Корольчук Віктор Володимирович,
провідний науковий співробітник відділу організації наукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник

ПЕРЕДУМОВИ ДОСЛІДЖЕННЯ ЗАПОБІГАННЯ КІБЕРШАХРАЙСТВА В УКРАЇНІ

Починаючи з 2020 року, коли пандемія та локдауни стали глобальною реальністю, Інтернет досяг небаченого попиту. Більшість людей почали проводити значну частину свого часу в онлайн-просторі, що призвело до значного зростання кількості правопорушень у цифровому середовищі. При цьому чимало таких правопорушень залишаються без належного покарання, оскільки системи законодавства не встигають адаптуватися до стрімких змін і появи нових правових інститутів. Цифровізація суспільства стала поштовхом для виникнення нових видів злочинів, пов'язаних із використанням інформаційних технологій.

Комп'ютери, мобільні телефони та шкідливі програми часто стають інструментами для вчинення кіберзлочинів. Одним із таких явищ є цифрове шахрайство, відоме також як кібершахрайство чи інтернет-шахрайство. Його правове регулювання набуває особливої актуальності через те, що цифрове середовище стало невід'ємною частиною повсякденного життя. У цьому просторі ми зберігаємо найважливіші ресурси, включаючи фінансові засоби, банківські картки, конфіденційні дані, особисту переписку та інші приватні речі [5, с. 275].

Пандемія COVID-19 показала, як швидко злочинні організації здатні адаптувати свої методи, знаходячи нові способи шахрайства щодо людей та бізнесу, що призводить до щоденного викрадення мільйонів доларів, зазначив генеральний секретар Інтерполу Юрген Шток [4].

Кібершахрайство залишається найбільш поширеним видом злочину, який здійснюється на міжнародному рівні. Швидкий розвиток цифрових технологій створює сприятливі умови для шахраїв, які знаходять нові способи отримання доступу до особистої та фінансової інформації людей. Вже сьогодні зібрані дані про користувачів можуть використовуватися зловмисниками для незаконного заволодіння грошима.

Світовий ринок виявлення та запобігання шахрайству оцінюють у 25,1 млрд доларів США у 2022 році, і, за оцінками, до 2028 року він перевищить розмір ринку в 118,95 млрд доларів США за середньорічного темпу зростання 24,89% протягом прогнозованого періоду 2022–2028 років [3].

У зв'язку з цим важливо, щоб як окремі громадяни, так і організації були обізнані про способи захисту від подібних загроз. Крім фізичних осіб, значних фінансових втрат зазнають і юридичні особи, що додає масштабів проблемі. На цьому тлі питання законодавчого регулювання відносин у цифровому середовищі набуває особливої актуальності. Необхідно розробити механізми для закріплення відповідальності за злочини, скоєні в цифровому просторі, включаючи кібершахрайство.

У 2002 році Комісія ООН з прав міжнародної торгівлі (ЮНСІТРАЛ) вперше взяла до розгляду питання шахрайських практик, які чинять суттєвий негативний економічний вплив на світову торгівлю і шкодять функціонуванню законних комерційних інститутів. Внаслідок проведених консультацій з експертами і державними службовцями, які регулярно стикаються з випадками комерційного шахрайства та працюють у різних регіонах, представляють різні підходи і галузеві знання, ЮНСІТРАЛ усвідомив широке розповсюдження цих шахрайських практик і їхній суттєвий вплив у світі, незалежно від рівня економічного розвитку держави чи її системи управління [2, с. 118].

У рамках розгляду можливих підходів до реагування на зазначену загрозу було підкреслено, що освіта та професійна підготовка можуть відігравати ключову роль у запобіганні комерційному шахрайству. Особливо важливим аспектом у цьому процесі є ідентифікація загальних ознак і індикаторів, що сигналізують про потенційну наявність шахрайських дій. З цієї метою впродовж наступних років Секретаріат ЮНСІТРАЛ організував серію зустрічей із міжнародними експертами та державними службовцями, які мають відповідний досвід у виявленні та протидії комерційному шахрайству. У результаті цих консультацій було розроблено спеціалізований перелік із двадцяти трьох показників, які дозволяють ідентифікувати комерційне шахрайство. Основна мета вказаного проекту полягала у сприянні ефективному запобіганню шахрайським діям через створення простого у використанні та загальнодоступного документа. Цей документ містить релевантні показники, що допомагають як потенційним жертвам, так і організаціям, до яких вони належать, ідентифікувати поведінкові моделі, які можуть сигналізувати про наявність комерційного шахрайства або бути його складовою. Для забезпечення максимальної ефективності цього інструменту рекомендується органам державного управління, а також іншим установам і організаціям активно поширювати означені матеріали та стимулювати їх застосування в межах заходів із запобігання шахрайству [1, с. 115–116].

