УДК 159.9.072 : 004.056.53
DOI: 10.33099/2617-6858–21–60–2–143-149

Теслик Н. М. *кандидат психологічних наук,*
Сумський державний університет,
https://orcid.org/0000-0002-1564-8323;
Гончаренко А. Р. *Сумський державний університет*
Громико Д. В. *Сумський державний університет*

ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ СПРИЙНЯТТЯ КІБЕРШАХРАЙСТВА СТУДЕНТСЬКОЮ МОЛОДДЮ

Віртуалізація міжперсональної взаємодії провокує перехід незаконних способів впливу на людину у кіберпростір. Кібершахрайство є ознакою сучасного соціального життя людини у віртуальному просторі, особливо загрожуючи молоді як однієї із найбільш віртуально активних когорт суспільства. Раціональність сприйняття кібершахрайства визначає ступінь кібербезпеки користувачів кіберпростору.

Ключові слова: *кібершахрайство; психологічні особливості сприйняття; кіберпростір; кібербезпека; студентська молодь.*

Вступ. Соціальна активність людини регулюється різноманітними соціальними нормами, зокрема, правовими. Порушення встановлених законом обмежень визначає ризики для прав інших людей чи систем. Одним із найпоширеніших злочинів можна вважати шахрайство, в результаті якого виникають передумови втратити особисті ресурси. З психологічної точки зору, специфіка шахрайства полягає в переважанні методів активного психологічного впливу на жертву.

Розвиток віртуальних технологій другої половини XX – початку XXI століття, окрім можливостей самореалізації індивіда у кіберпросторі в цілому, спровокував певні види девіантної та делінквентної поведінки. Можна впевнено говорити про відтворення більшості відомих видів правопорушень у віртуальному просторі. Наприклад, порівняння кібершахрайства із аналогічними видами злочинів у реальному просторі свідчить про відтворення базових структурних елементів злочинного діяння. У 2017 році в Україні відбулася масштабна атака вірусом Petya: були вражені енергетичні компанії, українські банки, аеропорти в Києві та Харкові, Чорнобильська АЕС, урядові сайти, київський метрополітен і т. д. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya склали близько 850 млн. доларів [1].

Віртуалізація даного виду злочинної діяльності неминуче впливає на формування специфічних проявів кібершахрайство порівняно із шахрайською діяльністю. Загальновизнані наукові досягнення у визначенні психологічних особливостей шахрайської діяльності Ю.М. Антоняна, Б.С. Волкова, П.С. Дагеля, О.А. Герцензона, О.В. Рудзитіса, О.О. Данилова, Є.Л. Доценко, О.В. Кравченко та багатьох інших дослідників. Однак актуальним питанням слід визнати аналіз різноманітних проявів кібершахрайства як своєрідного виду злочину. Метою даного дослідження є проаналізувати психологічні особливості шахрайства у кіберпросторі.

Теоретичне підґрунтя. Особливими характеристиками соціального віртуального простору є те, що у більшій мірі зберігається анонімність при взаємодії та у меншій ця взаємодія може бути контрольована правоохоронною системою. Особливо у період обмежень соціальної взаємодії, детермінованих пандемією. З часу запровадження карантинних обмежень в Україні зафіксовано понад 700 звернень щодо випадків кібер-шахрайства виключно з тематики протидії поширенню захворюваності на COVID-19, йдеться про маніпуляції щодо товарів індивідуального захисту, фейкову інформацію, СМС-розсилки та дзвінки, пов’язані із шахрайськими повідомленнями [3].

Для здійснення шахрайства, злочинець використовує психологічні засоби впливу на психіку жертви. Як зазначив Г. О. Ковальов, вплив – це цілеспрямований процес, в якому беруть участь дві або більше упорядкованих систем, в результаті якого спостерігаються

будь-які зміни хоча б однієї з цих сторін. Психологічний вплив має певні ознаки, визначені Сергієм та Світланою Ніколаєнками як усвідомлення здійснення впливу, котрий передбачає певний результат; вплив на мислення, почуття, думки із застосуванням психологічних методів; цілеспрямованість; вольові зусилля людиною, яка виконує вплив; інформаційність впливу [6].

