

Bulletin of Taras Shevchenko National University of Kyiv.
Series "Psychology". № 2(16), pp. 19-24 (2022)
УДК 159.9
DOI: [https://doi.org/10.17721/BSP.2022.2\(16\).4](https://doi.org/10.17721/BSP.2022.2(16).4)

ISSN 1728-3817
© Taras Shevchenko National University of Kyiv,
Publishing and Polygraphic Center "Kyiv University", 2022

Ганна Коваль, канд. психол. наук, доц.
ORCID: 0000-0003-0291-7501

Одеський національний університет імені І. І. Мечникова, Одеса, Україна

ПСИХОЛОГІЯ ДЕВІАНТНИХ ФОРМ ЕКОНОМІЧНОЇ ПОВЕДІНКИ ОСОБИСТОСТІ В КІБЕРПРОСТОРИ

Розглянуто психологічні особливості девіантних форм економічної поведінки особистості в кіберпросторі. Під час написання статті використовували синтез, логіку і структуру викладу, аналіз й узагальнення проблематики наукових джерел. Підсумовано, що особливості девіантних форм економічної поведінки особистості в кіберпросторі все ще недостатньо вивчені, а увагу зосереджено більше на популярніших різновидах кібердевіантності.

Ключові слова: особистість злочинця, кіберзлочинність, трансформація соціально-економічної системи, протидія кіберзлочинності, безпека, кібердевіантність, онлайн-віктимізація.

Вступ. Стрімкий розвиток інформаційних технологій протягом останнього десятиліття супроводжується динамічним розвитком злочинів у цій сфері. Будь-який розвиток і прогрес, що давав людству цивілізаційні блага й нові можливості, завжди супроводжувався негативними явищами. Масова комп'ютеризація та стрімкий розвиток цифрових технологій, що суттєво спростили життя людини, не є винятком. Кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, оскільки з кожним роком кіберзлочини стають все більш поширеними та небезпечними. Кіберзлочинність – невід'ємна ознака глобалізації інформаційних процесів і, як наслідок, основна загроза соціально-гуманітарної складової. Дедалі більша кількість кіберзлочинів в установах й організаціях, безперервний розвиток інформаційних технологій і нові можливості для "вдосконалення" інструментарію їхнього вчинення створюють економічні загрози для глобальних інформаційних мереж [26].

В епоху інформаційних технологій неможливо відчувати себе захищеним у кіберпросторі. З розвитком технологій кількість злочинів у цій сфері стрімко зростає, а тому можна з упевненістю стверджувати, що саме кіберзлочинність у ХХІ ст. залишатиметься серед найчисленніших правопорушень. Більшість сучасних дослідників звертають увагу на своєрідність таких правопорушень і принципово економічну складову в мотивації цієї діяльності, стверджуючи, що кіберзлочинність – це не традиційна злочинність, а відносно нове явище, пов'язане з народженням і поширенням мережі інтернет як постмодерністського явища.

З огляду на свою антисоціальність і приховану ідентичність цей вид злочинів від самого початку виявився зручним і легким для зловмисників, шахраїв, правопорушників і просто мережових хуліганів. Окрім інформаційного та психологічного дисбалансу, що зазвичай стають логічним наслідком кіберпорушень, є сенс актуалізувати й економічну вигоду від таких дій. Адже особливо часто такі злочини у просторі мережової культури вчиняються із прагматичним мотивом незаконного збагачення [19].

Мета дослідження – розглянути психологічні особливості девіантних форм економічної поведінки особистості у кіберпросторі.

Під час написання статті використовували класичний перелік філософсько-світоглядних, загальнонаукових методів для реалізації проблемної повноти нашого дослідження й отримання науково обґрунтованих і достовірних результатів та загальнозначущих висновків:

синтез, логіка і структура викладу, аналіз й узагальнення проблематики наукових джерел.