Передбачається, що окрім запобігання окремим випадкам комерційного шахрайства шляхом інформування та підвищення обізнаності, даний проєкт протидії шахрайству має три головні

завдання. По-перше, створені матеріали мають на меті виявляти схеми та ознаки комерційного шахрайства, аби впорядковано та послідовно підтримувати приватний сектор у протидії такому шахрайству. По-друге, ці матеріали передбачається допомагати державним інституціям у розумінні того, яким чином можна ефективно підтримати як державний, так і приватний сектори у боротьбі з комерційними шахрайськими діяннями. Нарешті, вони можуть надати кримінально-правовому сектору інструменти для визначення оптимального підходу до залучення приватного сектора в цю боротьбу.

Дослідження різних індикаторів показало, що зазвичай вони виявляються у безлічі потенційних шахрайських схем, незалежно від того, наскільки досвідчений той, хто приймає фінансові рішення, і від рівня економічного розвитку конкретної держави. Для ілюстрації цього явища в даних матеріалах подано випадки та приклади кожного індикатора, зібрані з різних сфер юридичної практики, в яких жертвами виступають представники різних соціальних груп. Метою їх є продемонструвати, що ці індикатори слід застосовувати як у комерційному, так і в адміністративному середовищі; єдина риса, яку безсумнівно мають усі жертви, – це їхня вразливість до шахрайства, що виникає через прийняття ними фінансових рішень [2, с. 122].

Окрім того, слід усвідомлювати, що жоден індикатор сам по собі чи в сукупності з іншими не може беззаперечно підтвердити існування комерційного шахрайства. Навпаки, виявлення будь-якого окремого індикатора вказує лише на можливість шахрайської дії, а поєднання кількох індикаторів підвищує ймовірність її реалізації.

Весь перелік індикаторів оформлений за однією схемою: спочатку подається назва індикатора, далі йде його детальний опис, після чого наведено конкретні випадки та приклади застосування індикатора у сфері комерційного шахрайства в різних контекстах. Далі подаються рекомендації щодо заходів, які можна здійснити для запобігання негативних наслідків, пов'язаних з кожним індикатором, або для протидії їм, залежно від обставин. Нарешті, багато індикаторів можуть і мають частково перекриватися, оскільки їх визначення не є суворо науковим дослідженням; у цьому матеріалі передбачено перехресні посилання на відповідні індикатори, коли це необхідно [1, с. 117].

Банківська та фінансова індустрія продовжує інвестувати мільярди в боротьбу з шахрайством. Однак банківський сектор не може вирішити цю проблему самостійно. Для ефективного розв'язання цієї проблеми в кожному секторі має застосовуватися скоординований підхід. Незважаючи на те, що із закінченням пандемії кількість деяких видів шахрайства скоротилася, інші збільшилися, оскільки злочинці продовжують адаптувати свої методи. Хоча неможливо вказати конкретні значення, які можна віднести до окремих методів атаки, розвіддані, надані нашими членами, виділяють основні рушійні сили. Соціальна інженерія, за допомогою якої злочинці виманюють людей і

маніпулюють ними, щоб вони розголошували особисті або фінансові дані або переказували гроші, як і раніше, була ключовим фактором як несанкціонованих, так і санкціонованих збитків від шахрайства в першій половині 2022 року. Злочинці використовували шахрайські телефонні дзвінки, текстові повідомлення та електронні листи, а також підроблені веб-сайти і повідомлення в соціальних мережах, щоб обманом змусити людей передати особисті дані та паролі [3].