А. С. Булатов зауважує, що методи активного впливу на психічну активність мають зміст, котрий вигідний саме для маніпулятора. Суть здійснення маніпуляції полягає в тому, щоб створити певний дисбаланс у жертви і викликати внутрішній дискомфорт. Окрім того, щоб жертва не встигла знайти способи вирішення поданої ситуації, маніпулятор попередньо надає ці способи вирішення, зазвичай надаючи вибір, котрий можна назвати «вибір без вибору», тобто створюється ілюзія кращого вибору для обох сторін, хоча насправді кожен із наданих варіантів вигідні лише для самого шахрая. Сутність маніпуляції може бути не лише дискомфортною для жертви, а й навіть нестерпною, що не надає їй можливості включитися в раціональне мислення. Існують певні мішені, на котрі спрямований активний вплив. За класифікацією О. В. Кравченко до цілей впливу шахраїв в першу чергу відносять:

1. Когнітивні структури (інформаційне забезпечення діяльності людини).
2. Психічні стани (емоційні, фонові, функціональні).
3. Спонукачі діяльності людини (потреби, схильності, інтереси).
4. Регулятори діяльності людини (норми, правила, самооцінка, самоповага, гордість тощо).
5. Операційний склад активності (стиль мовлення, поведінки, звички, навички, спосіб мислення тощо) [4].

Інформаційні технології частково змінили світосприйняття людини, спричинивши формування нового віртуального простору та суспільства. За законодавством України, кіберпростір є певним середовищем, що надає можливості для комунікації в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням інтернету або інших мереж [8]. Дослідниця М. В. Палчинська визначає кіберпростір як особливу соціальну сферу, включену до системи існуючих соціальних відносин, не тільки як аналог, а і конкурент стосовно просторово-часових змін [7]. Типово кіберпростір порівнюють з міфологічним, так як він займає проміжну позицію між чуттєвим простором сприйняття і середовищем чистого пізнання. Як частина віртуального простору, кіберпростір є певним середовищем, що підтримується за допомогою сумісних комунікаційних систем, доступ до якого може бути отриманий за допомогою інтернету чи аналогічних мереж.

За своєю сутністю віртуальний простір є інформаційним середовищем, тобто має високу залежність від інформаційних впливів. Характер подачі інформації може змінювати її сприйняття, так М. Маклюен відзначає, що засіб передачі повідомлення можна розглядати як окремий тип повідомлення [2]. Однак для розуміння цього необхідне застосування конкретних меж сприйняття та аналізу. Важливо зазначити, що реальний, фізичний простір у цілому, має більш виражені рамки соціального регулювання. Віртуальний простір менше регламентується законом у зв'язку з новизною та невизначеністю конкретних рамок дозволенного, а також більшою складністю у ідентифікації злочинця, що спричинює виникнення багатьох межових феноменів, що провокує розвиток кібершахрайства [9]. У сучасному віртуальному просторі безліч феноменів, що можуть бути класифіковані як злочин, але при цьому залишаються діючими та достатньо популярними, наприклад «1XBET» або «треш-стріми». Порушення авторських прав, так зване «піратство», взагалі інтегроване в масову свідомість мешканців багатьох країн, у тому числі України.

Конвенція Ради Європи визначає сутнісні види кіберзлочинності: незаконний доступ; незаконне перехоплення; втручання у дані та у систему; зловживання пристроями; шахрайство, пов'язане із комп'ютерами, зокрема, підробка; правопорушення, пов'язані зі змістом, наприклад, з дитячою порнографією;

правопорушення, пов'язані з порушенням авторських та суміжних прав тощо.

Найпоширенішими видами кібершахрайства вважаються:

1. Кардинг – використання в операціях реквізитів платіжних карт.
2. Фішинг –спосіб незаконного заволодіння даними доступу до платіжних карт.
3. Вішинг – виманювання конфіденційних даних про платіжні картки телефонним шляхом.
4. Онлайн-шахрайство – імітація інтернет-аукціонів, інтернет-магазинів та інших віртуальних засобів.
5. Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті.
6. Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення.
7. Соціальна інженерія – технологія управління людьми в кіберпросторі.
8. Мальваре – створення та розповсюдження шкідливого програмного забезпечення.
9. Протиправний контент – з метою пропаганди екстремізму, тероризму, наркоманії, порнографію, культу жорстокості і насильства.
10. Рефайлінг – незаконна підміна телефонного трафіку [10].