Лінгвістичну методологію та метод пізнання використано для дослідження проблемних питань пропонованої роботи в єдності їхнього наочного та фактичного сприйняття, соціального змісту, юридичної та термінологічної форми репрезентації. Системно-структурний підхід дав змогу концептуально сформувати, реалізувати теоретичні засади та змодельовати складність дослідницького дискурсу.

Аналіз висновків про досліджувану проблему, надання огляду інших досліджень. Поширення комп'ютерів та інформаційних технологій у суспільстві змінило поведінку, пов'язану з інформацією; люди розв'язують інформаційні проблеми та діляться своїми знаннями й інформацією в інтернеті. Згідно з різними показниками, як-от використання інтернету, доступ до високосшвидкісного інтернету й оцінки електронної інформації, інформатизація є інтенсивною. Відповідно, зміни способу життя прискорилися завдяки розвитку бездротового інтернету, а також використанню смартфонів і планшетів.

Інтернет – це відкритий простір зі свободою вираження думок і правами, заснованими на принципах віддаленості та розширення. Хоча інтернет загалом пропонує суспільству підвищену ефективність, зручність, ефективність, продуктивність і розваги, він заохочує до девіантної поведінки в кіберпросторі, такої, як особиста безвідповідальність і вторгнення у приватне життя через анонімність, віддаленість, швидке поширення інформації тощо.

Інтернет має переваги й недоліки, оскільки втілює нові етичні проблеми порівняно з реальним простором, а девіантна поведінка в кіберпросторі виходить за межі психотравматичних впливів й охоплює економічні негативні наслідки. Девіантна поведінка в кіберпросторі виявляється як самовиявлення порнографії, фальсифікації особистої інформації та видавання себе за інших, незаконне завантаження музики і фільмів, плагіат.

З міждисциплінарної позиції девіантність є темою, що цікавить соціологів і психологів, оскільки стосується порушення затверджених правил і норм. Існує велика кількість опублікованих досліджень на визначену проблематику, що, однак, робить процес розуміння явища досить складним.

Результати дослідження. Особливу категорію девіантності, що стає дедалі більш поширеною в наш час, є кібердевіантність, яка стосується шкідливої діяльності, що відбувається в цифровій сфері [11, 16, 29].

© Коваль Ганна, 2022

Це характеризує випадки шкідливої поведінки, які так чи інакше пов'язані з комп'ютером, що викликає потужну реакцію з боку ЗМІ, політиків, науковців і громадськості. Таке трактування окреслює дві основні характеристики кіберзлочинності, а саме: електронне середовище та вплив, пов'язаний із підвищеною турботою про кібербезпеку.

Стверджуючи, що представлено визначення кіберзлочинності є надто широким, варто концептуалізувати кіберзлочинність як сукупність незаконних дій, пов'язаних з інформаційно-комунікаційними технологіями. Отже, кіберзлочинність стосується шкідливої діяльності в інтернеті, що санкціонована офіційними законами. Інші типи підривної діяльності в інтернеті об'єднані в загальне поняття кібердевіантності, що стосується неформальних порушень законів [11, 16, 29].

Зростання кіберзлочинності зумовлене трансформацією соціально-економічних систем, переходом до цифрової економіки та віртуального середовища проживання. Виділяють три основні групи кіберзлочинців [9]:

- Кіберзлочинці, які здійснюють злочинну діяльність лише в кіберпросторі. Злочинні угруповання сформовані в умовах криміналізації кіберпростору. Без факторів криміногенності такі особи становлять меншу суспільну небезпеку, ніж реальні злочинці.

- Кіберзлочинці, які здійснюють злочинну діяльність як у кіберпросторі, так і в реальному житті. Їхня психологія загалом є кримінальною. Однак вплив криміналізації кіберпростору незначний.

- Особи, які раніше вчиняли злочини, не пов'язані з кіберпростором, але згодом вчинили кіберзлочини. Цю групу утворюють організовані злочинні співтовариства, що використовують можливості, надані інтернетом. Хороші організаторські здібності допомагають таким кіберзлочинцям використовувати людей зі спеціальними знаннями для вчинення злочинів. Їхні основні зусилля спрямовані на максимізацію прибутку та збільшення свого впливу [9].

