантажуються на комп'ютер, а з нього за допомогою спеціального декодера – на магнітну стрічку викраденої, знайденої або незаконно виготовленої картки. Інформація, яка міститься на магнітній стрічці, потім витискається на картці і ніякого додаткового обладнання чи витрат ця операція не потребує. Скіммери використовуються, як правило, особами, що приймають картки до оплати – офіціантами, адміністраторами, касирами, які копіюють дані з картки два рази – один для оформлення платежу, другий – на скіммер для злочинців [5]. Як варіант, на банкомат прикріплюють мініатюрну відеокамеру, яка знімає руку, що вводить пін-код, і робить запис у модуль пам'яті або передає його дистанційно на комп'ютер шахрая. Загалом у випадку дистанційної передачі шахрай знаходиться недалеко та приймає відеодані за допомогою ноутбука [12].

Шиммінг є різновидом скіммінгу і останньою з вигадок викрадачів, одним із способів незаконного зняття грошей за допомогою використання тонкої плівочки, схожої на скотч. Така плівка наклеюється на клавіатуру, а потім із неї зчитується необхідна інформація. Незвичайна клавіатура банкомата не викликає підозри, що значно полегшує завдання злочинцям [5].

З метою протидії вищезазначеним злочинним діям в Україні 19 березня 1999 р. українськими банками, членами платіжної системи Euroray International була створена Асоціація «ЕМА». З 11 листопада 2004 р. Асоціація має назву Українська міжбанківська асоціація членів платіжних систем «ЕМА». Ця структура взаємодіє з членами міжнародних платіжних систем та інших систем, що використовують платіжні картки, електронні засоби платежів і працюють за загально визначеними міжнародними або галузевими стандартами.

Асоціація функціонує у напрямі вирішення трьох основних завдань:

1. Забезпечення взаємодії з державними органами (НБУ, КМУ, ВРУ, АМКУ, Держфінмоніторинг, МВС), представлення та захист в державних органах законних прав та інтересів членів Асоціації (і їх клієнтів) в сфері безготівкових розрахунків та кредитування, юридичних і технологічних питань роздрібного бізнесу.

2. Удосконалення системи колективної безпеки та спільні заходи щодо запобігання шахрайським діям і відмиванню коштів з використанням платіжних інструментів та електронних засобів розрахунку, розвитку механізму кредитного ризик-менеджменту.

3. PR-активність для популяризації безготівкових розрахунків, кредитування та електронної комерції, роз'яснювальна робота про заходи та засоби безпечного використання платіжних і кредитних інструментів; перепідготовка співробітників банків і представників державних органів, відповідальних за безготівкові розрахунки, кредитування, електронну комерцію, а також захист і безпечне використання платіжних і кредитних інструментів [9].

Отже, діяльність Асоціації «ЕМА» відіграє значну роль у запобіганні картковому шахрайству. Серед шляхів протидії даному виду зловмисної діяльності в Україні також варто виділити наступні:

1) підвищення обізнаності громадян України про ефективні способи захисту власної інформації та правила безпечного використання платіжних карток, електронних платежів і банкоматів;

2) вдосконалення системи оперативного отримання та перевірки правоохоронними органами інформації про злочини з платіжними картками, електронними платежами і в банкоматах;

3) вдосконалення взаємодії між банками, патрульною поліцією, кіберполіцією і слідством при розслідуванні та протидії злочинам з платіжними картками, електронними платежами і з банкоматами;

4) підвищення обізнаності суддів і прокурорів про схеми скоєння злочинів з платіжними картками, інтернет-платежами і в банкоматах, аналіз судової практики та формування рекомендацій щодо кваліфікації карткових і платіжних злочинів;

5) удосконалення кримінального законодавства України в сфері неправомірного використання засобів платежу та приведення його у відповідність до світових стандартів і поширених видів карткових і платіжних злочинів [8].

Кіберзлочинці відчувають себе вільно не тільки завдяки низькому рівню фінансової грамотності українців, а й вельми лояльному кримінальному законодавству. В Україні шахрай при першій судимості несе відповідальність у вигляді лише штрафу. Водночас навіть ліберальний ЄС рекомендує за кібершахрайство призначати перше покарання у вигляді позбавлення волі не менш, ніж на один рік. В Іспанії за це можна отримати 12 років, в Польщі – до 25 років, в США – три-чотири довічні терміни. В Україні у 2016 р. потрапили до в'язниці лише десять шахраїв [3].

