УДК 343.85
DOI 10.33244/2617-4154.3(12).2023.194-200

О. М. Бодунова,
канд. юрид. наук, доцент,
Державний податковий університет
ORCID ID 0000-0001-9179-5985

ЗАПОБІГАННЯ КІБЕРШАХРАЙСТВУ У ФІНАНСОВОМУ СЕКТОРІ

У статті розглянуто проблеми та особливості запобігання кібершахрайству у фінансовому секторі. Зазначено, що, враховуючи сучасний етап цифровізації усіх сфер фінансового життя у світі, а також кризові явища в економіці, очевидним стає те, що проблема фінансового шахрайства стає все більш актуальною як для фізичних, так і для юридичних осіб. Щороку у процесі розвитку цифрових технологій з'являються нові види та способи шахрайства з фінансовими ресурсами, фінансове шахрайство має усі передумови та можливості до швидкої адаптації в сучасних умовах здійснення суб'єктами господарювання своєї підприємницької діяльності. Не є винятком і той факт, що фінансове шахрайство є доволі поширеним явищем на підприємствах.

Особливо актуальним це питання стало під час повномасштабної війни в Україні, оскільки кібершахрайство набуло особливих масштабів. Користуючись війною та скрутним становищем українців, злочинці маніпулюють емоційним станом людей, у такий спосіб незаконно отримуючи від них кошти.

Найбільш поширений серед нових – це фейкова соціальна допомога від державних чи міжнародних організацій. Із середини 2022 року до сьогодні за ним спостерігається найбільша активність. Так, щодня в Україні за посиланнями на шахрайські фішингові сайти переходять у середньому 10 000–15 000 громадян, які, відповідно, стають жертвами шахраїв. Застосовуючи шкідливі фішингові ресурси, злочинці намагаються ошукати громадян та отримати доступ до їхніх фінансових даних. Такі сайти в основному стилізовані під урядові портали, Дію, Є-Допомогу, під сайти українських банків, міжнародних організацій та відомих платіжних сервісів.

Звернено увагу на міжнародний досвід у цій сфері. Для протидії протиправним посяганням на електронні інформаційні ресурси має бути закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку й арешту електронних доказів, насамперед закріплення процесуально значимої можливості копіювання інформації, а також імплементація в національне законодавство положень про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, власниками ресурсу (вебсайту) із забезпеченням їх цілісності.

Ключові слова: *кіберзлочинність, кібершахрайство, воєнний стан, фішингові компанії, економічна злочинність.*

Метою наукової статті є аналіз та дослідження наукових доробків, статистичних даних і правозастосовної практики щодо запобігання шахрайству у фінансовому секторі в умовах воєнного стану в Україні.

Постановка проблеми. Розвиток світової економіки та кон'юнктура ринку призвели до зростання ролі фінансів у житті кожної людини. Запровадження безготівкових форм розрахунків, поширення мереж банків та інших фінансових установ, поява міжнародних фінансово-кредитних організацій, активне використання новітніх інформаційних технологій фінансових операцій призвели до зростання шахрайства у фінансовому секторі. Шахрайство здійснюється як внутрішніми учасниками підприємницької діяльності, так і зовнішніми суб'єктами та зачіпає інтереси учасників практично всіх сфер суспільних відносин. Шахрайство посягає на найбільш важливі економічні відносини – відносини з формування, розподілу і використання грошових коштів, завдає багатомільйонні збитки національній економіці та добробуту громадян, підриває розвиток підприємницької та інвестиційної діяльності. Боротьба із шахрайством й іншими економічними кримінальними правопорушеннями є надзвичайно складним завданням, проте за сучасного нестабільного ландшафту ризиків [1, с. 60].

Враховуючи сучасний етап цифровізації усіх сфер фінансового життя у світі, а також кризові явища в економіці, очевидним стає те, що проблема фінансового шахрайства стає все більш актуальною як для фізичних, так і для юридичних осіб. Щороку у процесі розвитку цифрових технологій з'являються нові види та способи шахрайства з фінансовими ресурсами, фінансове шахрайство має усі передумови та можливості до швидкої адаптації в сучасних умовах здійснення суб'єктами господарювання своєї підприємницької діяльності. Не є винятком і той факт, що фінансове шахрайство є доволі поширеним явищем на підприємствах. За даними проведених досліджень, в Україні близько половини підприємців у певний спосіб стають жертвами шахраїв. Це призводить до значної кількості негативних наслідків у функціонуванні суб'єктів господарювання, зокрема впливає на зниження репутації самого підприємства, а також підриває його фінансовий стан загалом. Нині шахраї володіють широким арсеналом прийомів, водночас як представники правоохоронних органів тільки починають розробляти механізми запобігання та виявлення зловживань, а більшість компанії в Україні взагалі не проводить розслідувань фінансового шахрайства [4, с. 71].