Шахрайство у віртуальному просторі має схожі риси з звичайним, але має більш масовий і відповідно до характеристики самого простору «стихійний» характер. Л.М. Прудка на основі аналізу праць У. Альбрехта, Дж. Венца та Т. Уільяма, відзначає, що шахраї, зокрема і ті, які орудують у кіберпросторі, не мають сутнісно відмінних психологічних особливостей від законослухняних громадян. Тобто, схильність до кібершахрайства не може бути визначена превентивним обстеженням. Хоча окремі дані щодо злочинця можуть бути отримані завдяки профайлінгу, наприклад, психологічний портрет шахрая представлений в основному авантюрним складом особистості.

Мотивами кіберзлочину можуть виступати, у першу чергу, корисливі, але їх також можуть доповнювати мотиви самоствердження, прагнення до влади, ігровий мотив. Залежно від домінування певного мотиву, кібершахраї виявляють типові моделі поведінки, демонструють раціональний підхід до здійснення шахрайства, що виражається у активному підготовчому етапі вчинення злочинного діяння та усвідомленні його наслідків або отримують задоволення від процесу злочинної діяльності [9].

Угорські дослідники Н. Арато, А.Н. Зідо, К. Ленард та Б. Лабаді визначають, що більшість агресорів у кіберпросторі лишаються анонімними. Кіберпростір забезпечує більш широку аудиторію для шахрайства. Кібершахраї схильні вчиняти злочини щодо осіб, що мають проблеми з регулюванням своїх емоцій, підвищений рівень агресивності, депресивність, підвищену схильність до стресу [11].

О.П. Дзьобань розрізняє два типи сприйняття інформації людиною у віртуальному просторі. У першому варіанті увага людини концентрується на чомусь логічному, всезагальному, абстрагованому. У другому варіанті йдеться про певне занурення у так зване «міфологічне» сприйняття, що зосереджене на чомусь конкретному, неповторному, емоційно-образному. Таким чином, другий тип у більшості випадків створює віртуальну реальність, тобто індивід віртуалізується. Віртуальна реальність характеризується більшою суб'єктністю, нелінійністю, зміщенням просторових та часових меж, зануреністю з боку віртуалізованої особистості, вона стає «співучасником» цього світу. Але цей вимір неоднорідний, він має безліч можливих варіацій, залежних від контексту, тому кожна із них, будучи відомою людині, може провокувати різні поведінкові або емоційні реакції.

Віртуальна реальність проявляє і більш загальний, соціальний вплив. У ній стираються державні кордони, з'являються нові цінності, моделі поведінки, стереотипи. Віртуальній реальності, згідно О.П. Дзьобаню, також характерне зміщення реальності, що може нести як позитивний у соціальному аспекті зміст – розширення життєвого досвіду, смислу, так і негативний – необмежена та неконтрольована, деструктивна творчість [2]. Попри те, що користування віртуальним і зокрема кіберпростором не означає неминучої

віртуалізації індивіда, певною мірою можливості занурення зростають. Принаймні, у разі використання специфічного розважального, ігрового контенту. Враховуючи змінений стан волі та свідомості у віртуальній реальності, можливості активного впливу на людину, значно зростають. Водночас пересічне послугування віртуальним простором, відмежоване від віртуальної реальності, не створює очевидних передумов до послаблення захисних можливостей психіки.

Методи дослідження. Для визначення ризиків активних методів впливу на особистість у віртуальному просторі з боку кібершахраїв проведене емпіричне дослідження 84 осіб у віці від 18 до 24 років. До вибірки увійшли студенти закладу вищої освіти технічних та соціогуманітарних спеціальностей. Вікові межі вибірки визначило переконання, що молодь є однією із найбільш активних когорт серед користувачів кіберпростору, що детермінує ризики її віктимізації з боку кібершахраїв.

