УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2022-11/132

КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРШАХРАЙСТВО В УМОВАХ ВОЄННОГО СТАНУ

CYBERCRIME AND CYBERFRAUD UNDER MARTIAL LAW

Діброва Т.А., студентка V курсу факультет прокуратури
Національний юридичний університет імені Ярослава Мудрого

Пісенко Д.О., студентка V курсу факультету прокуратури
Національний юридичний університет імені Ярослава Мудрого

Сметаніна Н.В., к.ю.н., доцентка, член Ради молодих вчених, асистентка кафедри кримінально-правової політики
Національний юридичний університет імені Ярослава Мудрого

Наукову статтю присвячено проблемі трансформаційного явища – кібершахрайства в умовах воєнного стану. Проаналізовано причини, умови, законодавче визначення шахрайства та кіберзлочину, оптимізацію кримінальної відповідальності, сучасний стан та статистику кримінальних правопорушень у мережі інтернет.

Так, сьогодні можна знайти значний обсяг інформації про вчинені кіберзлочини, збитки від них, потерпілих, наприклад, у засобах масової інформації, Інтернеті, облікових даних правоохоронних органів тощо.

Проведено аналіз сучасних тенденцій вчинення шахрайський дій, та наведено шляхи боротьби з ними. Світ не стоїть на місці, відповідно і держава розивається в боротьбі з кіберзлочинністю, тому нею створенні грунтовні проєкти збереження населення від шахраства як і інтернеті так і в реальному житті. Зростаюча кількість кіберзлочинної діяльності на підприємствах, постійне вдосконалення інформаційних технологій і нові можливості «вдосконалення» інструментів їх скоєння створюють економічні загрози для глобальних інформаційних мереж.

Актуальність статті полягає в щоденному зростанні кількості вчинених шахрайських діянь у мережі Інтернет. Злочинці, завдаючи шкоди українцям у кіберпросторі допомагають агресору у цій війні. Окрім того, потерпілими нерідко стають іноземці, що підриває авторитет та довіру до нашої країни у соціальному та політичному просторі. Авторки вважають виправданим запровадження більш суворих санкцій та криміналізацію окремих діянь.

Також слід зазначити, що кібершахрайство є цілком новим явищем, оскільки безпосередньо воно пов'язане з розвитком новітніх інформаційних технологій та вимагає від правопорушників відповідних навичок, проте вчиняти такі правопорушення може майже кожна особа, яка має вільний доступ до мережі Інтернет. Особливим аспектом цієї статті є характеристика кібершахрайства як дійсно небезпечного виду кримінальних правопорушень, так як внаслідок нього щодня люди втрачають свої кошти, їх особиста інформація стає незаконно доступною для кола осіб, які можуть її використовувати у своїх цілях.

Ключові слова: шахрайство, кіберзлочин, кібершахрайство, протидія кіберзлочинам, шахрайство під час воєнного стану, причини зростання кіберзлочинності.

The scientific article is devoted to the problem of transformational phenomenon - cyber fraud in martial law. The reasons, conditions, legal definition of fraud and cybercrime, optimization of criminal liability, current state and statistics of criminal offenses on the Internet are analyzed.

Thus, today it is possible to find a significant amount of information about committed cybercrimes, losses from them, victims, for example, in the media, the Internet, law enforcement agencies' accounts, etc.

The current trends of fraudulent actions were analyzed and ways to combat them were presented. The world does not stand still, respectively, and the state is struggling to fight cybercrime, so it has created thorough projects to protect the population from fraud both on the Internet and in real life. The growing number of cybercrime activities in enterprises, the constant improvement of information technology and new opportunities to «improve» the tools for their commission create economic threats to global information networks.

The relevance of the article lies in the daily increase in the number of fraudulent acts committed on the Internet. Criminals, harming Ukrainians in cyberspace, help the aggressor in this war. In addition, foreigners often become victims, which undermines the credibility and trust in our country in the social and political space. The authors consider it justified to introduce stricter sanctions and criminalize certain acts.

It should also be noted that cyber fraud is a completely new phenomenon, as it is directly related to the development of the latest information technologies and requires appropriate skills from offenders, but almost anyone who has free access to the Internet can commit such offenses. A special aspect of this article is the characterization of cyber fraud as a really dangerous type of criminal offense, since as a result of it people lose their money every day, their personal information becomes illegally accessible to a range of persons who can use it for their own purposes.

