## *ПРОТИДІЯ ЗЛОЧИННОСТІ: ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ*

УДК 303.09:336.717.1 doi: https://doi.org/10.33270/01191134.8

***Черняк А. М.*** – доктор юридичних наук, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України, м. Київ
ORCID: https://orcid.org/0000-0002-4958-783X;

***Прозоров А. Ю.*** – кандидат юридичних наук, м. Київ
ORCID: https://orcid.org/0000-0003-0307-1659

# Аспекти запобігання правопорушенням у сфері використання банківських платіжних карток під час проведення безконтактних й інтернет-платежів та їх кваліфікація

***Метою*** *статті є визначення проблемних питань запобігання та кваліфікації злочинів, пов'язаних із використанням платіжних карток під час проведення безконтактних та інтернет-платежів, а також напрацювання відповідних рекомендацій.* ***Методологія.*** *Для дослідження проблематики використано методи формальної логіки та спеціально-правові методи: порівняльно-правовий, системно-структурний і системного аналізу.* ***Наукова новизна*** *публікації полягає в тому, що автори одними з перших комплексно дослідили проблемні питання запобігання, класифікації та кваліфікації злочинів, пов'язаних із використанням зловмисниками новітніх технологій для запровадження нових форм злочинної діяльності у сфері обігу платіжних карток під час проведення безконтактних та інтернет-платежів. У статті розглянуто особливості кваліфікації та запобігання правопорушенням у сфері використання платіжних банківських карток під час здійснення безконтактних платежів і платежів у мережі Інтернет. Констатовано, що застосування злочинцями новітніх технологій у проведенні відповідної протиправної діяльності створює нові виклики для правоохоронної системи й держави загалом. Увагу зосереджено на необхідності запровадження превентивного комплексу заходів реагування. Актуалізовано питання використання зловмисниками RFID-технологій для запровадження нових форм злочинної діяльності у сфері економіки. Узагальнено здобутки провідних іноземних й українських науковців щодо класифікації відповідної злочинної діяльності, з огляду на спорідненість злочинів в аналізованій сфері. Виокремлено проблемні аспекти надання правової оцінки залежно від об'єктивної та суб'єктивної сторін злочинних посягань. Зіставлено різні позиції стосовно криміналістичної характеристики таких виявів, увагу акцентовано на їх латентності.* ***Висновки.*** *Розглянуто такі види інтернет-шахрайства з використанням банківських платіжних карток, як фішинг, вішинг та фармінг. Визначено найпоширеніші з них у нашій державі: «розіграші і лотереї», «робота в Інтернеті», «фальшиві інтернет-крамниці» та «навчальні матеріали». Окреслено способи запобігання їм, мінімізації настання протиправних наслідків. Запропоновано заходи превентивного й реакційного спрямування для запобігання цій категорії злочинів у національній економіці.*

**Ключові слова:** електронний платіжний засіб; безконтактна банківська платіжна картка; банківський рахунок; фішинг; вішинг; фармінг.

### Вступ

Динамічний розвиток інформаційних технологій не лише сприяв оптимізації життя людей, а й призвів до появи нових викликів для економічної та інформаційної безпеки людини та держави. Останніми роками суттєво зріс рівень кіберзлочинності, зокрема у сфері використання платіжних банківських карток під час здійснення безконтактних та інтернет-платежів. З огляду на це, актуальності набуває питання запобігання злочинам у кіберпросторі. Ефективна нейтралізація їх потребує розроблення комплексу правових (законодавчих), технічних, організаційних та інформаційних заходів, спрямованих на зниження ризику таких злочинів і мінімізацію шкідливих наслідків для суспільства й особи.

Такі науковці, як А. Абрамова, Н. Данік, Н. Деркач, Н. Дребот, А. Жаворонок, Я. Коваль, І. Крівцун, Л. Павленко, В. Семенець, В. Сідак, Т. Тіхонова, М. Федишин у своїх працях висвітлювали аспекти функціонування банківської системи України й надання банківських послуг (Sidak, & Koval, 2018; Drebot, 2018; Fedyshyn, Abramova, Zhavoronok, & Marych, 2019; Kryvtsun, 2018; Danik, Tichonova, & Derkach, 2018; Pavlenko, & Semenets, 2019).

Дослідники О. Головко й О. Мороз увагу акцентували на проблемі впровадження та розвитку системи електронних платежів в Україні (Pavlenko, & Semenets, 2019).