Метою збору практичних даних було визначення рівня активності і поінформованості молоді про феномен та особливості кібершахрайства, пов'язані з цим необхідні заходи кібербезпеки, а також вплив особистісних властивостей користувачів на сприйняття кібершахрайства. У дослідженні використано самостійно розроблений опитувальник та психогеометричний тест С. Делінгер, за яким визначають головні риси характеру та особливості поведінки [5]. Для аналітичного опрацювання даних використані r-критерій Пірсона та φ-критерій Фішера.

Результати і обговорення. Проведене дослідження підтвердило високу актуальність тематики, адже 78 осіб, тобто 93% опитаних обізнані із темою кібершахрайства, хоча лише 6 опитуваних (7% вибірки) змогли вірно визначити перелік шляхів незаконного маніпулювання кібершахраїв. Єдине уявлення, можна вважати стійким, - щодо небезпеки переходу за сумнівними посиланнями.

Серед досліджуваних не виявилося жодного студента, чиє користування кіберпростором не було б щоденним. Натомість 71 чол. (84%) вказали, що приділяють кіберпростору щоденно від 3 до 10 годин і більше. Цілком імовірно, що на отримані результати могли вплинути карантинні обмеження та дистанційне навчання, однак це лише посилює актуальність проблеми. Домінуючими мотивами користування кіберпростором для студентської молоді виявилися соціальні, навчальні чи професійні та розважальні (перегляд відео контенту тощо). Цікаво, що тривалість користування мережею пов'язана із частотою зміни паролів (табл. 1). Однак причиною є не набуття навичок безпечного користування кібепростором, а зовнішні фактори: забування старих паролів (цей варіант як причину вказали 35 осіб, 42 % опитаних); зафіксовані ознаки зовнішнього втручення (11 осіб, тобто 13%); особливості конкретних сайтів (9 осіб, 11%). При цьому четверта частина досліджуваних (20 ос.) довіряє таку інформацію, як паролі, сім'ї чи друзям. І навіть 2 відповівді (2% респондентів) зафіксовані відповіді щодо готовності поширити таку інформацію представникам організації, з якою пов'язаний даний сайт.

Можна визначити існування загального уявлення про небезпеку кібершахрайства, зокрема, 77 студентів (92% вибірки) висловили установку щодо відмови від користування підозрілими ресурсами, якщо вони пов'язаними із ризиками щодо персональних даних чи фінансів. У той же час ці уявлення варто визначити недостатньо чіткими, адже 12 опитаних (14%) готові публікувати у мережі будь-які персональні дані або не задумуються про безпеку цих даних. Більшість опитаних (59 осіб, 70%) не має уявлення про ризики використання програмного забезпечення із джерел, подібних Play Маркет чи App Store. І дуже незначна частка опитаних (по 9 осіб, це 11%) свідомо відмовляються від користування «піратськими» сайтами чи принаймні намагаються їх уникати. Третина респондентів (31 студент, це 37%) не мають інформації щодо фінансових пірамід.

Таблиця 1.

Взаємозв'язки проявів сприйняття кібершахрайства та особистісних рис молоді

	1	2	3	4	5	6	7	8	9	10
1. Фігура	1									
2. Час у кіберпросторі	-	1								
3. Частота і причини зміни паролів у кіберпросторі	-	,28**	1							
4. Оцінка ризиків у кіберпродажах	-	-	-	1						
5. Готовність відмовитися від кіберресурсів	-	-	-	-	1					
6. Користування «піратським» контентом	-	-	-	-	-	1				
7. Уявлення про шляхи кібершахрайства	-	-	-	-	-	-	1			
8. Досвід віктимізації від кібершахрайства	-	-,284**	-	-	-	-	-	1		
9. Стать	-	-	-,284**	-	-	-	-	-	1	
10. Напрям підготовки	-,22*	-	,22*	-	-	-	-	-	,53**	1

Примітки: * p≥0,05; ** p≥0,01

Підкріплює висновок щодо необхідності інтенсивного впливу на здатність безпеченого користування віртуальним простором дані щодо частоти особистого досвіду віктимізації від кібершахраїв. 37% (31 чол.) знають про випадки кібершахрайства серед свого кола знайомих, а 12% опитаних (10 осіб) визнали себе жертвами кібершахраїв. Цікаво, що у блоці питань фінансової безпеки у кіберпросторі жертвами кібершахраїв у ситуації купівлі-продажу визнали себе дещо більше опитаних – 11 осіб, 13%.

