УДК 343.72:004(477)
DOI https://doi.org/10.24144/2788-6018.2024.02.106

ШАХРАЙСТВО В ІНТЕРНЕТІ ЯК ОДИН ІЗ ВИДІВ ШАХРАЙСТВА

Чекмарьова І.М.,
кандидат юридичних наук, доцент,
професор кафедри кримінального права та кримінології
ФПФОДР Одеського державного університету внутрішніх справ.
ORCID: 0000-0003-3167-2144

Чекмарьова І.М. Шахрайство в Інтернеті як один із видів шахрайства.

Стаття є дослідженням актуальних аспектів шахрайства в Інтернеті в умовах пандемії коронавірусу та російсько-української війни. Зростання використання Інтернету під час карантину та воєнного стану створює нові можливості для шахраїв, які використовують цю ситуацію для обдурювання людей. Емоційна нестабільність, фінансові проблеми та поширення дезінформації також сприяють зростанню шахрайства в мережі. Стаття аналізує законодавчий підхід до боротьби з шахрайством в Україні та визначає особливості цього виду кримінального правопорушення. Завдяки доступності Інтернету, шахраї швидко адаптували свої схеми до цифрового середовища, що робить користувачів мережі більш вразливими.

У статті досліджується різноманітність методів та видів шахрайства в Інтернеті, зокрема фішинг, шахрайство в сфері криптовалют, соціальна інженерія та інші схеми. Автори наводять дані звіту «Data Breach and Incident Response» (DBIR). Детально розглядаються такі методи, як фішинг, фармінг, шахрайство через соціальні мережі та електронну пошту, а також маніпуляції з ICO та криптоінвестиційними фондами. Окрема увагу приділяється шахрайству в умовах війни, де згадується про збір коштів для військових, обманні схеми з родинними оголошеннями та фейкові повідомлення про евакуацію. Оцінюється рівень вразливості користувачів, особливості географії та вікова категорія, яка найчастіше стає жертвами інтернет-шахрайства. В статті також розглядається аспект комп'ютерної техніки, мобільних пристроїв та інших засобів доступу до Інтернету, які використовуються зловмисниками для здійснення шахрайських дій.

Автори наголошують на поширенні шахрайств в Інтернеті, де зловмисники намагаються зламати веб-сайти урядових організацій, банків або медіа з метою отримання конфіденційної інформації або поширення фейкових новин. Пропонуються заходи для боротьби з цим явищем. Детально розглядаються різні види шахрайства в Інтернеті та методи їх запобігання, включаючи оновлення програмного забезпечення, встановлення антивірусного програмного забезпечення, використання сильних паролів та двофакторної аутентифікації. Зазначається, що усвідомленість та відповідальний підхід до захисту в Інтернеті є ключем до запобігання шахрайству. Крім того, обговорюється кримінальна відповідальність за шахрайство в Україні та можливість посилення цієї відповідальності в умовах воєнного стану.

Ключові слова: інтернет-шахрайство, воєнний стан, інформаційна безпека, антивірусне програмне забезпечення, кримінальна відповідальність, заходи захисту, протидія шахрайству, громадська безпека.

Chekmaryova I.N. Internet fraud as one of the types of fraud.

The article investigates the current aspects of internet fraud in the context of the coronavirus pandemic and the Russian-Ukrainian war. The increased use of the Internet during quarantine and wartime creates new opportunities for scammers, who exploit this situation to deceive people. Emotional instability, financial problems, and the spread of misinformation also contribute to the growth of fraud online. The article analyzes the legislative approach to combating fraud in Ukraine and identifies the specifics of this type of criminal offense. Due to the accessibility of the Internet, scammers quickly adapt their schemes to the digital environment, making network users more vulnerable.