Учені В. Густі та Т. Матковська вивчали питання функціонування програмно-апаратного комплексу для захисту RFID-міток банківських безконтактних платіжних карток на базі технологій PayPASS (MASTERCARD) ТА PayWAVE (VISA) від несанкціонованого зчитування (Husti, & Matyovka, 2018).

Дослідження правопорушень, що посягають на функціонування банківської системи, здійснили такі науковці, як О. Бущан, Д. Голосніченко, О. Джужа, О. Дудоров, А. Клочко, С. Кудінов, Г. Матусовський, В. Навроцький, В. Попович, С. Фальченко, С. Чернявський, В. Яні та ін. Зазначені вчені у своїх роботах розглядали особливості протидії злочинам у банківській сфері, що були притаманні різним періодам розвитку інформаційних технологій, відповідали певному періоду державо-творення. Виникнення нових кіберзагроз у банківській сфері, що можуть завдати істотної шкоди інтересам не тільки банків, а й людини, суспільства та держави, зумовлює потребу дослідити питання запобігання їм.

**Мета і завдання дослідження**

Мета статті – окреслити проблемні аспекти запобігання правопорушенням у сфері використання безконтактних банківських платіжних карток під час проведення безконтактних та інтернет-платежів, розглянути класифікацію їх, а також розробити рекомендації щодо запобігання таким правопорушенням.

**Виклад основного матеріалу**

Упровадження RFID-технологій (радіочастотна ідентифікація) у банківську систему, з одного боку, спростило процедуру розрахунків клієнтами за надані послуги й товари, а з іншого – зацікавило злочинців у контексті неправомірного поводження з безконтактними банківськими платіжними картками. Як наслідок – останніми роками в нашій державі, як і в більшості країн світу, поряд з раніше відомими видами шахрайства із засобами доступу до банківських рахунків, правоохоронні органи частіше фіксують факти вчинення протиправних дій з використанням безконтактних банківських платіжних карток.

Засобами доступу до банківських рахунків є платіжні доручення, платіжні вимоги, вимоги-доручення, векселі, чеки, банківські платіжні картки й інші дебетові та кредитові платіжні інструменти, що застосовують у міжнародній банківській практиці ("Zakon Ukrainy", 2001).

На думку вітчизняних науковців, шахрайства із засобами доступу до банківських рахунків можна класифікувати як: шахрайство з втраченими та викраденими пластиковими електронними картками; шахрайство з підробленими картками; шахрайство з картками, не отриманими законним держателем; шахрайство з використанням рахунка; інші форми шахрайств (Holubiv, Havlovskyi, & Tsymbal, 2002, p. 243).

Відповідно до ст. 190 КК України, шахрайство є корисливим злочином проти власності, що полягає в заволодінні чужим майном або придбанні права на майно шляхом обману чи зловживання довірою ("Kryminalnyi kodeks", 2001). Шахрайство з використанням банківських безконтактних платіжних карток окремо не належить до зазначеної класифікації, хоча стало доволі поширеним.

У Законі України «Про платіжні системи та переказ коштів в Україні» платіжну картку (payment card) визначено як електронний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовують для ініціювання переказу коштів з рахунка платника або відповідного рахунка банку з метою оплати вартості товарів і послуг, перерахування коштів зі своїх рахунків на рахунки інших осіб, отримання коштів у готівковій формі в касах банків через банківські автомати, а також здійснення інших операцій, передбачених відповідним договором ("Zakon Ukrainy", 2001; "Sait "Ofitsiine internet-predstavnytstvo"). Своєю чергою безконтактна банківська платіжна картка – це різновид банківської платіжної картки, у якій впроваджено RFID-чип. Технології безконтактної оплати товарів стали поширюватися в Україні з кінця 2000-х років.

На думку О. Дудорова, суспільно небезпечні посягання на власність, які вчиняють з використанням платіжних карток або їх реквізитів і які врешті-решт призводять до несанкціонованого законним держателем картки переказу грошових коштів з його рахунка, є підстави кваліфікувати не як крадіжку, а за ст. 190 КК України як шахрайство (Dudorov, p. 12). Об'єктивна сторона шахрайства характеризується тим, що потерпілий добровільно, унаслідок обману чи використання винним його довіри, передає грошові кошти злочинцю. Об'єктивна сторона крадіжки (ст. 185 КК України) характеризується вилученням чужого майна з володіння особи зловмисником усупереч волі потерпілого, без його згоди й таємно.

Правильна кваліфікація суспільно небезпечних діянь з безконтактними банківськими платіжними картками, об'єктом посягань яких є право власності, може гарантувати правомірне застосування положень КК України та справедливе притягнення злочинців до кримінальної відповідальності.

