УДК 347.73
DOI https://doi.org/10.32782/2524-0374/2023-3/65

ЗАКОНОДАВЧІ МЕХАНІЗМИ БОРОТЬБИ З КІБЕРШАХРАЙСТВАМИ У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ

LEGISLATIVE MECHANISMS OF FIGHTING CYBER FRAUD IN THE FINANCIAL SECTOR OF UKRAINE

Гарбінська-Руденко А.В., к.ю.н., доцент,
доцент кафедри публічного права
Державний податковий університет

Булківська В.А., студентка IV курсу
Навчально-науковий інститут права Державного податкового університету

Волинець В.В., студентка IV курсу
Навчально-науковий інститут права Державного податкового університету

Стаття присвячена пошуку нормативно-правових механізмів боротьби з фінансовими кібершахрайствами, які протягом останніх років стали значною загрозою для економіки країни в цілому, та для кожного громадянина окремо. Тому, наукове дослідження фінансового кібершахрайства є критично важливим для забезпечення фінансової стабільності та безпеки в сучасному світі.

Авторами окреслюється, що кібершахрайство у фінансовій сфері – це протиправні дії, які здійснюються з використанням технологій і мережі Інтернет з метою отримання незаконних вигод у фінансовій сфері. Виділено основні види фінансових кібершахрайств до яких відносять: фішинг, скімінг, віруси-вимагачі, рейдерство, тощо.

Надається коротка характеристика міжнародних законодавчих актів, що забезпечують кібербезпеку фінансової сфери, аналіз яких є надзвичайно важливим для українського законодавства, що проходить шлях вдосконалення у зв'язку з євроінтеграційним вектором розвитку.

У процесі розгляду нормативно-правових актів, що регулюють питання боротьби з кібератаками на фінансові установи були виявлені певні прогалини, зокрема відсутність чіткого визначення фінансових кібершахрайств в законодавстві України, недостатнє регулювання діяльності платіжних систем і електронних грошей та недостатня координація між різними органами державної влади та правоохоронних органів у процесі боротьби з фінансовими кібершахрайствами.

Авторами резюмується, що недостатність чіткої та ефективної регуляторної бази та механізмів контролю відкриває можливості для шахраїв реалізовувати свої злочинні дії та збагачуватися за рахунок відкритих прогалин системи безпеки фінансових установ та законодавства.

Запропоновані нові нормативні інструменти, які б забезпечили ефективний захист від кібершахрайств, що є важливим завданням для держави та фінансових установ. До таких інструменті віднесено законодавче регулювання та контроль за діяльністю компаній, які займаються обміном криптовалют, розробку та впровадження ефективних механізмів захисту персональних даних користувачів, використання сучасних технологій для виявлення та запобігання кібератакам та злочинам у фінансовій сфері.

Ключові слова: кібершахрайства, фішинг, кібератака, боротьба з шахрайствами, фінансова система.

The article is devoted to the search for regulatory and legal mechanisms to combat financial cyber fraud, which in recent years has become a significant threat to the country's economy as a whole, and to each individual citizen. The authors outline that cyberfraud in the financial sphere is illegal actions that are carried out using technologies and the Internet in order to obtain illegal benefits in the financial sphere, such as theft of money, confidential information, access to banking systems and payment cards, etc. The main types of financial cyber fraud are highlighted, which include: phishing, skimming, ransomware viruses, raiding, etc.

A brief description of international legislative acts that ensure cyber security of the financial sphere is provided, the analysis of which is extremely important for Ukrainian legislation, which is undergoing improvement in connection with the European integration vector of development.

In the process of consideration of legal acts governing the fight against cyber attacks on financial institutions, certain gaps were identified, in particular, the lack of a clear definition of financial cyber fraud in the legislation of Ukraine, insufficient regulation of the activity of payment systems and electronic money, and insufficient coordination between various state authorities and law enforcement agencies. bodies in the fight against financial cyber fraud.

The authors summarize that the lack of a clear and effective regulatory framework and control mechanisms opens up opportunities for fraudsters to carry out their criminal activities and get rich due to open gaps in the security system of financial institutions and legislation.