Залежно від мотивації злочинної поведінки виділяють такі типи кіберзлочинців (табл. 1).

Таблиця 1

Характеристика типів кіберзлочинців

Тип кіберзлочинця	Характеристика кіберзлочинів
Зацікавлений тип	Злочини, спрямовані на отримання конкретних предметів, цінних у кіберпросторі, наприклад, ігрових предметів для їхнього подальшого продажу
Залюбувальний тип	Кібербулінг і кіберпереслідування. Злочини, що характеризуються погрозами вбивством, доведенням до самогубства, можливо, з елементами шантажування за неопублікування певного особистого контенту
Сексуальний тип	Характеризуються незаконним розповсюдженням порнографічних матеріалів з метою отримання прибутку
Соціально-дезорганізуючий тип	Злочини, що порушують соціальні норми, передбачені законодавством, і здійснюють деструктивний вплив на суспільство
Ідеологічно або політично вмотивований тип	Є формою протесту, політичного або ідеологічного протистояння
Дослідницький тип	Мотивацією цих злочинів є дослідження програмно-апаратних компонентів електронних пристроїв та їхніх мереж, пошук вразливостей, можливості їхнього використання й усунення

Неповнолітні громадяни стають жертвами кіберзлочинців частіше, ніж дорослі. Найрезонанснішими подіями останніх років, пов'язаними з кіберзлочинністю, є масова участь підлітків у суїцидальних групах. Учасники груп отримують різноманітні завдання, спрямовані на заподіяння собі шкоди.

Вплив на неповнолітніх здійснюється або через приватні повідомлення в соціальних мережах, або через пропозиції перегляду відео, обговорення серіалів. Водночас такий вид злочинів має економічну складову – модератори таких соціальних груп й інтернет-сайтів за додаткову плату пропонують перегляд онлайн-трансляції самого самогубства.

Традиційна форма злочинності зазвичай здійснюється маргінальними членами суспільства, особливо молодими чоловіками, які страждають від численних депривацій або зловживають наркотиками чи алкоголем. На противагу цьому, люди, які мають порівняльну перевагу в онлайн-злочинності, зазвичай освічені і здібні, але вони живуть у соціумі з поганими перспективами працевлаштування й неефективною поліцією.

Високий рівень матеріальних цінностей створює напруження між індивідуальною орієнтацією на матеріальні цінності та колективною орієнтацією на сімейні й релігійні цінності. Це одним психологічним поясненням тенденції до шахрайства в інтернеті є тиск з боку однолітків. Молодь часто вважає за краще ідентифікувати себе із групою однолітків. Це пов'язано з тим, наскільки молодь схильна до впливу з боку друзів або близьких людей.

Група однолітків зі спільним досвідом є неминучим джерелом особистих стосунків. Часта взаємодія з однолітками, особливо з девіантними однолітками, іноді призводить до прийняття антисоціальної поведінки заради групового конформізму. Молоді люди потребують формування нової ідентичності та встановлення автономії від своїх батьків.

Часте спілкування з однолітками, навіть частіше, ніж із батьками, може призвести до того, що однолітки стають первинною основою для соціального порівняння. Узагальнена теорія соціального порівняння стверджує, що індивіди порівнюють власні матеріальні блага з матеріальними благами інших людей, щоб визначити свій соціальний статус. Однак багато досліджень вказують на те, що девіантні однолітки мають менший вплив на підлітків, які мають близькі стосунки з батьками.

Вплив однолітків і низький самоконтроль – основні фактори, що сприяють учиненню неповнолітніми кіберзлочинів, таких як комп'ютерний злам і знущання в інтернеті. Наявність друзів, які займаються кіберзлочинністю, є одним з найважливіших факторів, що визначають, чи будуть неповнолітні вчиняти кіберзлочини.

В іншому схожому дослідженні було представлено результати наукового опитування 435 учнів у шкільному окрузі штату Кентуккі [14].