Суть такого протиправного механізму схожа на перехоплення сигналів електрозамків викрадачами автомобілів. Більшість суспільно небезпечних діянь з безконтактними банківськими платіжними картками з об'єктивної сторони полягають у прихованому списанні злочинцями коштів або отриманні конфіденційних даних щодо банківських рахунків з карт PayPass і PayWave за допомогою мобільних (хакерських) ридерів, здатних сканувати платіжні картки з чипами RFID на відстані до 20 см, усупереч волі потерпілого. Отримані в такий протиправний спосіб дані шахраї можуть надсилати на картки-копії для проведення незаконних фінансових операцій – передусім переказ або списання коштів.

Аналіз об'єктивної сторони зазначеної групи правопорушень, на нашу думку, дає підстави кваліфікувати їх не як шахрайство (ст. 190 КК України), а все ж таки як крадіжку (ст. 185 КК України), оскільки злочинці в цьому випадку не зловживають довірою потерпілого, він самостійно не здійснює переказ чи списання коштів з власного банківського рахунка. Фактично такі дії ззовні становлять приховане вилучення грошових коштів з володіння особи зловмисником усупереч волі потерпілого, без його згоди.

Неправомірно списані в зазначений спосіб гроші зараховують на конкретний банківський рахунок, що фактично надає можливість правоохоронним органам ідентифікувати його власника та згодом затримати. Водночас з метою уникнення відповідальності злочинці можуть використовувати банківські рахунки, що належать «підставним особам», а саме: зареєстровані на осіб, які надали згоду користуватися своїм паспортом і банківським рахунком третім особам за фінансову винагороду чи з інших мотивів; зареєстровані за підробленими та недостовірними документами шляхом введення в оману представників банку; дані, щодо яких були незаконно отримані злочинцями шляхом скіммінгу (використання накладок на клавіатуру або картридеру банкоматів) чи в інший протиправний спосіб та які ще не встигли заблокувати власники; зареєстровані чи отримані злочинцями в інший протиправний спосіб, зокрема із залученням співробітників банку.

У цьому контексті слід зазначити, що Національний банк України поступово проводить політику, спрямовану на зменшення кількості правопорушень у банківській сфері. Так, згідно з постановою правління НБУ від 7 квітня 2016 року № 242, станом на 11 липня 2017 року мінімальний обсяг статутного капіталу банку має бути не меншим за 200 млн грн. Відповідно до постанови правління НБУ від 21 грудня 2017 року № 136, Національний банк пом'якшив графік збільшення мінімального розміру статутного та регулятивного капіталу банків, і станом на 11 липня 2020 року розмір статутного капіталу має бути 300 млн грн, а 500 млн грн – з 11 липня 2024 року. Також НБУ активно вживав заходів щодо забезпечення прозорості структури власності банківських установ, перевіряв фінансовий стан кінцевих бенефіціарів, суттєво підвищив вимоги до ділової репутації банківського менеджменту та власників. Зазначене сприяло очищенню банківського сектору та зменшенню кількості банківських одиниць зі 180-ти до 82 банківських установ (Pavlenko, & Semenets, 2019).

На ринку банківських послуг банки масово не довіряють клієнтам через: наявність значної кількості шахрайств із боку фізичних осіб (надання неправдивих даних, неправильних телефонів тощо); зловживання юридичних осіб, що супроводжувалося процесами закредитованості й низьким рівнем кредитоспроможності; несформованість культури вчасно розраховуватися за власними зобов'язаннями; значна кількість випадків шахрайств менеджерів банківських установ, які видавали позики неплатоспроможним клієнтам, тощо (Golovko, & Moroz, 2018).

У ст. 200 КК України передбачено кримінальну відповідальність за підроблення документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей. Із цього приводу О. Дудоров стверджує, що безпосереднім об'єктом цього злочину є встановлений порядок проведення грошових розрахунків, виготовлення та обігу платіжних документів й інших засобів доступу до банківських рахунків, майнові права та інтереси юридичних і фізичних осіб – учасників розрахункових відносин, зокрема емітентів та держателів платіжних карток (Melnyk, & Klymenko, 2004).

Таким чином, зазначені протиправні дії з безконтактними банківськими платіжними картками мають також й ознаки складу злочину, передбаченого ст. 200 КК України ("Kryminalnyi kodeks", 2001). На нашу думку, знаряддям такого злочину є мобільний (хакерський) ридер, а предметом – грошові кошти, що можуть списувати шляхом використання безконтактних банківських платіжних карток.