Особливо актуальним це питання стало під час повномасштабної війни в Україні, оскільки кібершахрайство набуло особливих масштабів. Користуючись війною та скрутним становищем українців, злочинці маніпулюють емоційним станом людей, незаконно отримуючи від них кошти.

Так, сума збитків банків, суб'єктів підприємницької діяльності, інших клієнтів від незаконних дій з платіжними картками за минулий рік становила 481 млн гривень. Це на 46 % більше ніж 2021 року. Кількість незаконних дій з платіжними картками, за

якими були понесені збитки, зросла торік на 8 %. Саме тому запобігання кібершахрайству у фінансовому секторі є надзвичайно актуальною темою сьогодення.

Стан опрацювання цієї проблематики. Дослідження шахрайства у фінансовому секторі здійснювали О. Барановський, С. Мельник, Дж. Т. Уеллс, С. Чернявський, Г. Чернишов та ін. Проте дослідженню особливостей, різновидів і наслідків шахрайств у фінансовому секторі, формуванню напрямів їх запобігання, особливо під час воєнного стану в Україні, приділено недостатньо уваги.

Виклад основного матеріалу. Через воєнні дії в Україні 85 % суб'єкти підприємницької діяльності вимушено вживають заходи з оптимізації бізнес-процесів. Серед цих 1 % підприємств припинили свою діяльність та не зможуть її відновити найближчим часом, а 35 % призупинили діяльність в очікуванні поліпшення економічної ситуації. Про це свідчать результати дослідження, проведеного компанією Gradus Research на замовлення Київської школи економіки [3]. Така ситуація не тільки є загрозою для економіки країни та розвитку підприємницької діяльності, але й створює додаткові можливості для корпоративного шахрайства в умовах, коли забезпечення надійності системи внутрішнього контролю не є пріоритетною статтею витрат. Проте такі дії в умовах, коли бізнес і так потерпає від кризи, є нищівними для нього.

Для оцінки рівня шахрайства з платіжними картками зазвичай аналізують не просто суму збитків, а порівнюють її із загальною сумою усіх видаткових операцій з платіжними картками. Це не набагато більше, ніж 2021 року (тоді було 65 гривень). Тож можемо констатувати, що минулого року сума збитків від шахрайства зростала зіставно до зростання загальної суми операцій з платіжними картками українських банків.

Якщо порівнювати динаміку рівня шахрайства з платіжними картками за місцем проведення операцій, то на 1 мільйон гривень операцій сума збитків від шахрайських дій 2022 року, порівняно з 2021 роком, у фізичних пристроях знизилась (у торговельній мережі – із 40 до 16 гривень, у банкоматах – з 29 до 5 гривень). Водночас рівень шахрайства в мережі «Інтернет» зріс із 114 до 133 гривень. Загалом 86 % від загальної кількості випадків минулого року відбувалося у мережі «Інтернет», тоді як лише 14 % – через фізичні пристрої (торговельна мережа, банкомати). Що стосується суми збитків від незаконних дій, 94 % припадає на мережу «Інтернет», 4 % – на торговельну мережу та 2 % – на банкомати [5].

Отже, там, де використовується фізична картка (торговельна мережа, банкомати, пристрої самообслуговування), проведення операцій наразі є більш безпечним. Адже підробити платіжну картку, щоб використати її у банкоматі чи торговельній мережі, досить складно, ніж виманити у клієнта дані картки та провести операцію в інтернеті.

Проте варто відмітити, що якщо механізми платіжного шахрайства під час війни залишаються ті самі, сценарії з'являються нові.

Найбільш поширений серед нових – це фейкова соціальна допомога від державних чи міжнародних організацій. Із середини 2022 року до сьогодні за ним спостерігається найбільша активність. Так, щодня в Україні за посиланнями на шахрайські фішингові сайти переходять у середньому 10 000–15 000 громадян, які, відповідно, стають жертвами шахраїв [5].