The explores the diversity of methods and types of internet fraud, including phishing, cryptocurrency fraud, social engineering, and other schemes. The authors provide data from the «Data Breach and Incident Response» (DBIR) report. Methods such as phishing, farming, fraud through social media and email, as well as manipulations with ICOs and crypto investment funds, are examined in detail. Special attention is paid to fraud in wartime, mentioning fundraising for military purposes, deceptive schemes with family announcements, and fake evacuation messages. The level of vulnerability of users,

geographical features, and the age category most often targeted by internet fraud are evaluated. The article also discusses the aspect of computer equipment, mobile devices, and other means of accessing the Internet used by criminals to carry out fraudulent activities.

The authors emphasize the prevalence of internet fraud, where perpetrators attempt to hack websites of government organizations, banks, or media to obtain confidential information or spread fake news. Measures to combat this phenomenon are proposed. Various types of internet fraud and methods of prevention are examined in detail, including software updates, installation of antivirus software, use of strong passwords, and two-factor authentication. It is noted that awareness and a responsible approach to protection on the Internet are key to preventing fraud. Additionally, the criminal liability for fraud in Ukraine and the possibility of strengthening this liability in wartime are discussed.

Key words: internet fraud, wartime, information security, antivirus software, criminal liability, protective measures, awareness-raising, fraud prevention, public safety.

Постановка проблеми. Шахрайство в Інтернеті стало особливо актуальним в умовах пандемії коронавірусу та російсько-української війни з кількох причин:

По-перше, зростання використання Інтернету: у зв'язку з обмеженнями під час воєнного стану і карантинними заходами, люди стали активніше користуватися Інтернетом для здійснення покупок, отримання інформації та зв'язку з оточуючим світом. Це створює більше можливостей для шахраїв залучити нових жертв.

По-друге, емоційна уразливість: пандемія та війна породили страх, тривогу та нестабільність в суспільстві. Шахраї використовують ці емоційні переживання, щоб обдурити людей, запропонувавши шахрайські схеми захисту від вірусу, військові благодійні фонди тощо.

По-третє, фінансові труднощі: багато людей втратили роботу або стали стикатися з економічними труднощами. Шахраї використовують події в країні, щоб запропонувати фіктивні можливості заробітку або фінансову допомогу.

Необхідно згадати і про дезінформацію: в умовах війни шахраї можуть використовувати дезінформацію для просування своїх інтересів. Вони поширюють фейкові новини, листи-ланцюги та іншу неправдиву інформацію, щоб отримати доступ до особистої інформації або грошей.

Та ще одна причина – це зміна поведінки користувачів: зміна у звичках користувачів Інтернету, таких як збільшення кількості онлайн-покупок, робить їх більш вразливими перед шахраями, які можуть створити фальшиві веб-сайти або надіслати шахрайські електронні листи.

Отже, в умовах останніх викликів шахрайство в Інтернеті стає ще більш поширеним через зростання використання Інтернету, емоційну уразливість, фінансові труднощі, дезінформацію та зміну поведінки користувачів.

Мета дослідження – проаналізувати розвиток шахрайства в інтернеті на тлі сучасних подій в Україні.

Стан опрацювання проблематики. Шахрайство в Інтернеті є об'єктом досліджень для багатьох вчених з усього світу. Деякі з найвідоміших дослідників в цій галузі включають:

Джоана Баррі (Joanne Barrick) – професор психології та експерт у галузі кібербезпеки, яка досліджує соціальний інженерінг та шахрайство в Інтернеті.

Роберт С. Соловей (Robert S. Soloway) – американський експерт з кібербезпеки, який спеціалізується на вивченні шахрайства в електронній пошті та соціальному інженерінгу.

Тайлер Мур (Tyler Moore) – професор інформаційних технологій та менеджменту в університеті Тулан, який досліджує кіберзлочинність, включаючи шахрайство в Інтернеті.

Сергій Демешкін (Sergey Demeshkin) – вітчизняний експерт з кібербезпеки та викладач, який активно досліджує кіберзлочинність в Україні, включаючи шахрайство в Інтернеті.

Микола Пенський (Mykola Penskyi) – український науковець із Інституту кібербезпеки в Києві, який спеціалізується на аналізі кіберзлочинності, включаючи шахрайство в Інтернеті.