Запобігти такій протиправній дії може фактично кожен власник безконтактної банківської платіжної картки самостійно, зберігаючи її у спеціальному гаманці (RFID blocking wallet) або використовуючи картки з чипами, які мають багатоступеневий захист, на відміну від тих, що мають лише магнітну стрічку.

Упродовж останніх років частка попиту з боку фізичних осіб на продукти дистанційного банківського обслуговування з доступом через Інтернет чи за допомогою мобільного зв'язку поступово зростає, що зумовлено ефективністю трансформації банківських продуктів та їх доступністю для населення в зручний час. Популярними стають мобільні додатки та їхні функціонали, спрощується процес підключення до онлайн банкінгу, дедалі активніше використовують для платежів новітні технології, наприклад, соціальні боти Facebook Messenger ("Zakon Ukrainy", 2001).

Інтернет-шахрайство з використанням банківських платіжних карток нині в Україні є надзвичайно поширеним явищем. До основних

його видів належать фішинг, вішинг і фармінг (хакерські дії).

Фішинг (англ. phishing, від fishing – «рибалка») – це вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів персональних даних клієнтів онлайнових аукціонів, сервісів з переказу чи обміну валюти, інтернет-магазинів ("Fishynh"). Об'єктивна сторона цього злочину полягає в тому, що зловмисники створюють власний сайт-клон відомого сайту, який пропонує товари або послуги, а доменне ім'я відрізняється від оригінального на один чи два символи. Під час замовлення продукту від клієнтів вимагають ввести реквізити їх банківської платіжної картки. Адміністратори таких сайтів здійснюють збір даних із карток потенційних покупців для подальшого проведення незаконних фінансових операцій, а товари й послуги не надають. Зафіксовано також випадки, коли інтернет-шахраї надсилали потерпілим електронні листи від імені авторитетних компаній з метою протиправного отримання персональних даних ("Fishynh").

За даними компанії PhishMe, станом на березень 2016 року 93 % всіх фішингових листів намагалися заразити комп'ютер жертви шкідливими програмами криптографічного здирництва (англ. ransomware) – вони шифрують дані на жорсткому диску та вимагають гроші від жертви за розшифрування їх. Також з-поміж стійких тенденцій до підвищення ефективності фішингових атак було виявлено випадки підлаштування вмісту листів під певну категорію жертв (за їхнім фахом) та із включенням певних елементів особистої інформації (зокрема, звернення до жертви за іменем) ("Fishynh"; "CSO Maria Korolov").

Вішинг (англ. vishing, від англ. voice – «голос», fishing – «рибалка») є різновидом інтернет-шахрайства, об'єктивна сторона якого полягає в тому, що зловмисники заволодівають у телефонному режимі, переважно вдаючи представників банку, конфіденційною інформацією про дані картки з її подальшим використанням для замовлення товарів чи послуг на інтернет-ресурсах або шляхом примушування до переказу коштів на картку злодіїв. Найчастіше його використовують для заволодіння коштами на банківських рахунках потерпілих, а також для проникнення до інформаційних систем приватних або державних установ, крадіжки конфіденційної інформації ("Vishynh").

Фармінг (англ. pharming) – це вид шахрайства, який полягає в організації зловмисниками злочинного механізму прихованого перенаправлення жертви на хибну IP-адресу, використовуючи навігаційну структуру (файл hosts, система доменних імен, DNS). Об'єктивна сторона такого злочину, як фармінг, є прихованим варіантом фішингу ("Farminh").

За результатами дослідження Української міжбанківської асоціації членів платіжних систем «ЕМА», понад половина випадків шахрайства припадає на шахрайські «розіграші і лотереї» (32 %) та «роботу в Інтернеті» (22 %), «фальшиві інтернет-крамниці» (18 %) та «навчальні матеріали» (15 %). Решта в сукупності становить лише 13 % ("Ukrainska mizhbankivska asotsiatsiia").

Аналіз об'єктивної сторони зазначеної групи правопорушень, на нашу думку, дає підстави кваліфікувати їх не як крадіжку (ст. 185 КК України), а все ж таки як шахрайство (ст. 190 КК України), оскільки злочинці в цьому випадку зловживають довірою потерпілого й він самостійно передає конфіденційну інформацію, пов'язану з його платіжною карткою, або здійснює переказ чи списання коштів з власного банківського рахунку. Фактично такі дії передбачають уведення зловмисниками в оману потерпілого, унаслідок чого він добровільно передає грошові кошти або конфіденційні дані для здійснення незаконних фінансових операцій.