Застосовуючи шкідливі фішингові ресурси, злочинці намагаються ошукати громадян та отримати доступ до їхніх фінансових даних. Такі сайти в основному стилізовані під урядові портали, Дію, Є-Допомогу, під сайти українських банків, міжнародних організацій та відомих платіжних сервісів.

Людина, не усвідомлюючи, що це фейковий сайт, залишає на ньому інформацію, яку не варто розголошувати (наприклад, CVV-код, пін-код, логін та пароль для входу в інтернет-банкінг тощо). Після цього зловмисники просто крадуть її гроші з рахунків або ж психологічно тиснуть на людину, вимагаючи її здійснити платіж на користь шахраїв, тощо.

2022 року Національний банк України виявив більше 4 500 таких фішингових ресурсів. Водночас з початку 2023 року і до сьогодні вже виявлено більше 11 000 подібних шахрайських доменів. У середньому щодня виявляється більше 100 таких шахрайських ресурсів. Операторами цих шахрайств здебільшого є угрупування з росії. Приблизно дві третини з виявлених фішингових сайтів (68 %) походять з рф. Тобто, крім військової агресії, проти нас триває гібридна війна у віртуальному просторі із залученням кіберугруповань із росії [5].

Це зрозуміло навіть з текстів таких шахрайських повідомлень, які часто некоректно перекладені, у яких зустрічається багато русизмів, неправильно вжитих слів.

Саме тому проблема запобігання кібершахрайству у фінансовому секторі на сьогодні є значно важливою і потребує негайного вирішення.

У зв'язку з цим Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України спільно з Національним банком України запустили проєкт із протидії кібершахрайству у фінансовому секторі.

Основна його мета – посилити захист громадян від кіберзлочинців, які суттєво активізували діяльність у період воєнного стану в Україні. Як уже зазначали, для крадіжки коштів злочинці проводять фішингові кампанії, метою яких є виманювання даних для доступу до банківських рахунків. Обіцянки шахраїв варіюються залежно від актуальних новин, особливо тих, що стосуються надання громадянам державної та міжнародної фінансової допомоги, також вони організовують фейкові збори коштів для надання допомоги Збройним силам України.

Завдання проєкту – зменшити переходи користувачів на шахрайські сайти шляхом перенаправлення їх на сторінку з попередженням, що сайт створений зловмисниками. Результати вражають: лише за перший місяць зафіксовано близько 120 тисяч унікальних переходів на цю сторінку. Іншими словами, десятки тисяч громадян України щомісяця будуть захищеними від кримінально протиправних дій шахраїв.

Доцільно також звернути увагу на те, що 2022 року в Національному координаційному центрі кібербезпеки було створено робочу групу, до якої увійшли представники державних органів і провайдери з найбільшою інфраструктурою. Відбулося успішне тестування роботи системи захисту від фінансового фішингу. Першим великим провайдером, який активно долучився до проєкту, стала компанія Київстар, яка завжди приділяє велику увагу питанням кібербезпеки та захисту своїх абонентів від кіберзагроз.

Аналіз діяльності хакерських груп, які займаються подібним шахрайством, вказує на те, що вони діють не тільки в Україні, але і в країнах ЄС. Тому сьогодні ведуться переговори щодо обміну інформацією з відповідними органами з країн-партнерів, до яких після початку повномасштабного вторгнення виїхала значна кількість українців [2].

Отже, 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 і засобів, як не стати жертвою кібершахрайства. На спеціальному ресурсі пояснюють правила кібербезпеки й надають поради українцям, як надійніше захистити свої гроші. У межах кампанії Національний банк України разом із партнерами інформують 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. Варто наголосити, що кіберзлочинність має специфічні причини і боротьба з нею також передбачає застосування специфічних засобів.

Потрібно звертати увагу і на міжнародний досвід у цій сфері. Для протидії протиправним посяганням на електронні інформаційні ресурси має бути закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку й арешту електронних доказів, насамперед закріплення процесуально значимої можливості копіювання інформації, а також імплементація в національне законодавство положень про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, власниками ресурсу (вебсайту) із забезпеченням їх цілісності. ООН та її спеціалізовані установи й організації, мета діяльності яких передбачає забезпечення мирного існування та перевагу дипломатії над воєнним характером відносин, відіграє велику роль у боротьбі з кіберзлочинністю та кібершахрайством. Прийняття ряду правових актів спрямовані на підтримку інформаційної безпеки та боротьби і попередження кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Нежива М. О., Мисюк В. О. Протидія шахрайству в умовах війни. *Бізнес-інформ.* 2023. № 1. С. 160–166.