Потім цю інформацію використовують для виявлення жертв і переконання їх здійснити платіж злочинцеві. Шахрайство з інвестиціями залишається високим зі значними пов'язаними з цим втратами. Шахрайство значною мірою пов'язане з шахрайською рекламою в пошукових системах і соціальних мережах. Відомо багато випадків, коли злочинці видавали себе за приватні банки та інвестиційні фірми. Жертвам можуть зателефонувати шахраї, тоді як інші залишили свої дані на сайтах-клонах під час онлайн-пошуку інвестиційних можливостей. Шахраї також дедалі частіше використовують сайти соціальних мереж, щоб спокусити жертв, рекламуючи підроблені інвестиції, як-от схеми з криптовалютою, золото або нерухомість. У деяких випадках для просування таких схем і створення атмосфери легітимності можуть використовуватися «впливові особи» в соціальних мережах.

Збитки від шахрайства також пов'язані з крадіжкою особистих і фінансових даних клієнтів, що часто відбувається через витік даних у третіх осіб і в галузях, які не належать до фінансового сектору. Злочинці також крадуть дані, перехоплюючи пошту або впроваджуючи шкідливе ПЗ на пристрої клієнтів. Ці дані потім використовуються злочинцями для здійснення прямого шахрайства, наприклад, шляхом подачі заявки на отримання кредитної картки на ім'я жертви або купівлі товарів чи послуг в Інтернеті з використанням вкрадених даних. Злочинці також використовують «цифрові скімери» для крадіжки даних карт у клієнтів, коли вони роблять покупки в Інтернеті. У типовій атаці цифрового скімінгу злочинці додають шкідливий код на веб-сайт інтернет-магазину, який краде конфіденційну інформацію, включно з даними картки, на етапі оформлення замовлення. Потім ця інформація відправляється на домен, контрольований злочинцями, і часто перепродається шахраям, які використовують її для здійснення шахрайства з віддаленими покупками. Ці атаки продовжують підкреслювати важливість впровадження і підтримки надійних заходів безпеки в екосистемі онлайн-торгівлі.

Таким чином, шахрайство залишається одним із найпоширеніших злочинів проти власності. Аналіз судово-слідчої практики вказує на серйозні проблеми, пов'язані з видами цього суспільно-небезпечного діяння.

Список бібліографічних посилань

1. Babanina V., Tkachenko I., Matiushenko O., Krutevych M. Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga*. 2021. № 10 (38). P. 113–122.
2. Cherniavskyi S., Babanina V., Mykytchyk O., Mostepaniuk L. Measures to combat cybercrime: analysis of international and Ukrainian experience. *Cuestiones Políticas.* 2021. № 39 (69). P. 115–132.
3. Звіти міжнародних організацій та окремих юрисдикцій. URL: https://mof.gov.ua/storage/files/Методологічний%20бюлетень_%20Серійний%20номер%20Мінфін-AML-2025-08.pdf.
4. Інтернаціональна Правоохоронна Ліга : [сайт] / Генеральний секретар Інтерполу вітає G7 у справі транснаціональної організованої злочинності. URL: https://www.ilel-interpol.org/%D0%B3%D1%80%D1%83%D0%BC%D1%96%D0%BD%D0%B3-%D1%80%D0%B0%D0%B4%D0%B8%D0%BA%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F%D1%82%D0%B0-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8-4/.
5. Юріков О. О. Відповідальність за створення, керівництво електронно-комунікаційною шахрайською організацією, а також участь у ній: аналіз проєкту закону (№ 10190 від 25.10.2023). *Актуальні проблеми кримінального права :* матеріали XV Всеукр. наук.-теорет. конф. (Київ, 28 листоп. 2024 р.). Київ, 2024. С. 274–278.

Кошевський Віталій Станіславович,
викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ЗА СЕКСУАЛЬНЕ НАСИЛЬСТВО, ПОВ'ЯЗАНОГО З КОНФЛІКТОМ

Війна – це не лише протистояння армій та бойові дії, але й хаос, який відкриває двері для найжахливіших злочинів. Одним із найтяжчих є сексуальне насильство, яке в умовах збройного конфлікту виходить далеко за межі індивідуальних актів жорстокості та використовується як зброя для залякування, приниження та руйнування. Зґвалтування, сексуальне рабство, примусова стерилізація, каліцтво статевих органів – це лише деякі з жахливих форм, які воно може набувати. Головними мішенями стають не лише жінки та дівчата, а й чоловіки та хлопчики, які можуть зазнавати сексуального насильства. Тілесні та психологічні рани, завдані цими злочинами, залишаються на все життя, руйнуючи долі людей.