Key words: fraud, cybercrime, cyberfraud, counteraction to cybercrime, fraud during martial law, reasons for the growth of cybercrime.

Постановка проблеми. Сьогодні – переломний етап для України, так як після початку війни 24 лютого 2022 року у нашій державі бої відбуваються не тільки на полі бою, але і в інформаційному просторі мережі інтернет. Загибель близьких, втрата домівки, постійної роботи, введення режиму воєнного стану – всі ці явища вплинули не свідомість та поведінку людей, яка у більшості випадків стала антиправовою.

Активізація інтернет-шахраїв, які маніпулюють вразливим населенням України та небайдужими іноземцями – нагальна проблема, з якою веде боротьбу правоохоронна система нашої держави. Результатом стало поширення обсягу кіберзлочинів, особливо шахрайства в інтернеті.

Мета статті. У цій науковій праці аналізуються поняття «шахрайство», «кібершахрайство», «кіберзлочинність». Постає необхідність у визначенні причин та умов поширення зазначених кримінальних правопорушень та визначаються можливі заходи протидії та виявленню потенційних злочинців. Досліджуються статистичні дані та їх зміна в умовах воєнного стану.

Питання боротьби з кіберзлочинністю розглядалися багатьма науковцями. Зазначеним питанням приділяли увагу такі дослідники як О.М. Бандурка, В.В. Василевич, В.В. Голіна, Б.М. Головкін, А. П. Закалюк, О.М. Литвинов, В.В. Марков, В.І. Трапезніков, В.О. Туляков, І. В. Жук, Я. В. Левківська та інші. Їх дослідження є цінними для продовження наукових пошуків.

Термін «шахрайство» бере свій початок від слова «мошна», яке має такі значення: сумка, кошель, мішечок із зав'язкою для зберігання грошей, а під вчиненням шахрайства розумілося викрадення такої мошни; обман, шахрайські дії з корисливою метою. Шахраями називали «карманщиків, тяглецiв, кишенькових злодіїв; зернщиків, які обкрадали людей на базарах; злодюжків, ошуканців» [1].

Відповідно до Кримінального кодексу (далі – КК) України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (ст.190 КК України). Здійснення даного кримінального правопорушення в інтернеті науковці називають «кібершахрайством» [2].

Відповідно до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [3], кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України. До того ж це кримінальні правопорушення, передбачені розділом XVI КК України («Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку»), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – «з використанням високих інформаційних технологій і телекомунікаційних мереж».

Погоджуємось із твердженням, що кібершахрайство – це новий, відмінний від звичайного шахрайства вид кримінального правопорушення, який у результаті еволюції та впливу технологій вчинюється з використанням нових, раніше не досліджених методів, хоча за складом нагадує звичайне шахрайство [4, с. 41; 14, 15].

У процесі вивчення кримінально караного явища, необхідно дослідити причинну детермінацію, яка зумовлює вчинення кримінальних правопорушень, адже окресливши причини вчинення злочину – можна пропонувати та розробляти заходи протидії. Так серед умов та причин поширення кібершахрайства у воєнний час можна виділити: бідність населення, безкараність, втрата постійної роботи, психічне перевантаження і страждання через втрату близької особи, втрата місця проживання тощо. Підштовхують такі привабливі для злочинців фактори як: анонімність, доступність, складність виявлення, обтяжена перенавантаженням правоохоронних органів.

З метою уникнення будь-якої дестабілізації ситуації в Україні під час війні поліція з іншими правоохоронними органами працює в посиленому режимі безперервно. Збір, обробка та узагальнення інформації з якомога більшого кола джерел здійснюється цілодобово. Так, наприклад, на поліцейських покладено обов'язки з патрулювання вулиць, перевірки документів у підозрілих осіб, в залежності від ситуації з огляду речей, транспортних засобів, багажу, службових приміщень та житла громадян. Окрім того, існує необхідність в здійсненні перевірки магазинів щодо заборони торгівлі зброєю, сильнодіючими хімічними та отруйними речовинами, а також алкогольними напоями та речовинами, виробленими на спиртовій основі. Деякі громадяни здійснюють продаж гуманітарної допомоги – протидія цьому – також обов'язок правоохоронних органів.

