Таким чином, до процесуального оформлення виявлена на електронному пристрої інформація, що становить інтерес для органів досудового розслідування, може розглядатись лише як невід'ємна частина цього електронного пристрою, який, з огляду на вміст інформації, що в ньому зберігається, де-факто матиме статус речового доказу.

Після складення протоколу за результатами огляду переписки в месенджері установленого на електронному пристрої із дотриманням процедури визначеної КПК України (ухвала слідчого судді, обшук, добровільна згода, особистий обшук при затримані особи на підставі ст. 208 КПК України, інше) чи відповідного протоколу, у разі проведення НС(Р)Д, чи отримання висновку експерта останні може використовуватись в суді, як окремий документ для встановлення необхідних обставин вчинення кримінального правопорушення, а не як речовий доказ.

***Список використаних джерел***

1. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових джерел/ практичний посібник – 2020 р.: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

2. Кримінальний процесуальний кодекс України, URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

***Демедюк Сергій Васильович***
кандидат юридичних наук, заступник Секретаря Ради національної безпеки і оборони України

## ОСОБЛИВОСТІ ОНЛАЙН ШАХРАЙСТВА В УКРАЇНІ

On-line шахрайство є найбільш поширеним видом кіберзлочину. У загальній сукупності злочинів, протидія яким є пріоритетом в діяльності кіберполіції, більше третини складають кримінальні правопорушення, пов'язані із шахрайством, при вчиненні яких використовуються сучасні інформаційні та телекомунікаційні технології. Водночас, 84% шахрайств вчиняються саме у формі діяльності передбаченої частинами 3 та 4 ст. 190 ККУ, що ще раз підкреслює надзвичайну поширеність on-line шахрайства в Україні.

За методологією Європол IOCTA, із врахуванням значної різноманітності способів та засобів, що використовуються при

здійсненні платежів, розрізняється два види шахрайства з платежами: з використанням картки та без такої.

За сучасного стану найбільшим поширенням характеризуються загрози шахрайства з платежами, пов'язані з (*табл.1*): роздрібною торгівлею фізичними (51,4 %) та віртуальними товарами (40,6 %); конвертацією валют (криптовалют та електронних грошей) (46,6 %); а також позикою (46,6 %).

Експертами зазначається про певне загальне зниження масштабів поширення цієї групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення, хоча окремі з них характеризуються меншим трендом до зниження масштабів, зокрема, пов'язані з: позикою, роздрібною торгівлею фізичними товарами, конвертацією валют (криптовалют та електронних грошей) та використанням паливних карток.

*Таблиця 1*

**Загрози шахрайства з платежами без використання банківської картки**

| ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ БЕЗ ВИКОРИСТАННЯ БАНКІВСЬКОЇ КАРТКИ | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| 2.1. пов'язане з транспортом – авіаквитки | | 23,3 | | | | 33,91 |
| 2.2.пов'язане з транспортом – квитки на поїзд або автобус | | 30 | | | | 34,00 |
| 2.3.пов'язане з транспортом - оренда автомобілів | | 22,6 | | | | 31,83 |
| 2.4.пов'язане з позикою (послугою, орендою приміщення тощо) | | 46,6 | | | | 37,43 |
| 2.5.пов'язане з веб-сайтами азартних ігор | | 37,1 | | | | 33,67 |
| 2.6.пов'язане з роздрібною торгівлею – фізичні товари | | 51,4 | | | | 39,52 |
| 2.7.пов'язане з роздр торг– віртуальні товари | | 40,6 | | | | 36,66 |
| 2.8.пов'язане з конвертацією валют(криптовалют та електр грошей) | | 46,6 | | | | 38,95 |
| 2.9. з використанням паливних карток | | 37,4 | | | | 34,62 |
| 2.10.з використанням карток у роздрібній торгівлі продуктам | | 28,3 | | | | 32,53 |
| 2.11. з використанням клубних карток | | 16,3 | | | | 28,33 |
| 2.12.з використанням подарункових карток | | 18,3 | | | | 28,60 |
| 2.13.з використанням ігрових карток | | 19,7 | | | | 29,01 |
| 2.14. на ринку мобільного зв'язку | | 30,6 | | | | 32,23 |
| 2.15.в сфері комп'ютерних ігор (внутрішньоігрові перекази) | | 29,7 | | | | 30,02 |
| 2.16.пов'язане з букмекерськими послугами | | 28,3 | | | | 31,29 |
| 2.17.пов'язане з «move to» | | 21,1 | | | | 29,89 |

Зазначені види загроз шахрайства з платежами, без використання банківської картки, характеризуються і найвищим ризиком поширення у післявоєнний період, зокрема, пов'язані з: роздрібною торгівлею фізичними товарами (39,52 %), конвертацією валют (криптовалют та електронних грошей)

(38,95 %), позикою (37,43 %) та роздрібною торгівлею віртуальними товарами (36,66 %).

Водночас, було ідентифіковано 13 загроз, у якості різновиду поширення шахрайства з платежами, з використанням банківської картки (*табл. 2*).