Ці вчені та багато інших активно працюють над розумінням проблеми шахрайства в Інтернеті та розробкою стратегій для її запобігання та боротьби.

Виклад основного матеріалу. Шахрайство є поширеним видом кримінального правопорушення проти власності у багатьох кримінально-правових системах, включаючи українську. Такі злочини призводять до серйозних фінансових втрат, які можуть перевищувати десятки або навіть сотні тисяч гривень. З огляду на тенденцію до зростання кількості випадків розкрадань через шахрайство, боротьба з такими правопорушеннями є одним з основних пріоритетів правоохоронних органів. Ці злочини не лише ставлять під загрозу власність окремих осіб, але й наражають на ризик ефективне функціонування економічної системи держави [12].

Відповідно до статті 190 Кримінального кодексу України шахрайством є заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [5]. Серед особливостей шахрайства є те, що воно може бути вчинено як стосовно майна, так і стосовно права на таке майно. Шахрайство завжди повин-

но містити в собі прямий умисел на заподіяння саме шахрайства, а також мати корисливі мотиви вчинення.

З моменту, коли Інтернет набув розвитку в Україні та доступ до нього має майже кожна людина незалежно від вікової категорії, шахраї швидко почали використовувати цю можливість для своїх злочинних дій. Привабливість умов, що полягають у відсутності можливості безпосереднього контакту з особою, викликає зацікавленість зловмисників і стимулює їх до розробки різних злочинних схем для заволодіння майном, коштами та цінностями інших осіб.

Серед основних характеристик Інтернет-шахрайства можна виділити наступні:

– високий рівень прихованості;
– різноманітність методів скоєння злочину (спричинена широким спектром послуг у Інтернеті);
– глобальний характер (не обмежений чіткими кордонами);
– складність виявлення та запобігання таким діям.

Найпоширеніші види інтернет-шахрайства включають [2, с. 449]:

Фішинг – це спроби здійснення доступу до особистої інформації, такої як паролі, банківські реквізити, за допомогою підроблених веб-сайтів або електронних листів, що виглядають як легітимні.

Атаки «мані-в-середині»: це коли зловмисники впливають на звички користувачів, намагаючись їх переконати надіслати гроші або розкрити конфіденційну інформацію.

Малваре – це програмне забезпечення, яке шкідливим чином впливає на комп'ютер або пристрій, зазвичай для викрадення інформації або шантажу.

Різноманітні схеми: включають в себе фальшиві лотереї, пропозиції про роботу або інші обмани, що вимагають від користувачів оплати за якесь навмисне обманювання.

Кібербулінг – це використання Інтернету для психологічного та емоційного тиску на інших людей, зазвичай за допомогою соціальних мереж або онлайн-платформ.

Одним з основних методів шахрайських схем є обман користувачів через різноманітні маніпуляції на сайтах розіграшів, лотерей або оферт роботи в Інтернеті. За даними статистики, зібраної користувачами Інтернету, банками, їх клієнтами та органами кіберполіції, більшість випадків шахрайства припадають на ці види діяльності. Наступними в рейтингу є фальшиві онлайн-магазини та пропозиції навчання за вивченням матеріалів. Значну частку у схемах шахрайства займають сайти, що пропонують інвестувати кошти в різноманітні види бізнесу з обіцянкою високих прибутків. Також серед поширених схем є сайти, які обіцяють заробіток на соціальних опитуваннях та вимагають оплату реєстрації. На пострадянському просторі широко поширеною є пропозиція участі в азартних іграх. Деякі сайти швидких кредитів пропонують сплатити комісію за отримання кредиту, але фактично не надають грошей, вимагаючи банківські дані та гроші від клієнтів. Крім того, деякі веб-ресурси пропонують компенсацію за медичні витрати, соціальні виплати чи перерахунки податків, з метою збору особистих та банківських даних для шахрайських маніпуляцій.