Дискусійним залишається питання правової кваліфікації такого злочину, як фармінг. Об'єктивна сторона його полягає в тому, що процедуру отримання зловмисниками доступу до конфіденційної інформації, пов'язаної з банківським рахунком потерпілого, усупереч його волі в прихований спосіб через використання спеціального програмного забезпечення та здійснення незаконних фінансових операцій без його відома. Таким чином, незаконне вилучення грошових коштів зловмисниками з банківського рахунку потерпілого шляхом використання фармінгу в деяких випадках може бути кваліфіковано як крадіжка (ст. 185 КК України).

Окреслені різновиди інтернет-шахрайства з банківськими платіжними картками мають також ознаки складу злочину, передбаченого ст. 200 КК України ("Kryminalnyi kodeks", 2001). На нашу думку, знаряддям у цих злочинах можуть бути спеціальне програмне забезпечення, комп'ютерна техніка, засоби мобільного й інших видів зв'язку, а предметом – грошові кошти, що можуть незаконно списувати, а також конфіденційна інформація щодо банківської платіжної картки потерпілого, яка надає можливість отримати доступ до його банківського рахунку для проведення незаконних фінансових операцій.

До найпоширеніших способів запобігання інтернет-шахрайствам з використанням платіжних карток, що застосовують українські банки, належать такі: встановлення лімітів під час розрахунків і запровадження віртуальної банківської картки виключно для платежів через мережу

Інтернет; унікальний одноразовий пароль, який власник банківського рахунку отримує на мобільний телефон.

Серед основних заходів протидії кібер-шахрайствам дослідники Г. М. Яровенко й М. М. Бояджян пропонують розроблення та запровадження алгоритмів з використанням інструментів Data Mining, за допомогою яких відбуватиметься відслідковування операцій, перевірка їх на предмет шахрайства за певними ознаками. Дієвим є застосування нейронних мереж, що надасть можливість постійно налаштовувати систему на нові ознаки шахрайства. Тобто у випадку, коли шахрай знімає всю суму коштів з рахунка, система здійснює перевірку операції. У випадку шахрайства операція блокується ("Sait "Ofitsiine internet-predstavnytstvo").

Власник банківської платіжної карти може самостійно запобігти можливим шахрайським діям під час проведення платежів через Інтернет, зосередивши увагу на адресі в рядку браузера. Під час переходу безпосередньо до форми оплати він має містити літеру «s», а початок адреси буде виглядати так – «https://»; поруч з ним повинен бути символ «зелений замочок». Зазначене є свідченням того, що дані передають через захищений канал зв'язку. Також на сайті Асоціації членів платіжних систем є сервіс, який допомагає перевірити, чи підроблений сайт: https://ema.com.ua/report-an-incident/black-list/ ("Yak korystuvatysia", 2018).

## Наукова новизна

Наукова новизна публікації полягає в тому, що автори одними з перших комплексно дослідили проблемні питання запобігання, класифікації та кваліфікації злочинів, пов'язаних із використанням зловмисниками новітніх технологій для запровадження нових форм злочинної діяльності у сфері обігу платіжних карток під час проведення безконтактних та інтернет-платежів. Виокремлено її провідні форми в нашій державі та запропоновано превентивні й реакційні заходи реагування як складової відповідного комплексу.

## Висновки

У статті розглянуто такі види інтернет-шахрайства з використанням банківських платіжних карток, як фішинг, вішинг та фармінг. Визначено найпоширеніші з них у нашій державі: «розіграші і лотереї», «робота в Інтернеті», «фальшиві Інтернет-крамниці» та «навчальні матеріали». Окреслено способи запобігання їм, мінімізації настання протиправних наслідків. Запропоновано заходи превентивного й реакційного спрямування для запобігання цій категорії злочинів у національній економіці.

Застосування злочинцями новітніх інформаційних технологій у проведенні протиправної діяльності на шкоду особі, суспільству й державі ставить нові виклики перед нашою державою, що потребують розроблення та впровадження ефективного правового механізму запобігання правопорушенням у сфері використання безконтактних банківських платіжних карток та інтернет-платежів. У контексті зазначеного, з огляду на підвищення суспільної небезпечності злочинів аналізованої групи та їх поширеності, на нашу думку, поруч з іншими превентивними й реакційними заходами впливу на потенційних злочинців можна запропонувати посилити покарання шляхом внесення змін до санкцій ч. 1 та 2 ст. 200 КК України в частині заміни штрафу до десяти тисяч і двадцяти тисяч неоподатковуваних мінімумів доходів громадян відповідно.

