

СЕКЦІЯ 5 ПРИКЛАДНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

УДК 343.359

*Андрусиник Ангеліна Володимирівна
(наук. керівник – д-р філол. наук, професор Шкіцька І. Ю.)
Західноукраїнський національний університет, м. Тернопіль*

СУЧАСНІ ТЕНДЕНЦІЇ ТА ФОРМИ ІНТЕРНЕТ-ШАХРАЙСТВА

Анотація. Тези присвячено аналізу актуальної кримінальної проблеми – інтернет-шахрайства, його різноманітних форм і характеристик. Розглянуто найбільш поширені шахрайські схеми та їх соціально-економічні наслідки. Обґрунтовано необхідність комплексного підходу до протидії інтернет-шахрайству, що передбачає підвищення обізнаності населення, вдосконалення технічних засобів захисту та оптимізацію нормативно-правової бази.

Ключові слова: інтернет-шахрайство, кібербезпека, зловмисники, цифрове середовище, персональні дані, онлайн-торгівля.

Шахрайство в онлайн-середовищі є актуальною кримінальною проблемою, що проявляється в різноманітних формах, включно з телефонним, інтернет-та поштовим шахрайством, а також інвестиційними аферами, спрямованими на протиправне заволодіння майном, коштами або особистою інформацією шляхом обману та зловживання довірою людей. За об'єктом атаки виокремлюють шахрайство з банківськими картками, страхове шахрайство та крадіжку особистих даних.

Від початку широкого розповсюдження мережі Інтернет в Україні та забезпечення доступу до неї практично для всіх категорій громадян спостерігається оперативне використання цифрового середовища зловмисниками для здійснення протиправної діяльності. Привабливість умов, що характеризуються відсутністю прямого міжособистісного контакту, зумовлює зацікавленість правопорушників та слугує стимулом для розробки різноманітних кримінальних схем, спрямованих на незаконне заволодіння майном, грошовими коштами та іншими цінностями фізичних і юридичних осіб.

Ключовими характеристиками інтернет-шахрайства є:

- 1) високий ступінь прихованості та анонімності;
- 2) опосередкований контакт із потенційною жертвою;
- 3) різноманітність методів вчинення протиправних діянь (обумовлена широким спектром послуг, доступних в інтернеті);
- 4) глобальний характер (відсутність чітких територіальних обмежень);
- 5) складність виявлення та запобігання зловмисним діям [2].

До найбільш розповсюджених форм протиправної діяльності в інтернеті належать такі види шахрайства:

1. Схеми зі спадкоємством. Такі махінації передбачають розсилання електронних повідомлень, що імітують офіційне інформування про наявність значного спадку від невідомих або віддалених родичів, з подальшим зверненням до потенційного отримувача з проханням про здійснення попереднього грошового пере-

казу, необхідного для врегулювання формальних юридичних процедур, пов'язаних з оформленням спадщини.

2. Маніпуляції у сфері онлайнової торгівлі – зловмисні дії через імітацію зацікавленості у придбанні товару через інтернет, з подальшим надсиланням продавцю сфальсифікованого платіжного документа (зокрема банківського чека), сума якого штучно завищена відносно узгодженої вартості товару. Під час цього шахрай пропонує продавцю повернути різницю між вказаною сумою та ціною товару, що призводить до фінансових втрат продавця після відправлення товару та виявлення фіктивності платіжного документа.

3. Емоційне шахрайство на платформах онлайн-знайомств. Ідеться про встановлення зловмисником тривалого емоційного контакту з користувачем платформи знайомств із метою подальшого отримання від нього грошових коштів під різноманітними вигаданими приводами, часто пов'язаними з обіцянкою майбутньої особистої зустрічі, після чого шахрай припиняє будь-яке спілкування та знищує з отриманими коштами.