Більшість студентів (60 осіб, 71%) користуються віртуальним простором для здійснення фінансових операцій. При цьому лише 7 осіб (8%) відчувають себе у безпеці щодо кібершахрайства.

Не виявлено відмінностей в рівні критичності оцінки рекламних продуктів у віртуальному просторі залежно від досвіду використання віртуальних продуктів, поширені рекламними засобами ($\varphi_{емп.}$= 0.82).

За методикою Деллінгера визначено домінування психотипу «коло», пов'язаного із комунікативною спрямованістю особистості, серед студентів соціогуманітарних спеціальностей ($\varphi_{емп.}$=1,69, p≥0,05), а серед студентів технічних спеціальностей – психотипу «трикутник», який пов'язують із лідерськими схильностями ($\varphi_{емп.}$=2,32, p≥0,01). Зазначимо, що цей результат слід у першу чергу пов'язувати із нерівномірним розподілом досліджуваних за статтю. Важливо, що результати дослідження свідчать про відсутність взаємозв'язків суб'єктивних проявів сприйняття кібершахрайства та так званою «суб'єктивною фігурою» С. Делінгера (табл. 1).

Висновки. Кібершахрайство, як злочин, що реалізується у віртуальному просторі, маю специфічні прояви відносно аналогічного типу злочинів у реальному житті. Віртуальна взаємодія відзначається особливими ризиками деперсоніфікації користувачів, меншим ступенем регламентації та соціального контролю. Поширеність віртуальної взаємодії та її проникнення у різноманітні сфери соціального життя людини обумовлює зростання частоти, різноманіття та масштабів кібершахрайства.

Для студентської молоді проблема кібершахрайства є актуальною. Досвід користування кіберпростором, життєвий досвід переживання кібершахрайства, загальні особистісні схильності індивіда не можуть вважатися надійними превентивними чинникам, які гарантовано попереджають злочин. Існує потреба віктимологічного дослідження віртуальної взаємодії молоді з метою виявлення ефективних шляхів зниження ризиків кібершахрайства.

Список використаних джерел

1. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. Юрист&Закон. 2020. №12. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення 07.04.2021).

2. Дзюбань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфи. Стратегічні пріоритети, 2017. №3. С. 163-170. URL: https://dspace.nlu.edu.ua/bitstream/123456789/14077/3/St_Dzeban.pdf (дата звернення 07.04.2021).

3. Кіберполіція розповідає про типові випадки шахрайства під час коронавірусу. Офіційний сайт Департаменту кіберполіції Національної поліції України. 25 березня 2020 р. URL: https://cyberpolice.gov.ua/article/kiberpolicziya--rozpovidaye-pro-typovi-vypadky-shaxrajstva-pid-chas-koronavirusu-1820/ (дата звернення 09.04.2021).

4. Кравченко О. В. Психологічні особливості шахрайства: автореф. дис… канд. психол. наук : спец. 19.00.06 НУВС, 2005. 23 с. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/VKhnuvs_2004_28_90.pdf (дата звернення 07.04.2021).

5. Мацко Л. А. Основи психології та педагогіки. Психологія : лабораторний практикум / Л. А. Мацко, М. Д. Прищак, Т. В. Первушина. Вінниця : ВНТУ, 2011. 139 с.

6. Ніколаєнко С., Ніколаєнко С. Категорія психологічного впливу в психології. Світогляд-Філософія-Релігія, 2011. №1 (1). С. 51-61. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39499/09-Nikolaienko2.pdf?sequence=1 (дата звернення 07.04.2021).

7. Палчинська М. В. Віртуальний простір в умовах соціокультурних трансформацій : автореф. дис. … докт. філол. наук : 09.00.03. Одеса, 2016. 43 с. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/715/1/ПальчинськаМар'янаВікторівна.aref.pdf (дата звернення 07.04.2021).

8. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року. № 45. ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 07.04.2021).