Результати дослідження показали: найбільшим предиктором того, що неповнолітні можуть учинити кіберзлочини, є вплив однолітків. Також було зауважено, що низький самоконтроль має як прямий, так й опосеред-

кований вплив на кіберзлочинність серед неповнолітніх – через інших однолітків-правопорушників.

У дослідженні зазначено, що низький рівень самоконтролю і девіантні асоціації однолітків були пов'язані не тільки з кіберзлочинністю, але й із учиненням інших злочинів. Правопорушення з боку однолітків мають сильніший вплив на інших правопорушників, ніж низький самоконтроль. У дослідженні йдеться, що кіберзлочини можуть бути більш привабливими для молоді, ніж правопорушення в реальному світі через відносну анонімність, яку інтернет надає своїм користувачам.

Чим менший вік молоді, тим необачнішу поведінку вони демонструють (18–30 років). Це спостереження має значення для практики інтернет-шахрайства. Вік позитивно корелює з кіберзлочинністю.

Освітній рівень також виявився значущим у вияві злочинної поведінки. Шкільні досягнення є предиктором просоціальної поведінки або поведінки, спрямованої на підтримання моральних цінностей суспільства. Це пов'язано з тим, що академічні досягнення взаємопов'язані в суспільстві з кількома іншими змінними, як-от фінансовий успіх, висока самооцінка та внутрішній локус контролю. Ця конкретна модель може пояснити причини того, що особи з високим коефіцієнтом інтелекту (IQ) зазвичай мають меншу схильність до злочинної поведінки, ніж із низьким IQ.

Дедалі більше занепокоєння щодо шахрайської діяльності в інтернеті потребує врегулювання на рівні розроблення відповідних заходів. На закінчення, інформація на основі даних про фактори, пов'язані з кіберзлочинністю серед молоді, має бути наданою для інформування політики та її реалізації.

Для розв'язання цих проблем розглядали питання, чи будуть психологічні фактори, такі як самоконтроль, вплив однолітків, матеріальні цінності, імпульсивність, значною мірою незалежно та спільно прогнозувати тенденції шахрайства в інтернеті серед молоді. Важливим також є з'ясування міри впливу таких психологічних факторів, як демографічні – вік, стать та освіта.

Психологічні фактори, такі як самоконтроль, вплив однолітків, матеріалістичні цінності, імпульсивність і демографічні – вік, стать та освіта, незалежно та спільно прогнозують тенденції інтернет-шахрайства серед молоді. Усі змінні спільно передбачають тенденцію до інтернет-шахрайства. Однак ті молоді люди, які більш схильні до впливу однолітків, надають перевагу матеріальним цінностям та є імпульсивними, мають більшу схильність до шахрайства в інтернеті.

Професійна злочинність і правопорушення пов'язані як із внутрішніми факторами, що опосередковують злочинні схильності, так й із зовнішніми – як, наприклад, взаємодія з іншими видами злочинності. За індивідуального прогнозування вік, стать, матеріальні цінності та вплив однолітків були значущими, тоді як вплив однолітків мав найбільшу передбачуваність. Високий рівень матеріалістичних цінностей, як було виявлено, є посередником між індивідуальною орієнтацією на матеріальні цінності та колективною орієнтацією на сімейні та релігійні цінності. Водночас у молодіжному середовищі прагнення молоді до матеріального збагачення є одним із факторів, що додатково схиляє її до інтернет-шахрайства.

Вплив однолітків на поведінку інтернет-шахраїв також відзначали інші науковці [3, 12]. Вони з'ясували, що спілкування з однолітками-правопорушниками є важливим предиктором злочинної поведінки серед молоді. Цей результат спостерігали під час впливу необачної

поведінки серед молоді [6]. Важливість висновків учених полягає в тому, що чим старша молодь, тим більше вона схильна до шахрайства в інтернеті.