New regulatory tools are proposed that would provide effective protection against cyber fraud, which is an important task for the state and financial institutions. These tools include legislative regulation and control over the activities of companies engaged in cryptocurrency exchanges, development and implementation of effective mechanisms for protecting users' personal data, and the use of modern technologies to detect and prevent cyber attacks and crimes in the financial sphere.

Key words: cyber fraud, phishing, cyber attack, fight against fraud, financial system.

Проблема фінансового кібершахрайства є дуже актуальною не тільки в світі, але й в Україні, а кількість кібератак на фінансові установи стрімко зростає щороку. За даними дослідження IBM Global Average Data Breach, у 2022 році глобальні втрати даних від кібератак становили 4,4 мільйона доларів, порівняно з 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році [1]. При цьому загальні збитки від кіберзлочинності в галузі фінансів можуть сягати мільйонів і навіть мільярдів доларів.

Україна не є винятком, так у 2022 році збитки від шахрайства в інтернеті та з використанням методів соціальної інженерії зросли на 96% порівняно з попереднім роком і досягли 1 млрд грн, повідомила асоціація членів платіжних систем ЄМА. Середня сума однієї шахрайської операції зросла на 49% – до 7900 грн [2].

Нинішня нестабільна ситуація в соціально-економічній та політичній сферах, що спричинена повномасштабним військовим вторгненням російської федерації на територію України, сформувала сприятливе підґрунтя для поширення різного роду шахрайських схем на теренах цифрової мережі. Таким чином, протягом 2022 року збитки від шахрайства в інтернеті та з використанням методів соціальної інженерії зросли на 96% порівняно з попереднім роком. Розрахункова сума збитків громадян від шахрайства з використанням методів соціальної інженерії зросла на 99% – до 968,5 млн грн [2]. Зважаючи на

це пошук сучасних інструментів боротьби з кібершахрайствами у фінансовому секторі є нагальним питанням, яке потребує вирішення на різних рівнях, в тому числі й законодавчому.

Дослідженням поняття фінансових кібершахрайств протягом останніх десятиліть цікавилось чимало вітчизняних та закордонних науковців, серед яких, зокрема, О.В. Тихонова, Л.В. Герасименко, О.О. Шевчук, М.О. Акімов, які провели порівняльний аналіз боротьби з економічними та фінансовими злочинами в Україні та ЄС; Х. Юнис, Т.Н. Ат-Тавиль дослідили взаємозв'язок законодавчої бази про кіберзлочинність та захист громадян й бізнесу (на прикладі Об'єднаних Арабських Еміратів); І.Л. Панделіч в загальному описував феномен кіберзлочинності. Наукове дослідження фінансових кібершахрайств може допомогти при розумінні та аналізі цього явища, розробці нових методів та технологій для протидії цим правоорушенням, а також у попередженні виникнення нових форм кіберзлочинності.

Метою статті є дослідження правового регулювання фінансових кібершахрайств в Україні та пошук нових нормативних інструментів боротьби з цим негативним соціально-економічним явищем.

Попри значну кількість наукових робіт, проблема фінансових кібершахрайств до кінця не вивчена та не досліджена, адже, в силу різних обставин, мережеве шахрайство має властивість постійно змінюватися та швидко поширюватися. Зокрема для національного законодавства залишається відкритим питання пошуку нових методів боротьби з шахрайствами у фінансовій сфері, задля зменшення шкоди національній економіці та гарантування безпеки громадянам під час дії воєнного стану.

Фінансові кібершахрайства є досить новим явищем, яке з'явилось в наслідок зростання використання інтернету та електронних платежів. Історія виникнення фінансових кібершахрайств починається з появи перших електронних грошей в 1990-х роках [3, с. 236]. Тоді ж народилися і перші кіберзлочинні організації, які використовували світову мережу для протиправних дій.

З поширенням інтернету та зростанням кількості електронних операцій з'явилися нові можливості для кіберзлочинців, такі як крадіжки інформації про кредитні картки, фішингові атаки, скімінг та інші види кібератак на фінансові установи та користувачів.