На додаток до вищезазначених обов'язків – запровадження безпекового режиму, а саме комендантської години, встановлення блокпостів, на яких транспортні засоби після перевірки документів водіїв та пасажирів пропускають представники тероборони, нацгвардійці та офіцери поліції.

Отже, шахраї користуються зайнятістю правоохоронних органів, залишаються безкарними, що породжує наміри на вчинення повторних, обтяжуючих кримінальних правопорушень з використанням нових, більш інноваційних і технологічних методів.

Серед поширених схем шахрайства у воєнний час можна виокремити: пропозиція з оренди неіснуючого чи вже зайнятого житла для осіб, які вимушені покинути власні домівки, фейкові перевезення та квитки для в'їзду в місто, недійсні талони на паливо, маніпуляції з продажу затребуваних під час війни товарів, надання недостовірної інформації про родичів, полонених військових, різного роду збори у соціальних мережах на допомогу військовим, постраждалим особам.

Поширеною шахрайською схемою стала пропозиція отримання грошової допомоги, яку видають за грошову допомогу від держави, Організації Об'єднаних Націй, благодійних фондів тощо для окремих категорій осіб. Вимога шахраїв – авторизаціія за схемою, яка передбачає введення своїх особистих даних, номеру телефону, інформації про банківські рахунки, де завершення процедури підтверджується прийняттям дзвінка або текстового повідомлення, після чого з картки отримувача списуються кошти [5, с. 522].

У процесі реагування на швидке зростання рівня кіберзлочинності Верховна Рада України провела оптимізацію кримінального та кримінально-процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Так, було внесено зміни до відповідних законів: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» No 2137-IX від 15 березня 2022 року та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» No 2149-IX від 24 березня 2022 року [6; 7].

Дійсно, можна констатувати підвищення ефективності боротьби з кіберзлочинністю за допомогою посилення відповідальності за наведені кримінальні правопорушення. Розширення меж діяльності правоохоронних органів щодо розслідування кіберзлочинів, посилення санкцій, додаткова криміналізація окремих діянь – стримують потенційних шахраїв, проте проблема постає в тому, що кримінологічні дослідження у більшості випадків спираються на облікові дані злочинності, при цьому відсутнє вивчення соціальних, економічних, політичних, демографічних, організаційних та інших причин кібершахрайства.

Пропозицією постає масштабне, глибоке дослідження проблеми з метою розробки більшого кола заходів із протидії кібершахрайству. Необхідно інформувати населення про витончені методи шахраїв, аби не тільки попереджати вчинення нових кримінальних правопорушень, але й виявляти потенційних злочинців.

В Україні за минулий рік зріс рівень збитків від незаконних дій з платіжними картками. Водночас в Нацбанку підкреслили, що він залишається відносно низьким. «За 2021 рік кіберполіції вдалося задокументувати злочинну діяльність та скерувати до суду понад 2000 кримінальних проваджень, що стосуються саме інтернет-шахрайства, до їх вчинення були причетні 422 зловмисники. Також у роботі на сьогодні перебуває ще понад 6600 проваджень. До речі, саме шахрайські дії в мережі Інтернет становлять майже 70% від усіх звернень, які надходять до кіберполіції. Найрозповсюдженішими у 2021 році шахрайськими схемами були: продаж неіснуючих товарів, псевдовиграші, телефонні шахрайства, фішингові ресурси для привласнення грошей або збору персональних даних, заволодіння грошима під приводом надприбутків та прохання знайомих про допомогу в соціальних мережах. У цілому за минулий рік, за зафіксованими Національною поліцією випадками, кіберзлочинці ошукали громадян більше ніж на 193 мільйони гривень», – зазначив керівник відділу протидії злочинам у сфері комп'ютерних систем Департаменту кіберполіції Євгеній Дороганов [8].