### *REFERENCES*

CSO Maria Korolov 93% of phishing emails are now ransomware. (n.d.). *www.csoonline.com.* Retrieved from http://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html.

Danik, N.V., Tichonova, T.R., & Derkach, M.A. (2018). Reforming the banking system of ukraine: problems and prospects. *Economy and Society, 19,* 981-985. doi: https://doi.org/10.32782/2524-0072/2018-19-147.

Drebot, N.P. (2018). The Trends in the Development of a Regional Network of Bank Branches in Ukraine. *Scientific Bulletin of UNFU, 28(4),* 52-55. doi: https://doi.org/10.15421/40280409.

Dudorov, O.O. *Problemy kvalifikatsii shakhraistva [Problems of fraud qualification].* Retrieved from http://law-dep.pu.if.ua/conference2014/articles/dudorov.pdf [in Ukrainian].

Farminh [Farming]. *Sait "Vikipedii", Site "Wikipedia".* Retrieved from http://www.uk.wikipedia.org/wiki/Фармінг [in Ukrainian].

Fedyshyn, M.F., Abramova, A.S., Zhavoronok, A.V., & Marych, M.G. (2019). Management of competitiveness of the banking services. *Financial and credit activity: problems of theory and practice, 1(28),* 64-74. doi: https://doi.org/10.18371/fcaptp.v1i28.163340.

Fishynh [Phishing]. *Sait "Vikipedii", Site "Wikipedia".* Retrieved from http://www.uk.wikipedia.org/wiki/Фішинг [in Ukrainian].

Golovko, O.G., & Moroz, O.K. (2018). Features of the development of the market of electronic payment systems in Ukraine. *Economy and Society, 19,* 976-980. doi: https://doi.org/10.32782/2524-0072/2018-19-146.

Holubiv, V.O., Havlovskyi, V.D., & Tsymbal, V.S. (2002). *Problemy borotby zi zlochynamy u sferi vykorystannia kompiuternykh tekhnolohii [Problems in combating computer crimes].* R.A. Kaliuzhnyi (Eds.). Zaporizhzhia: ZIDMU [in Ukrainian].

Husti, V.V., & Matyovka, T.V. (2018). Software complex for protection of rfid-tag of bank contactless payment card based on papas (MasterCard) and paywave (visa) technologies from unreacted reading. *Uzhhorod University Scientific Herald, 44,* 165-174. doi: http://dx.doi.org/10.24144/2415-8038.2018.44.165-174.

Kryminalnyi kodeks Ukrainy: vid 5 kvit. 2001 r. No. 2341-III [The Criminal Code of Ukraine from April 5, 2001, No. 2341-III]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].

Kryvtsun, I.M. (2018). Modern banking: risks and protection. *Economy and Society, 18,* 789-793. doi: https://doi.org/10.32782/2524-0072/2018-18-110.

Melnyk, M.I., & Klymenko, V.A. (Eds.). (2004). *Kryminalne pravo Ukrainy: Osoblyva chastyna [Criminal Law of Ukraine: Special Part].* Kyiv: Yuryd. dumka [in Ukrainian].

Pavlenko, L.D., & Semenets, V.P. (2019). Systema derzhavnoho antykryzovoho upravlinnia bankivskoiu systemoiu yak osnova stabilnoho funktsionuvannia vitchyznianoi ekonomiky [The system of state anti-crisis management of the banking system as the basis for stable functioning of the domestic economy]. *Investytsii: praktyka ta dosvid, Investment: practice and experience, 2,* 48-55. doi: 10.32702/2306-6814.2019.2.48 [in Ukrainian].

Ruda, O.L. (2019). Suchasnyi stan bankivskoi systemy Ukrainy ta yii konkurentospromozhnist [The current state of the Ukrainian banking system and its competitiveness]. *Efektyvna ekonomika, An efficient economy, 4.* Retrieved from http://www.economy.nayka.com.ua/pdf/4_2019/63.pdf. doi: 10.32702/2307-2105-2019.4.61 [in Ukrainian].

Sait "Ofitsiine internet-predstavnytstvo NBU" [Site "NBU Official Website"]. *www.bank.gov.ua.* Retrieved from http://www.bank.gov.ua/control/uk/publish/article?art_idMcI=123521 [in Ukrainian].

Sidak, V., & Koval, Y. (2018). Anti-crisis management economic safety of banking institutions on the state level: problems and ways of their solution. *European and scientific journal of Economic and financial innovation, 2,* 20-28. doi: http://doi.org/10.32750/2018-0203.