Один з видів шахрайства в Інтернеті є фішинг, який використовується для отримання конфіденційної інформації, шляхом неправдивих приводів, створених зловмисниками. Часто цей метод шахрайства називають «підводним полюванням» або фішинг-атаками. За даними звіту «Data Breach and Incident Response» (DBIR), фішинг був основним методом атак в 32% випадків всіх витоків даних. Зазвичай це виявляється у вигляді надсилання електронних листів з проханням підтвердити реєстрацію облікового запису, з посиланням на сайт, який виглядає точно так само, як оригінальний. Це змушує користувачів самостійно вводити конфіденційну інформацію. Ще одним варіантом фішингу є фармінг, коли зловмисники змінюють DNS (Domain Name System) адресу сайту, але інтерфейс залишається незмінним, щоб користувачі могли несумнівно вводити особисті дані на фальшивому сайті, вважаючи його за оригінал [9, с. 69].

Найпоширенішими шахрайськими схемами у сфері криптовалют є наступні: обман через соціальні мережі, використання соціальної інженерії, шахрайство під час нерегульованого обміну криптовалюти, фішингові атаки через електронну пошту, маніпуляції з ICO (Initial Coin Offering), криптоінвестиційні фонди, а також шахрайство в хмарному майнінгу.

Також широко поширені наступні шахрайські схеми: телефонні шахрайства, продаж неіснуючих товарів, обманні розіграші, фішингові ресурси для отримання особистих даних, а також зловживання довірою для заволодіння коштами під виглядом обіцяних виграшів або прохань про допомогу у соціальних мережах. Серед шахрайств з платіжними картками, як в Україні, так і в усьому світі, залишається популярним метод соціальної інженерії, коли люди самі передають гроші шахраям або розкривають їм дані своїх карток [11, с. 419].

Важливо відзначити широке поширення шахрайства, що виникає при спілкуванні на романтичні теми з вимаганням коштів у майбутньому. Злочинці активно використовують соціальні мережі для пошуку потенційних жертв, спираючись на психологічні характеристики,

такі як вік, відсутність активності в мережі, чи професійні досягнення. Надсилають заздалегідь підготовлені листи з пропозицією розпочати спілкування, часто вигадуючи історії про службу в армії або участь у міжнародних місіях для створення довіри. Навіть при поверхневому огляді ця модель шахрайства може виявитися ефективною, особливо з урахуванням доступності особистої інформації, використання технологій штучного інтелекту для автоматизації шахрайських сценаріїв та впливу на поведінку людей через персоналізоване середовище та профілювання в інтернеті [3, с. 117].

Окремо варто відзначити види шахрайств через Інтернет, які відбуваються в умовах війни, такі як збір коштів для військових, шахрайства, пов'язані з оголошеннями про зникнення рідних або їх потрапляння в полон, а також обманні схеми, які використовують фейкові повідомлення про евакуацію за умови передплати або фінансову допомогу.

В умовах збройної агресії з боку рф українці стали більш вразливими емоційно, і злоумисники реагують на ці зміни, використовуючи актуальні проблеми суспільства в своїх шахрайських схемах. До інструментів для здійснення онлайн-шахрайства варто віднести комп'ютерну техніку, мобільні пристрої та інші універсальні пристрої, за допомогою яких можна збирати, отримувати або переглядати конкретні дані. На думку деяких експертів, до засобів шахрайства також слід віднести доступ до Інтернету та пристрої для його отримання і передачі, такі як маршрутизатори або роутери, а також банківські рахунки підставних осіб та картки [8, с. 288].

Географія інтернет-шахрайства в умовах воєнного стану широка і охоплює всі області країни. Більшість кримінальних правопорушень цього типу вчиняють чоловіки у віці від 21 до 55 років, з основною кількістю випадків у віці від 30 до 42 років, але також трапляються випадки вчинення неповнолітніми. Жінки становлять приблизно 20% від усіх випадків інтернет-шахрайства і, головним чином, використовують соціальні мережі для розміщення фейкових оголошень про продаж товарів або здачу в оренду житла [1, с. 176].

