Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ФІНАНСОВО-КРЕДИТНОЇ СИСТЕМИ УКРАЇНИ

МАТЕРІАЛИ
IV Всеукраїнської науково-практичної on-line-конференції
(Суми, 21–22 листопада 2019 року)

У двох частинах

Частина 1

Суми
Сумський державний університет
2019

Список використаних джерел

1. Про затвердження Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні. Постанова Правління Національного банку України від 22.11.2014 № 755. URL: https://zakon.rada.gov.ua/laws/show/v0755500-14

2. Річний звіт з оверсайта платіжних систем за 2018 рік. Національний банк України. 2019. 26 с.

УДК 343.5

Орєхова Катерина Віталіївна,
к.е.н., доцент,
Джанумян Едгар Артурович,
бакалавр,
Шихова Тетяна Вікторівна,
магістрантка,
Харківський навчально-науковий інститут
ДВНЗ «Університет банківської справи», м. Харків

ФІНАНСОВЕ ШАХРАЙСТВО В СУЧАСНИХ УМОВАХ

Стрімкий розвиток фінансових відносин, поширення глобалізаційних процесів, залучення інформаційних технологій та мережі Інтернет до обслуговування фінансових операцій спричинили активізацію економічної злочинності в Україні та, зокрема, такого її різновиду як фінансове шахрайство [4].

На основі аналізу фінансово-економічної літератури [1; 2; 3; 4; 5] встановлено, що ознаками фінансового шахрайства є:

— сфера посягання – фінансова сфера, тобто економічні відносини з формування, розподілу та використанню централізованих та децентралізованих фондів грошових коштів;

— специфічний суб'єкт злочинних посягань. Як правило, це фізичні особи-підприємці або посадові особи суб'єктів господарської діяльності, які мають необхідні знання бухгалтерського обліку, законодавства тощо;

— фінансове шахрайство є злочинною діяльністю; як правило, має складний механізм злочинних дій.

Фінансове шахрайство – це кримінологічне явище, що являє собою злочинну діяльність та виражається у системі кримінально-караних та легальних дій, які вчиняються шляхом обману або зловживання довірою в процесі формування, розподілу та використання грошових коштів з метою здобуття матеріальної вигоди [2].

Отже, в табл. 1 представлені сучасні види фінансового шахрайства в Україні [1; 3; 5].

Таблиця 1. - Сучасні види фінансового шахрайства в Україна

Вид	Характеристика
Скіммінг	Шахраї встановлюють на картрідер банкомату спеціальний зчитувальний пристрій, що копіює дані магнітної смуги банківської картки. Таким чином зловмисники отримують всі дані про пластик і можуть створити клон картки.
Кеш-трепінг	Для крадіжки готівки з банкоматів стали частіше використовувати спеціальні пастки, при виготовленні яких використовується двосторонній скотч. Він не дозволяє купюрам вийти назовні. Власник карти думає, що банкомат несправний, і йде ні з чим, а його готівка дістається шахраям.
Фізичні атаки	Із розвитком інформаційних технологій стали популярними логічні атаки на банкомати і термінали. Зловмисники встановлюють шкідливе програмне забезпечення на комп'ютер банкомату (локально чи віддалено через мережу) або підключають спеціальні пристрої, щоб управляти видачею грошей.
Соціальна інженерія та інтернет	Соціальна інженерія – збірна назва цілого ряду схем, за допомогою яких аферисти отримують доступ до закритої фінансової інформації банківських клієнтів. Часто жертви добровільно розкривають дані про свої рахунки, картки та інше. У соціальній інженерії безліч інструментів, серед яких: фейкові веб-сайти; телефонні дзвінки; фальшиві смс-повідомлення; фіктивні продавці;несанкціонований перевипуск sim-карти.