Ukrainska mizhbankivska asotsiatsiia chleniv platizhnykh system EMA Hrymasy shakhraiskykh saitiv [Ukrainian Interbank Association of Members of EMA Payment Systems Fraudulent]. (n.d.). *www.ema.com.ua.* Retrieved from http://www.ema.com.ua/cyber-safety-school/grimasi-shahrajskih-sajtiv-statistika [in Ukrainian].

Vishynh [Vishing]. *Sait "Vikipedii", Site "Wikipedia".* Retrieved from http://www.uk.wikipedia.org/wiki/Вішинг [in Ukrainian].

Yak korystuvatysia bankivskoiu kartkoiu i zalyshyty shakhraiv ni z chym [How to use a bank card and leave fraudsters with nothing]. (2018). *Sait "Minfim", Site "Ministry of Finance".* Retrieved from https://minfin.com.ua/ua/2018/09/25/35031214 [in Ukrainian].

Yarovenko, H.M., & Boiadzhian, M.M. (2018). Analysis of the cyber fraud consequences in the banking system of Ukraine. *Economy and Society, 18,* 836-844. doi: https://doi.org/10.32782/2524-0072/2018-18-116.

Zakon Ukrainy "Pro platizhni systemy ta perekaz koshtiv v Ukraini": vid 5 kvit. 2001 r. No. 2346-III [Law of Ukraine "On payment systems and funds transfer in Ukraine" from April 5, 2001, No. 2346-III]. (n.d.). *zakon1.rada.gov.ua.* Retrieved from https://zakon1.rada.gov.ua/laws/show/2346-14 [in Ukrainian].

Zhavoronok, A.V. (2018). Determination of the main problems of activation of the development of market of non-traditional banking services in Ukraine. *Economy and Society, 18,* 742-751. doi: https://doi.org/10.32782/2524-0072/2018-18-104.

Zhavoronok, A.V., Fedyshyn, M.F., & Kovalchuk, N.A. (2019). Transformation of banking products and services in modern conditions. *Problems and prospects of economics and management, 2(18),* 202-215. doi: 10.25140/2411-5215-2019-2(18)-202-215.

### *СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ*

CSO Maria Korolov 93 % of phishing emails are now ransomware. URL: http://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html.

Danik N. V., Tichonova T. R., Derkach M. A. Reforming the banking system of ukraine: problems and prospects. *Economy and Society.* 2018. Vol. 19. P. 981–985. doi: https://doi.org/10.32782/2524-0072/2018-19-147.

Drebot N. P. The Trends in the Development of a Regional Network of Bank Branches in Ukraine. *Scientific Bulletin of UNFU.* 2018. No. 28 (4). P. 52–55. doi: https://doi.org/10.15421/40280409.

Дудоров О. О. Проблеми кваліфікації шахрайства. URL: http://law-dep.pu.if.ua/conference2014/articles/dudorov.pdf.

Фармінг. *Вікіпедія :* [сайт]. URL: http://www.uk.wikipedia.org/wiki/Фармінг.

Fedyshyn M. F., Abramova A. S., Zhavoronok A. V., Marych M. G. Management of competitiveness of the banking services. *Financial and credit activity: problems of theory and practice.* 2019. No. 1 (28). P. 64–74. doi: https://doi.org/10.18371/fcaptp.v1i28.163340.

Фішинг. *Вікіпедія :* [сайт]. URL: http://www.uk.wikipedia.org/wiki/Фішинг.

Golovko O. G., Moroz O. K. Features of the development of the market of electronic payment systems in Ukraine. *Economy and Society.* 2018. Vol. 19. P. 976–980. doi: https://doi.org/10.32782/2524-0072/2018-19-146.

Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч. посіб. / за заг. ред. Р. А. Калюжного. Запоріжжя : ЗІДМУ, 2002. 292 с.

Husti V. V., Matyovka T. V. Software complex for protection of rfid-tag of bank contactless payment card based on papas (MasterCard) and paywave (visa) technologies from unreacted reading. *Uzhhorod University Scientific Herald.* 2018. Issue 44. P. 165–174. (Series «Physics»). doi: http://dx.doi.org/10.24144/2415-8038.2018.44.165-174.

Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

Kryvtsun I. M. Modern banking: risks and protection. *Economy and Society.* 2018. Vol. 18. P. 789–793. doi: https://doi.org/10.32782/2524-0072/2018-18-110.

Кримінальне право України: Особлива частина : підручник / за ред. М. І. Мельника, В. А. Клименка. Київ : Юрид. думка, 2004. 656 с.

