

**Кушнерьов Олександр Сергійович,**

*аспірант кафедри економічної кібернетики,*

*Навчально-науковий інститут бізнес-технологій "УАБС", м. Суми*

**Яценко Валерій Валерійович,**

*к.т.н., доцент кафедри економічної кібернетики,*

*Навчально-науковий інститут бізнес-технологій "УАБС", м. Суми*

## **АНАЛІЗ ТЕНДЕНЦІЙ ПРОВЕДЕННЯ ШАХРАЙСЬКИХ ОПЕРАЦІЙ З ТРАНЗАКЦІЯМИ НА БАНКІВСЬКОМУ РИНКУ УКРАЇНИ**

На сьогоднішній день шахрайські операції здійснюють негативний вплив на діяльність банків, а шахрайських схем на сьогодні безліч, і вони урізноманітнюються, по мірі розвитку банківських технологій. Збільшується кількість банківських інструментів, розвивається Fin Tech – одночасно виникають високотехнологічні шахрайські схеми, де зловмисники використовують винайдені ними методи.

Таким чином, саме шахрайські операції з транзакціями можна охарактеризувати як найбільш технологічні, оскільки, якщо, наприклад, кредитне шахрайство пов'язане з фальсифікаціями, що мають кінцеву ланку (виконавця), то транзакції здебільшого дозволяють зберегти анонімність виконавця, що значно ускладнює повернення викрадених коштів та притягнення винних до відповідальності.

Дослідження показали, що найефективнішим способом боротьби з шахрайством є недопущення або мінімізація можливостей здійснення шахрайських операцій з транзакціями. Для цього потрібен постійний моніторинг та вивчення особливостей їх здійснення, аби запобігти поширенню того чи іншого шахрайського методу. Це вимагає постійної уваги дослідників до даної проблеми.

За даними Асоціація членів платіжних систем ЄМА, на українському банківському ринку домінують методи, пов'язані з так званою соціальною інженерією, а також шахрайські операції в мережі Інтернет. Розглянемо найбільш розповсюджену технологію шахрайства в мережі Інтернет.

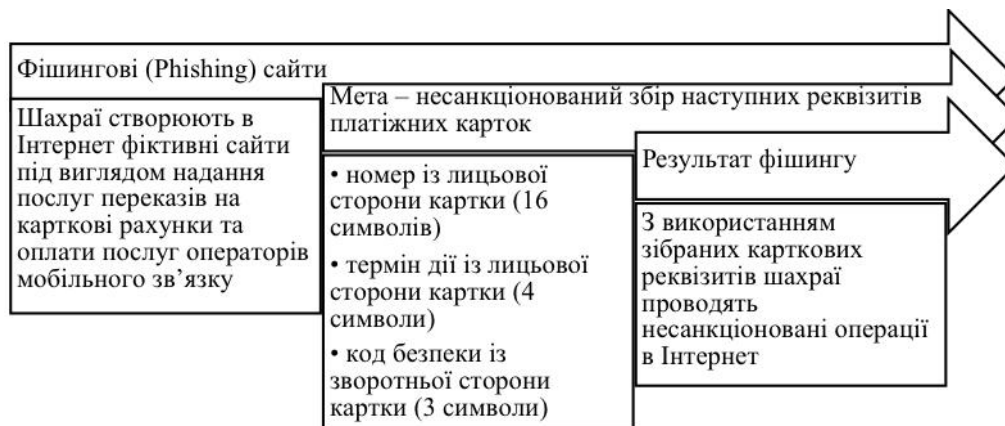


Рис. 1. Технологія фішингу, направлена на держателів платіжних банківських карт в мережі Інтернет [1]

Для протидії фішингу банки застосовують систему подвійного захисту з підтвердженням транзакції за допомогою одноразового паролю, який надходить на телефон користувача картки. Тому ефективний фішинг щодо банківських транзакцій можливий лише при умові «перехоплення» фінансового номеру телефону.

Технології соціальної інженерії значно більш чисельні (рис. 2).

|   |   |
|---|---|
| Вішинг (Vishing)                                | • Шахраї телефонують власникам карток з метою отримання їх карткових реквізитів та ідентифікаційних даних для проведення шахрайських операцій в Інтернет або з метою стимулювання жертви здійснити переказ коштів на картковий рахунок шахрая |
| Смішинг (Smishing)                              | • Шахраї надсилають SMS, щоб ініціювати подальшу комунікацію з власником картки за допомогою телефону (вішинг)  |
| Фіктивні продавці                               | • Під виглядом справжніх продавців шахраї отримують передплату за неіснуючі товари на платіжні картки та мобільні телефони  |
| Фіктивні покупці                                | • Під видом покупців шахраї вивідують у продавців (переважно, за приватними оголошеннями про продаж) реквізити платіжних карток   |
| Несанкціоноване використання фінансового номеру | • Шахрайський перевипуск SIM-карти власника платіжної картки з метою отримання кодів та паролів безпеки, які банк направляє клієнту для підтвердження фінансових операцій   |

Рис. 2. Основні види технологій соціальної інженерії, направлені на держателів платіжних банківських карт в мережі Інтернет[2]

Дана технологія не обмежується лише перерахованими видами, а постійно поповнюється новими схемами. В цілому, усе різноманіття шахрайських схем, пов'язаних з транзакціями банківських операціями, можна звести до двох типів:

1. Комунікації з метою вивідування конфіденційної інформації держателів банківських карт.
2. Комунікації з метою виконання транзакцій на користь зловмисника самою жертвою.