Директор Департаменту платіжних систем та інноваційного розвитку Національного банку Андрій Поддєрьогін також доповів, що, з одного боку, Національний банк вбачає продовження позитивного тренду на заміну форм-фактору платіжних карток із суто магнітною смугою

на більш захищені картки з чипом. Це відбилося, зокрема, і на обсягах шахрайства в таких каналах, де використовується фізична картка – торговельна мережа та банкомати. Так, на один мільйон гривень видаткових операцій з використанням платіжних карток обсяг збитків від шахрайських дій в торговельній мережі зменшився з 61 гривні (у 2020 році) до 40 гривень (у 2021 році), у банкоматах – із 33 гривень (у 2020 році) до 29 гривень (у 2021 році) [8].

Також за минулий рік майже на 45% зменшилася середня сума шахрайської операції в торговельній мережі – із 1 984 гривень (у 2020 році) до 1086 гривень (у 2021 році). У середньому на одну незаконну операцію у 2021 році припадало близько 1 600 гривень, що на 16% менше, ніж у 2020 році (1900 гривень) [8].

«Водночас ми спостерігаємо, що на один мільйон гривень видаткових операцій з платіжними картками, здійснених у мережі Інтернет, обсяг збитків збільшився з 61 гривні (у 2020 році) до 114 гривень (у 2021 році), – констатував Андрій Поддєрьогін. – Якщо порівнювати Україну та Європу, то в нас показник відносних збитків від загального обсягу операцій з платіжними картками залишається значно меншим. В Україні це 0,0065% (тобто 65 гривень збитків на один мільйон гривень), а у країнах ЄС, за даними Європейського центрального банку, цей показник у кілька разів вищий і сягав 0,036% у 2019 році (тобто 360 євро збитків на один мільйон євро). Фактично шахрайство через мережу Інтернет є світовим трендом. І у більшості випадків люди стають жертвами шахраїв через недотримання основних правил платіжної безпеки» [8].

Національний банк України в листі від 4 липня 2018 р. № 57-0009/36366 підготовив рекомендації стосовно запобігання та протидії шахрайству в банківській системі [9].

Крім того, слід зазначити, що з 14 лютого 2022 року стартувала інформаційна кампанія Національного банку з платіжної безпеки #ШахрайГудбай. Вона стане продовженням першої подібної кампанії, яка успішно пройшла у 2020 році. Її метою є поліпшення обізнаності громадян про кібергігієну та сприяння формуванню культури безпечної поведінки у віртуальному просторі, крім того, вона є нагадуванням про основні правила безпеки безготівкових розрахунків.

Проєкт #ШахрайГудбай, організатором якого виступають Національний банк України та Департамент Кіберполіції Національної поліції України, об'єднав навколо інформаційної кампанії більше 80 партнерів – це банки, платіжні системи, мобільні та поштові оператори, асоціації, мережі магазинів, маркетплейси, громадські спілки, комунальні підприємства, обласні державні адміністрації та інші державні органи.

Сайт цього проєкту досить наповнений, дуже детально надає поради користувачам щодо захисту їхніх фінансів від шахраїв. В розділі «Кібербезпека», можем спостерігати основні поради для захисту свого смартфону, зокрема:

- встановіть пароль на вхід / використовуйте біометричні дані для входу;
- налаштуйте сповіщення на заблокованому екрані у такий спосіб, щоб ховати їхній конфіденційний вміст;
- змініть заводський PIN-код до SIM-картки на стійкий (8-значний);
- використовуйте лише ліцензійні програми, мобільні застосунки та систематично їх оновлюйте [10].

Крім того, сайт містить багато корисної інформації щодо платіжної безпеки, ось декілька з них: «Змінюйте PIN-код до картки: регулярно 1 раз на 3 місяці, ситуативно: якщо виникла підозра, що ще хтось його може знати».

Дуже розповсюдженим є шахрайство-шопінг, коли користувачі купують потрібні їм речі на неперевірених сайтах, тому з метою уникнення подібного шахрайства були створенні спеціальні сервіси для перевірки справжності сайтів. Зокрема це «STOP HYPERLINK "http://cyberpolice.gov.ua/stopfraud/" HYPERLINK "http://cyberpolice.gov.ua/stopfraud/"FRAUD» Кіберполіції та «Black HYPERLINK "http://www.ema.com.ua/blacklist/" HYPERLINK "http://www.ema.com.ua/blacklist/"List» Асоціації «ЄМА».

Сайти, які приймають онлайн-платежі мають бути захищеними, для цього в назві адреси вони мають містити https:// та значок « ». На сайті мають бути значки захисту онлайн-покупок від платіжних систем – Verified by Visa та MasterCard SecureCode [10].