Продовження таблиці 1

Дублікат sim-карти	Користувачі прив'язують банківські сервіси, поштові аккаунти і соціальні мережі до номера мобільного телефону. Але біда в тому, що sim-карту можуть вкрасти разом із телефоном або відновити за номером. Шахраї використовують у своїх цілях облікові записи в соціальних мережах (Facebook, Instagram, Twitter), месенджерах (Viber, Telegram), Google акаунт, пошту, мультимедіа і, звичайно ж, BankID. Головна мета – гроші на вашому рахунку. Підробивши sim-карту, шахраї реєструються в мобільному додатку банку. Як тільки вони отримують доступ до рахунку жертви, відразу переказують гроші на свої рахунки інших банків. Банк надсилає одноразові паролі та смс-повідомлення про операції вже на новий фінансовий номер, який зареєстрував шахрай.
Ризики, пов'язані з переходом банків на IBAN	Перехід банків на міжнародний стандарт нумерації рахунків IBAN створив грунт для нового виду платіжного шахрайства. Зловмисники розсилають sms-повідомлення про те, що через перехід на новий стандарт банківський рахунок заблокований. Наведемо текст реального повідомлення від аферистів: Vash rakhunok zablokovano u zv'yazku z zaminou rozrakhunkovogo rakhunku. Balance 0.00.UAH 044*****. Мета шахраїв – налякати і змусити одержувача sms передзвонити на вказаний номер. Здійснюючи дзвінок, аферист представляється співробітником банку і виманює конфіденційні дані, щоб викрасти гроші своєї жертви.
Інциденти friendly-fraud	«Дружнім шахрайством» називають дитячу самодіяльність, яка зараз набирає обертів. Клієнти банків звертаються до фінансових установ зі скаргами на загадкові платежі, яких не робили. Під час розгляду справи з'ясовується, що це зовсім не шахрайство, а дитяча забаганка. Найбільш поширені випадки — оплата в інтернеті онлайн-ігор та послуг сайтів знайомств.
Фішинг	В інтернеті продовжують діяти фішингові сайти. Це фіктивні web-сторінки. Часто вони замасковані під реальні сервіси грошових переказів або оплати послуг мобільного зв'язку. Мета шахраїв – зібрати реквізити платіжних карт: номер, термін дії, код безпеки, що дасть їм можливість проводити з рахунків жертв несанкціоновані грошові операції в інтернеті.
Вішинг і смішинг	Телефонне шахрайство ділять на два види: вішинг і смішинг. У першому випадку банківські реквізити та ідентифікаційні дані виманюють під час телефонного дзвінка, у другому – через sms-повідомлення, яке штовхає жертву зателефонувати зловмисникам. Часто потерпілі самостійно здійснюють перекази грошей на картки аферистів.

Таким чином, для того, щоб захистити кошти на платіжним карткам рекомендовано вживати такі заходи:

1. Нікому не розголошувати конфіденційну інформацію: номер банківської картки, термін її дії, cvv-код, pin-код, логін і пароль інтернет-банку, інформацію з sms-повідомлення, фінансовий номер телефону.

2. Не телефонувати за номерами телефонів, вказаними у повідомленні, яке нібито надіслав банк. При виникненні питань бажано зв'язатися із співробітником банку за номером телефону, зазначеним на звороті карти або на офіційному сайті фінансової установи.

3. Встановлювати ліміти на суму транзакцій та геоліміти платіжних карток (обмеження за операціями одним містом, країною).

4. Не користуватися підозрілими сайтами. Не залишайте свої особисті дані в онлайн-анкетах.

5. Не прив'язувати публічний основний номер телефону до платіжної картки.

У випадку, якщо зловмисники отримали ваші конфіденційні дані, тоді рекомендовано вживати такі заходи:

- негайно зателефонувати до банку і заблокувати свій рахунок;
- заблокувати інтернет-банкінг;
- звернутися до співробітників кіберполіції.

Механізм попередження фінансового шахрайства застосовується для недопущення втрат фінансових ресурсів та передбачає врахування особливостей їх проявів на банківському ринку та прогнозів із їх поширення. Це є предметом подальшого дослідження авторів цього дослідження.

Список використаних джерел

1. Міністерство фінансів України: офіційний веб-ресурс. – Режим доступу: https://minfin.com.ua/.

2. Чернишов Г. М. До питання про визначення фінансового шахрайства / Г. М. Чернишов // Науковий вісник Ужгородського національного університету. Серія «Право». – 2014. – Випуск 26. – С. 230-234.

3. Войтенко І. С. Види шахрайств із використанням банківських платіжних карток та способи їх вчинення / І. С. Войтенко // Юридичний науковий електронний журнал. – 2018. – № 6. – С. 332-335.

4. Кізіма Т. Ідентифікація причин та потенційних наслідків фінансового шахрайства / Т. Кізима, А. Кізима // Вісник Тернопільського національного економічного університету. – 2019. – № 2. – С. 47-56.

5. Асоціація ЄМА: офіційний веб-ресурс. – Режим доступу: https://www.ema.com.ua/.

УДК 330.3:004.738.5(477)

Kozlovska Anna,
Candidate of Philological Sciences, Associate Professor
Student of the Pr.m-91 group ***Pavlenko Daria***
Sumy State University,
Sumy, Ukraine

DIGITAL ECONOMY: NEW OPPORTUNITIES AND PROSPECTS FOR UKRAINE

In the classical sense, digital economy is an activity in which digital data, both numerical and textual, are the main means of production [4, p. 73]. This is the economy based on digital computer technology, sometimes referred to as the new economy, the Internet economy or the web economy.

An economy that actively absorbs and uses digital technologies is called "digital." The digital economy means the sale, production and supply of products through computer networks. It is an essential driver of innovation, competitiveness and economic development. Our research *is aimed* at investigating new opportunities and prospects for Ukraine in terms of digital economy.

The use of digital data on a daily basis is a reference point for EU countries in the transition to the digital economy. This document was initiated in 2010 and provides a set of measures the ambitious goals of which will have been achieved by 2020. However, by 2015, some countries had begun reviewing and updating their