4. Фішингові атаки – масове розсилання електронних листів або інших видів електронних повідомлень, що маскуються під офіційні повідомлення від легітимних організацій, зокрема банківських установ або платіжних систем. Ці повідомлення містять гіперпосилання, що ведуть на фальшиві вебсайти, які візуально імітують справжні ресурси, з метою незаконного збору конфіденційних персональних даних користувачів, включно з логінами, паролями та платіжною інформацією, часто під загрозою блокування облікових записів або фінансових рахунків.

5. Шахрайські операції з використанням підроблених банківських карток. У такий спосіб зловмисники пропонують громадянам отримання кредитних платіжних карток із необґрунтовано високим кредитним лімітом та аномально низькою відсотковою ставкою за умови попередньої сплати певної суми у вигляді обов'язкової абонентської плати або комісії, що є ознакою шахрайства. Як наслідок, громадяни втрачають кошти і не отримують обіцяних платіжних інструментів.

6. Соціальна інженерія під виглядом термінової допомоги. Так, шахраї через різні канали електронної комунікації (месенджери, соціальні мережі, електронну пошту) розсилають повідомлення, що надходять нібито від імені знайомих, друзів або родичів, із терміновим проханням про надання фінансової допомоги у зв'язку з раптовими та непередбачуваними обставинами (хвороба, нещасний випадок тощо) [1].

7. Схеми дистанційного псевдопрацевлаштування. Ідеться про пропозиції потенційним здобувачам роботи високооплачуваних вакансій із можливістю дистанційного виконання завдань, що супроводжується вимогою попередньої оплати певних матеріалів, спеціалізованого обладнання, реєстраційних внесків або оплати за навчання, що є ознакою шахрайства та призводить до фінансових втрат без фактичного працевлаштування.

8. Маніпуляції з використанням фальшивих повідомлень про вірусне зараження. Зазвичай це має вигляд розміщення на вебсайтах оманливих попереджень, що імітують системні повідомлення про виявлення шкідливого програмного забезпечення на комп'ютері користувача, з одночасною пропозицією перейти за

вказаним гіперпосиланням та здійснити платіж за нібито необхідну процедуру «очищення» системи від вірусів, що є спробою отримання коштів шляхом обману та може призвести до встановлення шкідливого програмного забезпечення.

Інтернет-шахрайство є складним соціально-економічним явищем, що чинить деструктивний вплив не лише на індивідуальному рівні, але й зумовлює негативні наслідки для суспільства загалом. До основних проявів цих наслідків належать:

1. *Матеріальні збитки та фінансова дестабілізація.* Жертви шахрайських схем зазнають прямих фінансових втрат, що може призводити до значних матеріальних труднощів, погіршення їхнього економічного становища та зростання соціальної незахищеності.

2. *Компрометація персональних даних та супутні злочини.* Неправомірне заволодіння особистою інформацією внаслідок шахрайських дій створює передумови для подальшої протиправної діяльності, включно з крадіжкою ідентифікаційних даних, несанкціонованим відкриттям банківських рахунків та вчиненням інших фінансових злочинів від імені потерпілих. Не менш істотними є психологічні наслідки для жертв шахрайства: відчуття обману, розгубленості, емоційного дискомфорту та потенційного психологічного травмування, що негативно позначається на їхньому ментальному здоров'ї та реалізації в соціумі.

3. *Втрата соціальної довіри та інституційна криза.* Поширення шахрайських практик у віртуальному просторі призводить до зниження рівня довіри між громадянами, підриває авторитет державних і фінансових інституцій, а також зменшує загальний рівень довіри суспільства до цифрових технологій та онлайнової комунікації.

Для ефективної протидії явищу інтернет-шахрайства необхідно впроваджувати комплекс взаємопов'язаних заходів, що охоплюють різні аспекти цієї проблеми:

1. Підвищення рівня обізнаності населення. Одним із ключових елементів боротьби з інтернет-шахрайством є систематичне та всебічне інформування громадян про наявні різновиди шахрайських схем, їх характерні ознаки та ефективні методи запобігання. Проведення освітніх кампаній, розповсюдження інформаційних матеріалів і організація тематичних заходів сприятимуть підвищенню пильності та критичного мислення користувачів інтернету.