9. Прудка Л.М. Психологічні особливості шахрайства в мережі інтернет. Південноукраїнський правничий часопис, 2018. №2. С. 30-33. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/1382/1/Прудка_2_2018.pdf (дата звернення 07.04.2021).

10. Пфо О. М. Основні поняття і класифікація кіберзлочинності. Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. / Кіровоград. нац. техн. ун-т, Черкас. держ. технолог. ун-т та ін. ; [відп. За вип. : О. П. Доренський]. Кропивницький : КНТУ, 2016. С. 33-34. URL: https://core.ac.uk/download/pdf/84825482.pdf (дата звернення 07.04.2021).

11. Arató N., Zsidó A.N., Lénárd K. and Lábadi B. (2020) Cybervictimization and Cyberbullying: The Role of Socio-Emotional Skills. Front. Psychiatry 11:248. DOI: 10.3389/fpsyt.2020.00248 (дата звернення 07.04.2021).

References

1. Hazizova Yu. (2020). Kiberzlochynnist v Ukraini. Era tsyfrovykh tekhnolohii – era novykh zlochyniv [Cybercrime in Ukraine. The digital age is an era of new crimes]. Yuryst&Zakon. №12. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (in Ukrainian).

2. Dziuban O. P. (2017). Suchasnyi virtualnyi prostir: konhenialnist virtualnosti y mifu [The contemporary virtual space: the congeniality of virtuality and myth.]. Stratehichni priorytety №3. P. 163-170. URL: https://dspace.nlu.edu.ua/bitstream/123456789/14077/3/St_Dzeban.pdf (in Ukrainian).

3. Kiberpolitsiia rozpovidaie pro typovi vypadky shakhraistva pid chas koronavirusu [The Cyberpolice describes the types of incidents of mishandling during the coronavirus] (2020). Ofitsiinyi sait Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy. 25 March 2020. URL: https://cyberpolice.gov.ua/article/kiberpolicziya--rozpovidaye-pro-typovi-vypadky-shaxrajstva-pid-chas-koronavirusu-1820/ (in Ukrainian).

4. Kravchenko O. V. (2005). Psykholohichni osoblyvosti shakhraistva [Psychological features of fraud]: avtoref. dys… kand. psykhol. nauk : spets. 19.00.06. Kharkiv. 23 p. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/VKhnuvs_2004_28_90.pdf. (in Ukrainian).

5. Matsko L. A. (2011). Osnovy psykholohii ta pedahohiky [Basics of psychology and pedagogy]. Psykholohiia : laboratornyi praktykum / L. A. Matsko, M. D. Pryshchak, T. V. Pervushyna. Vinnytsia : VNTU. 139 p. (in Ukrainian).

6. Nikolaienko S., Nikolaienko S. (2011). Katehoriia psykholohichnoho vplyvu v psykholohii [The category of psychological influence in psychology]. Svitohliad-Filosofiia-Relihiia №1 (1). P. 51-61. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39499/09-Nikolaienko2.pdf?sequence=1 (in Ukrainian).

7. Palchynska M. V. (2016). Virtualnyi prostir v umovakh sotsiokulturnykh transformatsii [Virtual space in the context of socio-cultural transformations] : avtoref. dys. … dokt. filol. nauk : 09.00.03. Odesa, Pivdennoukrainskyi natsionalnyi pedahohichnyi universytet imeni K. D. Ushynskoho 43 p. URL: http://dspace.pdpu.edu.ua/bitstream/ 123456789/715/1/PalchynskaMarianaViktorivna.aref.pdf. (in Ukrainian).

8. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy (aw On Basic Principles of Cyber Security of Ukraine) Zakon Ukrainy vid 5 zhovtnia 2017 № 2163-VIII. № 45. p. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

9. Prudka L.M. (2018). Psykholohichni osoblyvosti shakhraistva v merezhi internet [Psychological characteristics of fraud on the Internet]. Pivdennoukrainskyi pravnychyi chasopys. №2. P. 30-33. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/1382/1/Прудка_2_2018.pdf. [in Ukrainian].