2. Стартував проєкт із протидії кібершахрайству у фінансовому секторі / Офіційний сайт Національного банку України. URL : https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori

3. Тарасовський Ю. Як український бізнес працює під час війни. Головні факти з дослідження Gradus Research. *Forbes.* 23.03.2022. URL : https://forbes.ua/ news/v-ukraini-35-biznesu-prizupinili-diyalnist-cher-ez-viynu-1-ne-planuyut-vidnovlennya-opituvannya-gradus-23032022-4950

4. Шикун В., Булик Д. Фінансове шахрайство на підприємствах та методи його запобігання. *Економічний часопис Волинського національного університету імені Лесі Українки.* 2023. № 1. С. 70–79.

5. Як протидіяти кібершахрайству у фінансовому секторі / Офіційний сайт видання The page. URL : https://thepage.ua/ua/news/yak-protidiyati-kibershahrajstvu-u-finansovomu-sektori

REFERENCES

1. Nezhyva M. O., Mysiuk V. O. Protydiia shakhraistvu v umovakh viiny. *Biznesinform.* 2023. № 1. S. 160–166.

2. Startuvav proiekt iz protydii kibershakhraistvu u finansovomu sektori / Ofitsiinyi sait Natsionalnoho banku Ukrainy. URL : https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori

3. Tarasovskyi Yu. Yak ukrainskyi biznes pratsiuie pid chas viiny. Holovni fakty z doslidzhennia Gradus Research. *Forbes.* 23.03.2022. URL : https://forbes.ua/ news/v-ukraini-35-biznesu-prizupinili-diyalnist-cher-ez-viynu-1-ne-planuyut-vidnovlennya-opituvannya-gradus-23032022-4950.

4. Shykun V., Bulyk D. Finansove shakhraistvo na pidpryiemstvakh ta metody yoho zapobihannia. *Ekonomichnyi chasopys Volynskoho natsionalnoho universytetu imeni Lesi Ukrainky.* 2023. № 1. S. 70–79.

5. Yak protydiiaty kibershakhraistvu u finansovomu sektori / Ofitsiinyi sait vydannia The page. URL : https://thepage.ua/ua/news/yak-protidiyati-kibershahrajstvu-u-finansovomu-sektori

O. Bodunova. Preventing cyber fraud in the financial sector

The article examines the problems and peculiarities of preventing cyber fraud in the financial sector. It is noted that given the current stage of digitalization of all spheres of financial life in the world, as well as the crisis in the economy, it is obvious that the problem of financial fraud is becoming increasingly relevant for both individuals and legal entities. Every year, as digital technologies develop, new types and methods of fraud with financial resources emerge, and financial fraud has all the prerequisites and opportunities for rapid adaptation in the current conditions of business activities of business entities. It is no exception that financial fraud is a fairly common phenomenon at enterprises.

This issue has become particularly relevant during the full-scale war in Ukraine, as cyber fraud has become particularly widespread. Taking advantage of the war and the difficult situation of Ukrainians, criminals manipulate the emotional state of people, thus illegally obtaining funds from them.

The most common of the new scams is fake social assistance from government or international organizations. From mid-2022 to the present, it has been the most active. For example, an average of 10,000–15,000 people in Ukraine follow links to fraudulent phishing sites every day, and fall victim to fraudsters. Using malicious phishing resources, criminals try to deceive citizens and gain access to their financial data. Such sites are mostly stylized as

government portals, Diia, E-Dopomoga, websites of Ukrainian banks, international organizations and well-known payment services.

Attention is drawn to international experience in this area. In order to counteract unlawful encroachments on electronic information resources, it is necessary to establish a mechanism for prompt restriction (blocking) of a certain information resource (information service) and to introduce special conditions for search and seizure of electronic evidence, first of all, to establish a procedurally significant possibility of copying information, and also to implement into national legislation the provisions on immediate recording and further storage of data by operators, telecommunications providers, owners of a resource (website) with.

Keywords: *cybercrime, cyberfraud, martial law, phishing companies, economic crime.*

Стаття надійшла до редколегії 5 травня 2023 року