2. Впровадження та постійне вдосконалення технічних засобів захисту. Фінансові установи, телекомунікаційні компанії та інші організації, що використовують конфіденційну інформацію та здійснюють онлайн-транзакції, повинні активно використовувати та безперервно модернізувати найновіші технологічні рішення для забезпечення кібербезпеки своїх систем та захисту даних користувачів від несанкціонованого доступу та шахрайських дій.

3. Оптимізація нормативно-правової бази. Державам необхідно розробляти та впроваджувати законодавство, що передбачає сувору відповідальність за скоєння інтернет-шахрайства, визначає чіткі процедури розслідування та кримінального переслідування осіб, причетних до таких злочинів, а також сприяє міжнародній співпраці в боротьбі з транскордонною кіберзлочинністю. Удосконалення

правового поля є важливим чинником для забезпечення ефективного правозастосування та стримування протиправної діяльності в онлайновому середовищі [3].

Отже, шахрайство в інтернеті є гострою кримінальною проблемою в Україні, яка характеризується різноманітністю форм, високим ступенем прихованості, глобальним характером та складністю виявлення. Протиправні дії, спрямовані на заволодіння майном, коштами або персональними даними шляхом обману та зловживання довірою, завдають значної матеріальної та психологічної шкоди потерпілим, а також негативно впливають на рівень довіри в суспільстві. Ефективна протидія інтернет-шахрайству потребує комплексного підходу, що передбачає підвищення обізнаності громадян, впровадження сучасних технічних засобів захисту та подальше удосконалення законодавчої бази з метою забезпечення належного покарання за вчинення таких злочинів.

Список використаних джерел

1. Кривенко О. І. Сучасні види шахрайства через мережу інтернет. *Сучасні проблеми правового, економічного та соціального розвитку держави*. Харків, 2017. С. 233–235. URL: https://univd.edu.ua/general/publishing/konf/01_12_2017/pdf/73.pdf (дата звернення: 18.03.2025).
2. Чекмарьова І. М. Шахрайство в інтернеті як один із видів шахрайства. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. РОЗДІЛ VIII. Кримінальне право та кримінологія; кримінально-виконавче Право. С. 639–643. URL: surl.lu/razqgy (дата звернення: 10.03.2025).



УДК 004.73:316.472.4]:316.77(043.2)

Баранова Інна Сергіївна

(наук. керівник – канд. наук із соц. комунікації, ст. викл. Василенко В. Ю.)
Донецький національний університет імені Василя Стуса, м. Вінниця

МОЖЛИВОСТІ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ПОБУДОВИ УСПІШНИХ КОМУНІКАЦІЙНИХ СТРАТЕГІЙ

Анотація. У роботі досліджено, як соціальні мережі доповнюють комунікаційні стратегії брендів. Розглянуто функціональні можливості платформ, роль візуального контенту, аналітики та співпраці з інфлюенсерами, а також потенційні ризики, що супроводжують використання соцмереж у комунікаціях.

Ключові слова: соціальні мережі, комунікація, комунікаційні стратегії, взаємодія з аудиторією.

Соціальні мережі стали ключовим інструментом для розробки комунікаційних стратегій завдяки їх зручним і численним функціям та мільйонам активних користувачів. Можливість спілкування в режимі онлайн, візуальне подання інформації через фото та відео, а також збір і аналіз даних про поведінку аудиторії докорінно змінили взаємодію між брендами та їх цільовими групами. Ці переваги дають змогу компаніям краще розуміти потреби клієнтів, оперативно реагувати на зворотний зв'язок та постійно вдосконалювати комунікаційні підходи, що