Досить красномовною є динаміка об'ємів такого роду шахрайських операцій (рис. 3).

Слід відзначити різкий «стрибок» доходів шахраїв у 2016-2017 рр. Відповідно, ці суми складають збитки ошуканих держателів платіжних карт. У 2018 р. тенденція різкого росту зникає, і суми, вилучені шахраями у своїх жертв за допомогою фішингу знижуються з 159,91 млн. грн. до 4,89 млн. грн., а суми шахрайських операцій загалом за 2018 р. складають 270,92 млн. грн. проти 509,72 млн. грн. у 2017 р. Це пов'язано здебільшого з превентивними заходами технологій банківського захисту. Проте є й результат заходів рестриктивного характеру. Так, у 2016 р. до «чорних» списків внесені 1337 ІПН та 595 телефонних номерів, а в 2017 р. вже 2423 ІПН та 3430 телефонних номерів; 2018 р. – 2338 ІПН та 5139 телефонних номерів.

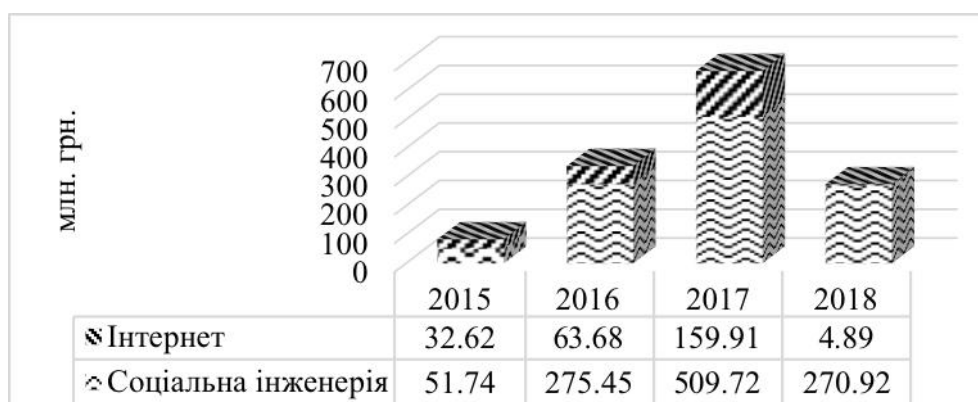


Рис. 3. Сукупний розрахунковий дохід шахраїв, млн. грн. [3]

Переходячи до аналізу сум шахрайських операцій, то соціальна інженерія характеризується більш значною сумою разової транзакції (рис. 4).

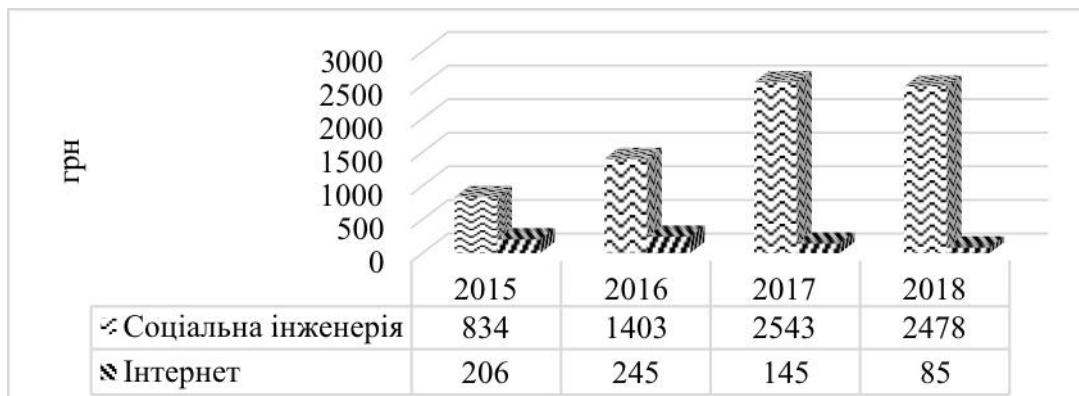


Рис. 4 - Середня сума шахрайської операції, грн. [3]

Тенденція до збільшення суми одиначної шахрайської транзакції в результаті застосування методів соціальної інженерії є тривожною, хоча така сума й дещо знизилася у 2018 р. (з 2543 грн. до 2478 грн.). Проте стійкий об'єм шахрайських операцій даного типу, а також порівняно значна сума окремої операції обумовлює винесення соціальної інженерії на перший план як найбільш небезпечної тенденції.

Таким чином, коли фінансові установи розширюють свої цифрові послуги, то шахраї також пристосовуються до цих змін. В Україні на даний час найбільшою небезпекою виступають шахрайські дії, пов'язані з соціальною інженерією. Не менш небезпечною, хоча й на даний момент не настільки розповсюдженою є проблема інтренет-шахрайства, оскільки розвиток фішингу стримують лише постійний контроль і моніторинг.

### Список використаних джерел

1. Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3>
2. Medium Corporation [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/@Emisare/socialnaya-ingeneria-9f16e0ba7fa5>

3. Офіційний сайт Асоціації ЄМА [Електронний ресурс] – Режим доступу до ресурсу: <https://ema.com.ua/>

Кушнерьов О. С., Яценко В. В. Аналіз тенденцій проведення шахрайських операцій з транзакціями на банківському ринку України : матеріали ІV Всеукраїнської науково-практичної on-line-конференції "Проблеми та перспективи розвитку фінансово-кредитної системи України", 21-22 листопада 2019 р. Сумі, 2019. С. 156–160.