Слід відзначити, що в Україні слід запроваджувати світовий досвід щодо посилення захисту банківських карток. Так, для боротьби з картковим шахрайством оператори міжнародних платіжних систем розробили новий стандарт платіжних карток EMV (технологія ЧІП та ПІН), а також різні додатки безпеки, зокрема, додаток 3D Secure для операцій онлайн. Як свідчать дослідження, платіжну картку нового стандарту набагато складніше клонувати. Відповідно, вона є більш безпечною для користувачів і банків. У країнах Європи запровадження карток цього стандарту суттєво зменшило кількість традиційного шахрайства, пов'язаного з клонуванням карток. Отже, це має спонукати українські банки прямувати до нового стандарту, щоб знизити кількість оспорюваних користувачами транзакцій [2].

**Висновки.** Таким чином, шахрайство з банківськими картками має значні негативні наслідки для стабільності фінансової системи держави, оскільки гальмує поширення безготівкової форми оплати, яка є визнаним пріоритетом розвитку світової фінансової системи, а також завдає значної економічної шкоди для різних суб'єктів господарських процесів. Тому активна боротьба із даним проявом кіберзлочинності – це нагальна вимога часу, що потребує консолідації зусиль банківських установ, правоохоронних органів, громадських організацій та, звичайно, користувачів банківських карток.

#### Список використаної літератури

1. Абрамов К. Інтернет-шахрайство з платіжними картками та методи захисту від нього [Електронний ресурс] / К. Абрамов. – Режим доступу : [http://www.ufin.com.ua/analit\\_mat/poradnyk/094.htm](http://www.ufin.com.ua/analit_mat/poradnyk/094.htm).
2. Глотов М. Как защитить свои деньги на карточке [Электронный ресурс]. [Электронный ресурс] / М. Глотов. – Режим доступа : <https://www.epravda.com.ua/rus/columns/2015/07/8/549843/>.
3. Некрасов В. Атака по телефону: Украину накрыла волна кибермошенничества [Электронный ресурс] / В. Некрасов. – Режим доступа : <https://www.epravda.com.ua/rus/publications/2017/01/30/619178/>.
4. Олійничук О. І. Правові основи протидії економічній злочинності: навч. посіб. / О. І. Олійничук. – Тернопіль : ФОП Шпак В. Б., 2016. – 242 с.
5. Осика І. М. Огляд Міжнародного науково-практичного семінару «Протидія економічній злочинності» [Електронний ресурс] / І. М. Осика. – Режим доступу : [http://www.univd.edu.ua/\\_projects/ezloch\\_kor/docs/zahid/oglyad.doc](http://www.univd.edu.ua/_projects/ezloch_kor/docs/zahid/oglyad.doc).
6. Пиріг С. О. Платіжні системи : навч. посіб. для вузів / С. О. Пиріг. – К. : ЦУЛ, 2008. – 239 с.
7. Поперешняк С. В. Ризики та алгоритми захисту сучасних банківських карткових технологій / С. В. Поперешняк // Вісник соціально-економічних досліджень. – 2013. – Вип. 2(2). – С. 60–67.
8. Посольство США. Украинская межбанковская ассоциация членов платежных. [Электронный ресурс]. – Режим доступа : <https://ema.com.ua/about-association/association-members-partners/partners/embassy-of-the-usa/>.
9. Результаты работы. Украинская межбанковская ассоциация членов платежных систем. [Электронный ресурс]. – Режим доступа : <https://ema.com.ua/about-association/history-of-organization/>.
10. Романенко Т. В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет / Т. В. Романенко // Молодий вчений. – 2016. – № 1(2). – С. 51–54.
11. Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки / С. В. Самойлов // Проблеми правознавства та правоохоронної діяльності. – 2014. – № 4. – С. 25–31.
12. Скімінг у банкоматах. [Електронний ресурс]. – Режим доступу : <http://www.chclub.ru/skimmingatm>.
13. У 2016 році кібершахраї вкрали з карток українців 339 мільйонів [Електронний ресурс]. – Режим доступу : <https://www.epravda.com.ua/news/2017/01/26/618965/>.
14. Шапочка С. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет/ С. Шапочка // Правова інформатика. – 2014. – № 3. – С. 89–95.

Стаття надійшла до редакції 20.04.2017.