Загалом кібершахрейство у фінансовій сфері можна визначити як протиправні дії, які здійснюються з використанням технологій і мережі Інтернет з метою отримання незаконних вигод у фінансовій сфері, таких як крадіжка грошей, конфіденційної інформації, доступ до банківських систем та платіжних карток тощо [3, с. 237].

За останні кілька років фінансові кібершахрайства стали дедалі більш поширеними та складнішими. Злочинні організації використовують нові технології та методи, щоб отримати доступ до цінної інформації та грошей [4]. Наприклад, хакери можуть використовувати шпигунський софт для віддаленого доступу до комп'ютерів та мобільних пристроїв, щоб отримати доступ до фінансових даних.

Розрізняють декілька сучасних видів кібершахрайств у фінансовій сфері серед яких:

1) Фішинг – це метод шахрайства, коли зловмисники використовують підроблені веб-сайти або електронні листи для того, щоб отримати конфіденційну інформацію від жертви, таку як паролі, номери банківських карток, персональні дані та інші. До прикладу, такі дії можуть бути спрямовані на користувачів банківських систем, електронних платіжних систем, а також на особисті електронні кабінети.

2) Скімінг – це використання пристроїв для копіювання інформації з магнітної смужки кредитної картки або використання підроблених пристроїв, які зчитують інформацію з чіп-карток. Тобто це метод кібершахрайства, при якому зловмисники встановлюють на банкоматах та терміналах оплати пристрої, які зчитують інформацію з магнітних смужок на картках, які вставляються в ці пристрої [5, с. 402].

3) Кібератаки на банківські установи – це вид кібершахрайства, при якому зловмисники намагаються використати різноманітні технології, такі як шкідливі програми та віруси, щоб отримати доступ до фінансової інформації банківських установ.

4) Кібератаки на платіжні системи – це вид кібершахрайства, при якому зловмисники намагаються отримати несанкціонований доступ до систем електронних платежів і викрасти гроші.

5) Кібератаки на криптовалюту – це вид кібершахрайства, при якому зловмисники намагаються використати технології блокчейну та криптографії, щоб викрасти криптовалюту.

6) Рейдерство – це кібершахрайство, яке використовується для отримання нелегального доступу до банківських систем та крадіжки грошей або конфіденційної інформації. Може бути здійснене шляхом зламування захисту комп'ютерної мережі або використання соціальної інженерії [5, с. 403].

На виникнення нових форм вираження фінансових шахрайств в мережі значною мірою вплинуло повномасштабне російське вторгнення на територію України. Відомо, що з початком активної фази російської збройної агресії 2022 року, в Інтернеті почали поширюватися нові форми фінансових кібершахрайств [6]. Наприклад, злочинці оформляють кредити на зниклих безвісти військовослужбовців і громадян, які виїхали за кордон, збираючи їхні SIM-картки та разом з тим отримуючи доступ до їхніх банківських рахунків й оформлюючи онлайн-кредити на їхнє ім'я.

З метою протидії фінансовим кібершахрайствам у багатьох країнах з'явилися спеціальні служби та законодавчі акти, що забезпечують кібербезпеку фінансової сфери, аналіз яких є надзвичайно важливим для українського законодавства, що перебуває в активному пошуку сучасних іструментів боротьби з кібершахрайствами у фінансовому секторі.

До прикладу, в Німеччині основним законом, який забезпечує кібербезпеку в фінансовій сфері є Закон про кібербезпеку мереж і інформації (Network and Information Security, NIS) – цей закон був прийнятий в 2015 році, а згодом змінений і переглянутий в 2017 році. Він встановлює стандарти кібербезпеки для критичних інфраструктурних секторів, включаючи фінансові послуги, та зобов'язує підприємства повідомляти про інциденти кібернападів [7].

В свою чергу, фінансові мережеві шахрайства регулюються відповідно до норм Закону про безпеку інформації від 7 серпня 2018 року (Loi relative à la sécurité de l'information). Цей закон встановлює правила та стандарти для захисту інформації, що обробляється компаніями, які надають фінансові послуги. Також варто звернути увагу на Закон про кібербезпеку від 5 вересня 2018 року (Loi pour une République numérique). Цей закон встановлює обов'язок компаній, які надають фінансові послуги, виконувати заходи для захисту своїх інформаційних систем від кібератак. Закон також вимагає, щоб компанії мали план дій для відновлення роботи своїх систем у випадку порушення безпеки.