Атаки на інфраструктуру стають все більш поширеними. Шахраї можуть намагатися зламати веб-сайти урядових організацій, банків або медіа для отримання конфіденційної інформації або для поширення фейкових новин, які спричиняють паніку серед населення.

Для боротьби з інтернет-шахрайством в умовах воєнного стану необхідно підвищити рівень інформаційної безпеки, проводити агітаційні кампанії з підвищення обізнаності населення та забезпечувати оперативний обмін інформацією між урядовими структурами, громадськістю та медіа [4, с. 73].

Інтернет-шахрайство є глобальною проблемою, яка потребує комплексного підходу до захисту. Освіта та інформування є ключовими аспектами протидії онлайн-шахрайству. Кожен повинен бути обізнаний з різними формами шахрайства та знати, як вони виглядають, щоб ефективно уникнути потенційних небезпек. Важливо регулярно оновлювати програмне забезпечення та операційні системи, оскільки вони часто містять важливі патчі безпеки. Встановлення антивірусного програмного забезпечення та його регулярне оновлення може допомогти у виявленні та блокуванні зловмисних програм та веб-сайтів. Користувачам слід бути обережними з електронними листами або повідомленнями, які містять підозрілі посилання або вкладення, та уникати їх відкриття. Для захисту особистої інформації важливо використовувати сильні та унікальні паролі для різних онлайн-акаунтів. Варто розглянути використання менеджера паролів для зберігання та генерації складних паролів. Двофакторна аутентифікація може додатково забезпечити захист акаунтів від несанкціонованого доступу.

Користувачам варто бути особливо уважними при наданні своєї особистої та фінансової інформації в Інтернеті. Перед введенням будь-яких даних важливо переконатися, що веб-сайт є надійним і безпечним. Перевірка SSL-сертифіката веб-сайту, який зазвичай позначається як замок біля URL, може допомогти визначити його надійність [10, с. 53].

Усвідомленість потенційних онлайн-загроз та відповідальний підхід до захисту в Інтернеті є ключем до запобігання шахрайству. Постійне навчання та розуміння нових методів шахрайства забезпечать захист від різних онлайн-загроз.

Кримінальна відповідальність за шахрайство в Україні визначається положеннями Кримінального кодексу. Шахрайство зазвичай описується як дії, спрямовані на отримання вигоди через обман або зловживання довірою.

У традиційних умовах, відповідальність за шахрайство може включати штрафи, конфіскацію майна, обмеження волі, а у важких випадках – позбавлення волі на певний термін, залежно від серйозності злочину, його обставин та наслідків.

У період воєнного стану кримінальна відповідальність за шахрайство та інші економічні злочини може бути посилена. Військові дії, надзвичайні ситуації та інші кризові умови можуть спонукати зловмисників до активних дій, використовуючи хаос, паніку та невизначеність ситуації в свою користь [6].

Під час введення воєнного стану уряд може приймати додаткові заходи для захисту населення від шахрайства. Це може включати збіль-

шення штрафів, покарань та введення додаткових обмежень для забезпечення громадського порядку та безпеки.

Для ефективної протидії шахрайству під час воєнного стану важливо забезпечити підвищену громадську обізнаність про потенційні злочини та шахрайські схеми. Громадяни повинні знати, як виявляти та повідомляти про шахрайські дії, а правоохоронні органи повинні бути готові реагувати швидко та ефективно на такі злочини, забезпечуючи безпеку громадян у період невизначеності.

Розуміння різновидів шахрайств не є достатнім для ефективної боротьби з цими злочинами. Ключовими є оволодіння основними стратегіями протидії онлайн шахрайству [7, с. 51]:

1. Захист інформації – використання надійного шифрування для захисту конфіденційної інформації та регулярне поновлення системи безпеки.
2. Освіта і підготовка – організація навчання для персоналу з метою вчасного розпізнавання та запобігання онлайн шахрайству.
3. Моніторинг мережі – постійний контроль мережі на наявність шкідливого програмного забезпечення та надзвичайних активностей.
4. Співпраця з іншими організаціями – встановлення партнерських зв'язків з іншими агентствами, включаючи військові підрозділи.
5. Розробка кризового плану – створення плану реагування на кібератаки та інші загрози.