Павленко Л. Д., Семенець В. П. Система державного антикризового управління банківською системою як основа стабільного функціонування вітчизняної економіки. *Інвестиції: практика та досвід.* 2019. № 2. С. 48–55. doi: 10.32702/2306-6814.2019.2.48.

Руда О. Л. Сучасний стан банківської системи України та її конкурентоспроможність. *Ефективна економіка*. 2019. № 4. URL: http://www.economy.nayka.com.ua/pdf/4_2019/63.pdf. doi: 10.32702/2307-2105-2019.4.61.

*Офіційне інтернет-представництво НБУ :* [сайт]. URL: http://www.bank.gov.ua/control/uk/publish/article?art_idMcl=123521.

Sidak V., Koval Y. Anti-crisis management economic safety of banking institutions on the state level: problems and ways of their solution. *European and scientific journal of Economic and financial innovation.* 2018. No. 2. P. 20–28. doi: http://doi.org/10.32750/2018-0203.

Українська міжбанківська асоціація членів платіжних систем ЕМА. Гримаси шахрайських сайтів. URL: http://www.ema.com.ua/cyber-safety-school/grimasi-shahrajskih-sajtiv-statistika.

Вішинг. *Вікіпедія :* [сайт]. URL: http://www.uk.wikipedia.org/wiki/Вішинг.

Як користуватися банківською карткою і залишити шахраїв ні з чим. *Мінфін :* [сайт]. 2018. URL: https://minfin.com.ua/ua/2018/09/25/35031214.

Yarovenko H. M., Boiadzhian M. M. Analysis of the cyber fraud consequences in the banking system of Ukraine. *Economy and Society.* 2018. Vol. 18. P. 836–844. doi: https://doi.org/10.32782/2524-0072/2018-18-116.

Про платіжні системи та переказ коштів в Україні : Закон України від 5 квіт. 2001 р. № 2346-III. URL: https://zakon1.rada.gov.ua/laws/show/2346-14.

Zhavoronok A. V. Determination of the main problems of activation of the development of market of non-traditional banking services in Ukraine. *Economy and Society.* 2018. Vol. 18. P. 742–751. doi: https://doi.org/10.32782/2524-0072/2018-18-104.

Zhavoronok A. V., Fedyshyn M. F., Kovalchuk N. A. Transformation of banking products and services in modern conditions. *Problems and prospects of economics and management.* 2019. Vol. 2 (18). P. 202–215. doi: 10.25140/2411-5215-2019-2(18)-202-215.

*Стаття надійшла до редколегії 05.09.2019*

***Cherniak A.*** – Doctor of Law, Chief Research Fellow of the Interagency Scientific and Research Centre on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4958-783X;

***Prozorov A.*** – Ph.D in Law, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-0307-1659

## Aspects of Prevention of Offences in the Sphere of Bank Payment Cards' Usage when Making Contactless and Internet Payments and their Classification

*The **purpose** of the article is to identify problematic issues in the prevention and qualification of offences related to the use of payment cards when making contactless and Internet payments, and to develop relevant recommendations. **Methodology.** While studying the issues, the authors used formal logic methods and special legal methods such as: comparative legal, system-structural and system analysis. **Scientific novelty.** The article describes the features of offences' qualification and prevention in the sphere of using payment bank cards when making contactless and Internet payments. It is noted that the use by criminals of the latest technologies in carrying out the corresponding illegal activities creates new challenges for the law enforcement system and the state as a whole. The need for the introduction of an appropriate preventive response package is indicated. The issue of the use of RFID-technologies by criminals for the introduction of new forms of criminal activity in the economic sphere is actualized. The accumulated achievements of leading foreign and Ukrainian scientists on the classification of relevant criminal activity, in spite of the significant relationship of crimes in this sphere, are summarized. Certain issues in providing a legal evaluation, depending on the objective and subjective aspects of criminal offenses are identified. Various views on the forensic characteristics of the corresponding manifestations were processed; attention was focused on certain aspects of their latency. **Conclusions.** The authors examined the following types of Internet fraud using bank payment cards such as phishing, vishing and pharming. Their statistics are analyzed and the most common types of frauds in our country are highlighted: «sweepstakes and lotteries», «work on the Internet», «fake online stores» and «training materials». The most common ways to prevent them, to minimize the onset of illegal consequences, are identified. Separate measures of a preventive and reactionary nature are proposed to prevent the corresponding category of crimes in the national economy.*

**Keywords:** electronic payment instrument; contactless bank payment card; bank account; phishing; vishing; pharming.