Цінним видається досвід Польщі. Характерним нормативно-правовим актом, норми якого спрямовані на забезпечення фінансової безпеки в мережі, є Закон про кібербезпеку. Цей закон забезпечує загальний фреймворк для забезпечення кібербезпеки в Польщі. Він визначає обов'язки державних органів, компаній та інших організацій у відношенні кібербезпеки та встановлює вимоги до захисту інформації [8].

Варто звернути увагу на те, що у 2020 році ЄС оголосив про запуск Стратегії кібербезпеки ЄС як ключової

складової формування цифрового майбутнього Європи та Плану відновлення Європи, сприяння глобальному та відкритому кіберпростору шляхом посилення співпраці. Європейська Комісія інвестувала понад 63,5 млн. євро в чотири пілотні проекти (CONCORDIA, ECHO, SPARTA, CyberSec4Europe) [13], що виступають основою для створення європейської мережі центрів експертизи з кібербезпеки, спрямованих на удосконалення системи протидії кіберзлочинам у різних сферах суспільного життя.

Щодо нормативного регулювання кібершахраств у фінансовому секторі України, то слід відзначити декілька нормативно-правових актів у цій сфері, серед яких:

Закон України «Про захист персональних даних», який регулює збір, зберігання та обробку персональних даних, що зберігаються фінансовими установами [9];

Закон України «Про банки і банківську діяльність», що встановлює вимоги щодо захисту банківської інформації та особливості здійснення банківської діяльності в інтернеті [10];

Закон України «Про електронний цифровий підпис», норми якого регулюють використання електронного цифрового підпису для забезпечення цілісності та автентичності електронних документів [11];

Постанова Національного банку України «Про затвердження Правил забезпечення кібербезпеки в банківській діяльності», якою встановлюються вимоги до захисту банківської інформації та систем обробки банківських операцій від кібернападів [12];

Постанова Національної комісії з цінних паперів та фондового ринку «Про затвердження Правил захисту інформації на фондовому ринку», що встановлює вимоги до захисту інформації, що обробляється на фондовому ринку, від кібернападів тощо.

Вважаємо за необхідне далі виокремити окремі аспекти прогалин в нормативному регулюванні проблеми фінансових кібершахрайств.

По-перше, це відсутність чіткого визначення фінансових кібершахрастів в законодавстві України, що є серйозною проблемою, оскільки ускладнює розуміння цього виду кіберзлочинності.

На сьогодні в Україні не існує окремого закону, який би визначав фінансові кібершахрасті, тому вони часто розглядаються як окремі види злочинності, такі як шахрайство, крадіжка, використання підроблених документів тощо. Це може спричиняти певні труднощі у проведенні розслідувань та притягненні злочинців до відповідальності за їхні дії. Для боротьби з цією проблемою важливо розробляти та приймати нові нормативні акти, які б визначали та описували фінансові кібершахрайства та встановлювали відповідні покарання за їх вчинення [3, с. 237]. Такі нормативні акти повинні передбачати чітке визначення видів кібершахрастів, їхній механізм вчинення, а також способи боротьби з ними та механізми захисту від таких дій.

По-друге, це часткове регулювання збору, зберігання та використання персональних даних користувачів з метою запобігання їхнього неправомірного використання.

Україна має законодавчу базу для регулювання збору, зберігання та використання персональних даних. Зокрема, основним законом, що регулює цей процес є Закон України «Про захист персональних даних». У рамках цього закону організації, які збирають персональні дані, повинні мати згоду користувача на збір, зберігання та використання цих даних. Вони також повинні гарантувати безпеку та конфіденційність персональних даних, що зберігаються у їхніх системах. Організації також повинні повідомляти про порушення безпеки персональних даних та приймати заходи для їх запобігання [9]. Однак, досить часто відбуваються порушення цих вимог, коли персональні дані користувачів збираються та використовуються без їхньої згоди або коли вони стають жертвами кібератак, під час яких їх персональні дані можуть бути викрадені.