Це лише загальний огляд, і насправді боротьба з онлайн шахрайством вимагає індивідуального підходу, адаптованого до конкретних умов та потреб. Узагальнюючи, ефективна протидія онлайн шахрайству вимагає поєднання технічних рішень, освіти та співпраці всіх зацікавлених сторін. Тільки через спільні зусилля можна забезпечити вищий рівень кібербезпеки та захист інтересів у цифровому просторі.

Висновки. З розвитком Інтернет-технологій та загальної інформатизації суспільства відкриваються широкі можливості доступу до інформації, проте це також ставить питання про обережність та захист персональних даних в цифровому середовищі.

Щороку можливості шахраїв зростають швидше порівняно з заходами протидії їм. Розуміння схем шахрайства в Інтернеті може допомогти людям захистити себе від дій зловмисників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Брисковська О.М., Гелемей М.О. Особливості вчинення шахрайства в мережі Інтернет в умовах воєнного стану. *Київський часопис права*, (3), 2023. С. 174–180.
2. Демидов З.Г., Колмик О.О. Фішинг-як шахрайство у мережі. *Study of modern problems of civilization*, 2020. С. 448–450.
3. Дубина В.Є., Калякін С.В. Попередження шахрайства і торгівлі людьми в кіберпросторі. Протидія кіберзлочинності та торгівлі людьми: *зб. матеріалів міжнар. наук. – практ. конф. (м. Вінниця, 31 трав. 2023 р.).* Вінниця: ХНУВС, 2023. С. 116–118.
4. Колісник Т.П. Інтернет-шахрайства в умовах воєнного стану. Кібербезпека в Україні: правові та організаційні питання = *Cybersecurity in Ukraine: Legal and Organizational Issues: матеріали Міжнар. наук. – практ. конф. МВС України, Одес. держ. ун-т внутр. справ.* Одеса: ОДУВС, 2023. С. 71–73.
5. Кримінальний кодекс України: Закон України від 05 квітня 2001 року № 2314-III. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text (дата звернення: 21.03.2024).
6. Кришевич О.В. Особливості кваліфікації шахрайства під час воєнного часу. URL: https: // dspace.oduvs.edu.ua/ server/api/core/bitstreams/0302753f–792b–4576-aef1-c7ab7cf72af5/content#page=101 (дата звернення: 21.03.2024).
7. Орлов Р.Р. Різновиди онлайн шахрайств та методи протидії злочинам у мережі Інтернет. Застосування інформаційних технологій у правоохоронній діяльності: *матеріали Круглого МВС України, Харк. нац. ун-т внутр. справ, ф-т № 6, каф. кібербезпеки та DATA-технологій.* Харків: ХНУВС, 2023. С. 50–52.
8. Павлова Н.В. Основні профілактичні заходи при розслідуванні кримінальних правопорушень, вчинених шляхом шахрайства. *Вісник Луганського навчально-наукового інституту імені Е.О. Дідоренка*, (1), 2023. С. 288–298.
9. Сабадаш І., Думанський Н. Методи шахрайства у мережі Інтернет. *Інформація, комунікація, суспільство 2020: матеріали 9-ї Міжнародної наукової конференції*. 2020. С. 68–69.
10. Самойленко О.А. Класифікація способів вчинення інтернет-шахрайств. *Редакційна колегія*, 2021. С. 52–55.
11. Севрук І.Ю. Види шахрайств, що вчиняється через мережу інтернет. *Редакційна колегія*, 2023. С. 418–421.
12. Чайка І. Стан наукового розроблення проблем запобігання шахрайству в кримінологічній та кримінально-правовій науці України. URL: http://pravoisuspilstvo.org.ua/ archive/2022/1_2022/30.pdf (дата звернення: 21.03.2024).