Ще одним видом шахрайства з картками є «скімінг» це такий вид шахрайства, коли шахраї копіюють інформацію з платіжної картки за допомогою спеціальних пристроїв, які встановлюють на банкомат. Надалі це дозволяє злочинцям виготовити дублікат платіжної картки та викрасти гроші з рахунку власника картки. Знаряддям такого шахрайства виступає спеціальний пристрій, який встановлюють в картоприймач банкомату. Це може бути: тонка пластинка, яка вставляється всередину картоприймача або накладка, що кріпиться на картрідер банкомата. Але, слід зазначити, що копії даних з платіжної картки шахраю не достатньо, потрібен ще і PIN-код. Тому, щоб вкрасти PIN-код шахраї використовують:

- мікрокамеру, для того щоб на відео побачити, який PIN-код буде вводити жертва;
- накладну клавіатуру для зчитування PIN-коду. Її шахраї використовують рідше, оскільки мікрокамера набагато дешевша та непомітніша[10].

Як вберегтися від скімінгу?

- Порівнювати зовнішній вигляд банкомату з його екранною заставкою.
- Прикривати клавіатуру під час введення PIN-коду.
- У такій спосіб, щоб його неможливо було підглядіти за допомогою мікровідеокамери.
- Підключити послугу інформування про операції з використанням картки.
- Це дозволить вчасно заблокувати картку, у разі шахрайських операцій з вашим рахунком.
- Встановити індивідуальні ліміти на зняття готівки, які відповідають саме вашій платіжній поведінці.
- Шахраю не вдасться всю суму зняти одразу, у вас з'явиться час заблокувати свою картку.
- Надавати перевагу платіжним карткам з чіпом, у яких складніший алгоритм захисту на відміну від карток з магнітною смугою [10].

Сучасним в Україні видом шахрайства є пенсійні афери, або ж допомога пенсіонерам від держави, соціальні виплати та допомога від європейських організацій.

Ці шахрайства пов'язані зі злочинцями, які пропонують людям помилкові фінансові можливості, обіцяють багато грошей і гарантовані високі допомоги від фондів, які можуть здатися занадто хорошими, щоб бути правдою. У соціальній мережі Facebook активізувалися шахраї, які спекулюють на темі грошових виплат українцям, про це повідомляє Державна служба спеціального зв'язку та захисту: «Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, попереджає про зростання кількості шахрайських сторінок у соціальній мережі Facebook. Зловмисники використовують тематику грошових компенсацій, фінансової допомоги від ООН, Європейського суду з прав людини, Товариства Червоного Хреста тощо», йдеться у повідомленні [11].

Зокрема, шахраї обіцяють виплати «за рахунок конфіскованих активів рф», посилаються на нечинні рішення різних органів влади України. Повідомляється, що в оголошеннях пропонують перейти за посиланням, яке веде на фішингову сторінку так званого «Єдиного Компенсаційного Центру Повернення Невиплачених Грошових Коштів». На цьому сайті користувачам пропонують отримати виплату за умови надання персональної інформації та здійснення додаткового платежу. В результаті дані банківської картки будуть скомпрометовані [11].

В 2017 році Публічне акціонерне товариство «Приватбанк» затвердив положення про запобігання шахрайству, метою якого є реалізація ефективних заходів запобігання шахрайству та зловживаням в Банку, отримання зворотнього зв'язку за результатами реалізованих заходів та їх подальше коригування. Відповідальність за боротьбу з шахрайством в банку несуть:

• за координацію побудови системи боротьби з шахрайством в Банку Напрямок «Fraudменеджмент» ГО;

• за протидію фактам шахрайства та зловживань в своєму колективі керівник підрозділу;

• кожен співробітник Банку [12].

Крім того, «Приватбанк» запустив послугу «Страхування від шахрайства», яка доступна до оформлення всім користувачам. Умовами цієї послуги є сплата 29 гривень на місяць, що захистить користувача від шахрайства на суму 50 000 грн, при цьому страховий тариф – 0,696% від страхової суми. У разі настання страхової події користувачу необхідно звернутись на гарячу лінію «Приватбанк», після чого карта буде заблокована, потім необхідно подати відповідну заяву в поліцію та взяти виписку з Єдиного реєстру досудових розслідувань. Страхове відшкодування зараховується на карту для виплат застрахованої особи [13].