По-третє, це відсутність ефективного механізму контролю за діяльністю компаній, які займаються обміном криптовалют, що є однією з ключових прогалин в законодавстві України, що стосується регулювання фінансових кібершахраств.

Це дозволяє злочинцям використовувати криптовалюту для викрадення коштів та інших злочинних дій, оскільки вони можуть легко використовувати анонімні криптовалютні гаманці для приховування своєї діяльності. Українське законодавство поки не має чіткого регулювання обміну криптовалют та не встановлює обов'язкові вимоги до діяльності таких компаній. Це створює проблеми в контролі за їхньою діяльністю та може призвести до зловживання використанням криптовалют для злочинних дій.

По-четверте, це недостатня координація між різними органами державної влади та правоохоронними органами, що є серйозною проблемою в боротьбі з фінансовими кібершахрастами. Це може призводити до того, що злочинці несуть мінімальні наслідки за свої дії, оскільки різні органи не можуть ефективно співпрацювати та обмінюватися інформацією [5, с. 402]. Вважаємо, що для того, щоб боротьба з кіберзлочинністю була ефективною, необхідно створити механізми координації та співпраці між різними органами державної влади та правоохоронними органами, щоб забезпечити швидке та ефективне реагування на кіберзлочинність.

Таким чином, удосконалення нормативного регулювання кібершахраства в фінансовому секторі України є доволі важливим завданням. Окремі напрямки його вдосконалення мають стосуватися:

– підвищення свідомості користувачів інтернет-послугами. Необхідно активізувати інформаційні кампанії щодо кібербезпеки, які б включали не тільки загальні поради, але й конкретні рекомендації щодо захисту персональних фінансових даних [13];

– впровадження нових технологій. Нові технології, такі як блокчейн, можуть допомогти у забезпеченні безпеки фінансових транзакцій та захисту від шахрайства.

– спеціалізація окремих органів державної влади саме на сферу боротьби з фінансовими кібершахрайствами, які б відповідали за забезпечення кібербезпеки в фінансовому секторі та координували дії між різними зацікавленими сторонами;

– забезпечення виконання нормативних приписів. Необхідно посили забезпечення дотримання нормативних вимог до захисту фінансових даних, включаючи контроль технічних засобів захисту та відповідальність за порушення цих вимог;

– саморегулювання сфери боротьби з фінансовими кібершахрайствами. Фінансові установи можуть самостійно встановлювати внутрішні правила та процедури для забезпечення кібербезпеки власних клієнтів. Це може включати перевірку працівників, проведення регулярних аудитів та встановлення технічних засобів захисту даних;

– консультації та співпраця у сфері боротьби з фінансовими кібершахрайствами. Державні органи можуть пропонувати консультації та рекомендації фінансовим установам щодо захисту від кібернападів. Також можлива співпраця між установами та державними органами для обміну інформацією та спільної роботи над запобіганням кібершахраства [12];

– забезпечення технічних засобів захисту у сфері боротьби з фінансовими кібершахрайствами. Державні органи можуть вимагати від фінансових установ використання певних технічних засобів захисту, таких як енкриптовані з'єднання та двофакторна автентифікація, захист від DDos-атак та інших технічних засобів захисту від кібернападів. Такі вимоги можуть бути встановлені у законодавстві або вимогах регуляторів, які контролюють фінансовий сектор. Для забезпечення використання певних технічних

засобів захисту можуть бути встановлені певні стандарти та сертифікаційні вимоги, які фінансові установи повинні дотримуватися. Також можуть бути встановлені санкції за недотримання вимог щодо технічного захисту, які можуть включати штрафи або втрату ліцензій на здійснення фінансової діяльності;

– міжнародне співробітництво у сфері боротьби з фінансовими кібершахрайствами. Україна має співпрацювати з міжнародними організаціями з метою вивчення досвіду та врахування рекомендацій щодо кібербезпеки в фінансовому секторі [4, с. 9].