10.Pfo O. M. (2016). Osnovni poniattia i klasyfikatsiia kiberzlochynnosti [Basic concepts and classification of cybercrime]. Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky : materialy Vseukr. nauk.-prakt. konf., m. Kropyvnytskyi, 23–25.11.2016 / Kirovohrad. nats. tekhn. un-t, Cherkas. derzh. tekhnoloh. un-t ta in. ; [vidp. Za vyp. : O. P. Dorenskyi]. Kropyvnytskyi : KNTU, 2016. P. 33-34. URL: https://core.ac.uk/download/pdf/84825482.pdf. (in Ukrainian).

11.Arató N., Zsidó A.N., Lénárd K. and Lábadi B. (2020) Cybervictimization and Cyberbullying: The Role of Socio-Emotional Skills. Front. Psychiatry 11:248. DOI: 10.3389/fpsyt.2020.00248 (in English).

Роботу виконано в межах науково-дослідної теми «Data-Mining для протидії кібершахрайствам та легалізації кримінальних доходів в умовах цифровізації фінансового сектору економіки України» (номер державної реєстрації 0121U100467).

Резюме

Теслик Н. Н. *кандидат психологичекских наук,*
Сумский государственный университет,
Гончаренко А. Р. *Сумской государственный университет*
Громыко Д. В. *Сумской государственный университет*

ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ВОСПРИЯТИЯ КИБЕРМОШЕННИЧЕСТВА СТУДЕНЧЕСКОЙ МОЛОДЕЖЬЮ

Виртуализация межперсонального взаимодействия обуславливает переход незаконных способов влияния на человека в киберпространство. Кибермошенничество является признаком современной социальной жизни человека в виртуальном пространстве, особенно угрожая молодёжи как одной из наиболее виртуально активных верств общества. Рациональность восприятия кибермошенничества определяет ступень кибербезопасности пользователей киберпространства.

Ключевые слова: *кибермошенничество; психологические особенности восприятия; киберпространство; кибербезопасность; студенческая молодежь.*

Summary

Teslyk N. *candidate of psychological sciences,*
Sumy State University
Honcharenko A. *Sumy State University*
Hromyko D. *Sumy State University*

PSYCHOLOGICAL CHARACTERISTICS OF STUDENTS' PERCEPTIONS OF CYBERFRAUD

Introduction. *Cyberfraud is a sign of modern human social life in virtual space which threats young people who are one of the most virtually active segment of the population. The rationality of cyberfraud perception determines the level of cybersecurity of cyberspace users. It is especially important to study cyberfraud in the context of the limitations of social interaction in real life due to COVID-19. For example, since the introduction of quarantine conditions, there has been an increase in the level of cybercrime in Ukraine.*

Purpose. *The purpose of our research is to determine the level of activity and awareness of young people about the phenomenon and characteristics of cyberfraud, the related necessary measures of cyber security, as well as the influence of personal characteristics of users on the perception of cyberfraud.*

Methods. *We created a youth activity in virtual space questionnaire and awareness of cyberfraud questionnaire for this study. In addition, we used S. Delinger's psychometric test to determine the main character traits and behavioral traits of students.*

Originality. *Our research involves both a theoretical study of the characteristics and importance of cyberfraud, as well as an empirical study. It is worth pointing out that the importance of studying cyberfraud lies in the fact that these actions are much more difficult to control and do not have a strong legislative basis, so there are more opportunities for fraud than in real life. Also, it should be noted that not all young people tend to be more or less active in virtual space, thus more exposing themselves to become a cyber victim. Factors influencing activity in cyberspace can be personal characteristics or character traits of users.*

Conclusion. *Cyberfraud can be considered a crime, which is implemented in virtual space and has specific features, relative to fraud in real life. Interaction in cyberspace involves risks of dispersal of users, less regulation and social control. The problem of cybercrime is definitely relevant for student youth. Experience of using cyberspace, life experience of cyberfraud experience, general character traits of a person cannot prevent this type of crime. Thus is why, there is a particular need for more research on this topic, namely through victimological study of youth virtual interactions, which will help to identify effective ways to eliminate the risks of cyberfraud.*

Keywords: *cyberfraud; psychological characteristics of perception; cyberspace; cybersecurity; students*.

Автори заявляють про відсутність конфлікту інтересів.
Recelved/Поступила: 20.04. 21.