Отже, можемо підсумувати, що боротьба з кібершахрайством в Україні реалізується в трьох основних напрямках діяльності: 1) попередження кіберзлочинів; 2) загальна організація боротьби з кіберзлочинністю та правоохоронна діяльність, спрямована саме на виявлення, запобігання та розкриття кіберзлочинів; 3) застосування заходів кримінальної відповідальності і покарання осіб, які вчинили кіберзлочини.

Попередження як одна з форм боротьби зі злочинністю передбачає як загальнодержавні заходи економічного, ідеологічного, правового та виховного характеру, так і спеціальні організаційні, технічні, програмні та криптографічні. В Україні діє багато платформ для інформування громадян щодо шахрайських схем та засобів, як не стати жертвою кібершахрайства. На спеціальном ресурсі пояснюють правила кібербезпеки й надають поради українцям, як надійніше захистити свої гроші. У межах кампанії Національний банк разом із партнерами інформуватимуть громадян про те, як вберегтися від платіжного шахрайства, зокрема через оновлену тематичну вебсторінку (лендинг) #ШахрайГудбай із детальною інформацією про кампанію та правила поведінки у віртуальному просторі. Ще раз слід наголосити, що кіберзлочинність має специфічні причини, і боротьба з нею також передбачає застосування специфічних засобів.

ЛІТЕРАТУРА

1. Бусель В. Т. Великий тлумачний словник сучасної української мови / Уклад. і го- лов. ред. К. Ірпінь: ВТФ «Перун», 2001. С. 1391.
2. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. URL: http://www.pjv.nuoua.od.ua/v3_2018/2018_3 (дата звернення: 11.11.2022).
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 No 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.112022).
4. Веліканов С. В., Волобуєв А. Ф., Журавель В. А., та ін. Криміналістична профілактика економічних злочинів: науково-практичний посібник. Харків : «Харків юридичний», 2006. 236 с.
5. Левківська Я. І. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. URL: http://dspace.onua.edu.ua/handle/11300/19993 (дата звернення: 20.11.2022).
6. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 20.11.2022).
7. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 берез. 2022 No 2149- IX : URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 20.11.2022).
8. Офіційний сайт Національного банку України. URL: https://bank.gov.ua/ua/news/all/startuye-informatsiyna-kampaniya-natsionalnogo-banku-z-platijnoyi-bezpeki-shahraygudbay (дата звернення 21.11.2022).
9. Лист Національного банку України «Рекомендації для зниження ризику шахрайських операцій» від 4 липня 2018 р. URL: https://vk24.ua/regulations_and_jurisprudence/listi/oplata-praci/list-nacionalnogo-banku-ukraini-rekomendacii-dlya-znizhennya-riziku-shakhrayskikh-operaciy
10. Офіційний сайт Національного банку України. Проєкт «#ШахрайГудбай». URL: https://promo.bank.gov.ua/stopfraud/#section-35
11. Стережіться «виплат»: ПриватБанк попереджає про нову схему шахрайства. *УНІАН*. URL: https://www.unian.ua/economics/finance/shahraystvo-z-bankivskimi-kartkami-privatbank-poperedzhaye-pro-novu-shemu-mahinaciy-novini-ukrajina-11895471.html
12. Положення «Про запобігання шахрайству»: затв. рішенням Правління банку «ПриватБанк» від 28.09.2017 р. URL: https://static.privatbank.ua/files/politika-zapobigannya-shaxrajstva-ta-korupcii.pdf
13. Захист від шахрайства. *Офіційний сайт ПриватБанк.* URL: https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva
14. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності. Міжнародні стандарти з кібербезпеки та їх застосування в Україні : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). Харків, 2016. С. 59–61.
15. Nizovtsev, Yuriy; Parfylo, Oleg; Barabash, Olha; Kyrenko, Sergij; Smetanina, Nataliia. Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of Money Laundering Control.* Volume 25, Issue 2, Pages 297–305. 21 April 2022. https://www.emerald.com/insight/content/doi/10.1108/JMLC-02-2021-0015/full/html.