Висновки. Отже, проблема фінансових кібершахрайств є актуальною для всього світового порядку, зокрема і для України, відповідно, пошук сучасних інструментів боротьби з кібершахрайствами у фінансовому секторі України є нагальним питанням нормативно-правового регулювання. У зв'язку з швидким розвитком технологій та збільшенням обсягів фінансових операцій в інтернеті, ризик кібершахрайств та кібератак на фінансові установи значно зріс. Недостатність чіткої та ефективної регуляторної бази та механізмів контролю відкриває можливості для шахраїв реалізовувати свої злочинні дії та збагачуватися за рахунок відкритих прогалин системи безпеки фінансових установ, та законодавства в цілому.

Вважаємо, що з метою гарантування фінансової безпеки держави та громадян, особливо в період дії воєнного стану, необхідно постійно вдосконалювати існуючі та впроваджувати нові дієві механізми боротьби з кібершахрайствами в фінансовому секторі. До таких інструментів варто віднести законодавче регулювання та контроль за діяльністю компаній, які займаються обміном криптовалют, розробку та впровадження ефективних механізмів захисту персональних даних користувачів, використання сучасних технологій для виявлення та запобігання кібератакам та злочинам у фінансовій сфері тощо.

ЛІТЕРАТУРА

1. Quarterly threat trends & intelligence report november 2021. URL: https://info.phishlabs.com/hubfs/PhishLabs%20-%20QTTI%20Report%20-%20November%202021.pdf (date of access: 23.03.2023).

2. Прасад А. Збитки українців від кіберзлочинності торік зросли до 1 млрд грн – дослідження «ЄМА» – forbes.ua. Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії. URL: https://forbes.ua/news/zbitki-ukraintsiv-vid-kiberzlochinnosti-torik-zrosli-do-1-mlrd-grn-doslidzhennyaema-21022023 (дата звернення: 23.03.2023).

3. Біленчук П.Д Обіход Т.В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис* Київського університету права. 2018. № 3. С. 235–239.

4. Савчук Н. В. Інтернет-картинг – новий вид фінансової кіберзлочинності. «Перспективні напрямки розвитку економіки, фінансів, обліку, менеджменту та права: теорія і практика» : Зб. тез доп. міжнар. науково-практ. конф. С. 9.

5. І.О. Харитоненко. Феномен кіберзлочинності в сучасній кримінологічній теорії. *Часопис* Київського університету права. 2020. № 4. С. 401–403.

6. Українці почали вдвічі частіше стикатися з шахраями в інтернеті, найбільше – в месенджерах: результати опитування – офіційний блог olx.ua. Офіційний блог OLX.ua. URL: https://blog.olx.ua/26779/ukrainci-stali-vdvichi-chastishe-stikatisya-z-shaxrayami-v-interneti-najbilshe-v mesendzherax-rezultati-opituvannya/ (дата звернення: 23.03.2023).

7. Kuzmenko O., Kushnerov O., Dotsenko T. Improving the financial monitoring system: automation of the bank's customer verification process. Scientific opinion: economics and management. 2021. No. 2(72). URL: https://doi.org/10.32836/2521-666x/2021-72-13 (date of access: 23.03.2023).

8. Семенуха Р. Як це робила Польща: досвід боротьби з кіберзагрозами. Економічна правда. URL: https://www.epravda.com.ua/columns/2017/10/12/630044/ (дата звернення: 23.03.2023).

9. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI: станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 23.03.2023).

10. Про банки і банківську діяльність : Закон України від 07.12.2000 р. № 2121-III: станом на 5 лют. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text (дата звернення: 23.03.2023).

11. Про електронний цифровий підпис : Закон України від 22.05.2003 р. № 852-IV : станом на 7 листоп. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 23.03.2023).

12. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Нац. банку України від 28.09.2017 р. № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 23.03.2023).

13. Що знають користувачі про безпеку в інтернеті: результати опитування. URL: https://blog.olx.ua/24800/shho-znayutkoristuvachi-pro-bezpeku-v-interneti-rezultati-opituvannya/ (дата звернення: 23.03.2023).