*Таблиця 2*

**Загрози шахрайства з платежами з використанням банківської картки**

| ВИДИ ЗАГРОЗИ ШАХРАЙСТВА З ПЛАТЕЖАМИ З ВИКОРИСТАННЯМ БАНКІВСЬКОЇ КАРТКИ | Оцінка сучасного поширення | % | Масштаби збільшились | Масштаби не змінилися | Масштаби зменшились | Ризик після війни, % |
|---|---|---|---|---|---|---|
| 3.1. Зняття готівки з банківських карт UA за межами UA | | 46,00 | | | | 40,45 |
| 3.2.Зняття готівки з банківських карт UA в межах UA | | 63,70 | | | | 42,23 |
| 3.3.Зняття готівки з іноземних банківських карток у межах UA | | 38,60 | | | | 37,40 |
| 3.4.PoS-покупки з використанням скомпрометованої платіж карти | | 45,10 | | | | 38,35 |
| 3.5.Шахрайство з платіжними картками: трешінг | | 30,90 | | | | 33,40 |
| 3.6.Шахрайство з платіжними картками: фармінг | | 32,00 | | | | 34,23 |
| 3.7.Шахрайство з платіжними картками: фішинг | | 52,30 | | | | 42,80 |
| 3.8.Шахрайство з банкоматом: скіминг | | 37,40 | | | | 35,67 |
| 3.9.Шахрайство з банкоматом: траппінг | | 29,10 | | | | 33,04 |
| 3.10.Шахрайство з банкоматом: фантом | | 27,40 | | | | 32,36 |
| 3.11.Шахрайство з банкоматом: jackpotting | | 26,90 | | | | 32,17 |
| 3.12.Шахрайство з телефоном та інтернетом: вішинг | | 44,90 | | | | 38,26 |
| 3.13.Шахрайство з телефоном та інтернетом: смішинг | | 38,60 | | | | 36,06 |

За сучасного стану, враховуючи і перші роки повномасштабного вторгнення, найбільшим поширенням серед таких загроз характеризуються: зняття готівки з банківських карт UA в межах UA (63,70 %); шахрайство з платіжними картками (фішинг) (52,3 %); зняття готівки з банківських карт UA за межами UA (46,0 %); PoS-покупки з використанням скомпрометованої платіжної карти (45,1 %), а також шахрайство з телефоном та інтернетом (вішинг) (44,9 %).

Водночас, важливо зазначити про незмінність масштабів поширення зазначеної групи загроз за останні роки, враховуючи і перші роки повномасштабного вторгнення. Водночас, окремі загрози, характеризувалися певним трендом підвищення масштабів поширення: шахрайство з платіжними картками (фішинг); зняття готівки з банківських карт UA в межах UA; зняття готівки з банківських карт UA за межами UA.

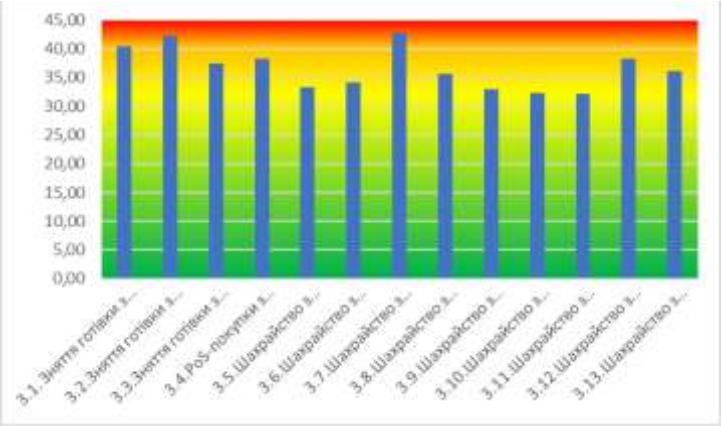


**Рис.** Оцінка ризиків поширення загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період

Оцінюючи ризики поширення групи загроз шахрайства з платежами, з використанням банківської картки, у післявоєнний період, такий же різновид шахрайства характеризуються найвищим ризиком (*рис.*): шахрайство з платіжними картками (фішинг) (42,8 %); зняття готівки з банківських карт UA в межах UA (42,23 %); та зняття готівки з банківських карт UA за межами UA (40,45 %).

Таким чином, шахрайство з платежами є найбільш поширеною загрозою у сфері кіберзлочинності, складаючи 67,10 % усіх випадків on-line шахрайства. Воно характеризується високим рівнем ризику і залишається важливою проблемою як до, так і після війни.

***Денисенко Богдан Анатолійович,***
експерт з питань організованої злочинності (Консультативна місія Європейського Союзу)

## ІТ ІНФРАСТРУКТУРА ДЛЯ ВПРОВАДЖЕННЯ ILP

Процес реформування сектору цивільної безпеки є складним та багатогранним. Для досягнення бажаного результату, в процесі реформування необхідно орієнтуватись на