Варто також зауважити, що незалежно від того, чи є батьки освіченими, чи ні, молодь все одно може брати участь в інтернет-шахрайстві. Стать молоді також відіграє певну роль у прийнятті відповідної поведінки. Чоловіки переважно більше залучені до скоєння злочинів, ніж жінки, як підтверджено в дослідженні [6].

У деяких випадках така молодь може бути або залучена до злочинної поведінки, або, ймовірно, утягнута в інші види шахрайських дій. Однак перераховані фактори не є вичерпними, оскільки існують ще й інші детермінанти, що можуть схилити молодь до інтернет-шахрайства.

Ідеологічно вмотивовані особи, які займаються економічними злочинами, отримують вигоду від взаємодії з корисливими правопорушниками та законними суб'єктами, що надають ресурси для злочинів у вигляді знань, навичок і співучасників [25]. Причиною цього є те, що профіль економічних правопорушників у кіберпросторі нині надзвичайно диверсифікований до такої міри, що стає дедалі важче відрізнити звичайного злочинця від типового економічного правопорушника, такого як міжнародний терорист або внутрішній політичний екстреміст.

З погляду психології, психологічне пояснення злочинності мало б простий вигляд, як-от "жадібність і нечесність". На думку вчених, таке пояснення є надто спрощеним [10]. Не всі нечесні люди вчиняють шахрайство. Отже, до цього часу жоден учений-біхевіорист не зміг надати психологічну характеристику, яка слугує валідним і надійним маркером, індикатором, символом або ознакою схильності індивіда до вчинення шахрайства. Як результат, існують численні приклади спроб відрізнити людей, які вчиняють шахрайство або схильні до вчинення шахрайства за наявності відповідної ситуації, від тих, хто цього не зробить.

Наукова дискусія. Основні висновки щодо різних факторів ризику для економічної форми кібердевіантності були потрібними.

По-перше, онлайн-рутини й активність відіграють значну роль як у різноманітності різних типів девіантних форм поведінки в кіберпросторі, так і полівіктимізації. Теоретичні передумови теорії рутинної діяльності добре узгоджуються з відповідними твердженнями. Чим активніші особистість діє в кіберпросторі, чим більше наражається на потенційних правопорушників й інші небезпеки, тим більша ймовірність, що вони стануть жертвами. Ці твердження узгоджуються з більшістю наявних досліджень онлайн-віктимізації [17].

Незважаючи на можливий контроль використання інтернету в різних ситуаціях та різними групами користувачів, також можливо, що лише певні типи моделей поведінки в мережі призводять до того, що люди стають, наприклад, жертвами переслідування або шкідливим програмам, що можуть пояснити результати багатьох наукових досліджень [4, 6, 24].

Навички користувача не функціонують як захисний фактор, який би зробив тих чи інших осіб менш придатними для ролі жертви для економічних кіберзлочинців. Однак це має сенс, оскільки попередні дослідження показали, що користувачі, які найбільш вільно спілкуються, також повідомляють про більш різноманітне використання інтернету [12]. Це означає, що навички користувачів зазвичай відображають активніше використання різних форм нових технологій, таким чином від-

дзеркалюючи вікно експозиції. З огляду на це зрозуміло, що ці ж елементи також пов'язані з більшим ризиком стати жертвою економічних кіберзлочинців. Це також показує, що в онлайн-контексті активніша присутність урізноманітнює діапазон ризиків віктимізації.

Результати аналізу різнопланових контекстів захисту користувачів від економічних кіберзлочинців є досить посередніми. Захисні заходи краще протидіють ризикам, пов'язаним зі зловмисним програмним забезпеченням і вірусами, ніж із соціальними діями та поведінкою. Для пересічного користувача різні захисні заходи, що застосовують виробники, розробники та постачальники платформ нових форм технологій, мають значення, коли цілком є техніка.

Головне питання полягає в тому, що робити, коли мішенню є конкретна людина. Майбутні дослідження також потребують проведення детальнішого аналізу віктимізації зловмисного програмного забезпечення, особливо коли йдеться про конкретні його форми. Саме цей формат економічної кіберзлочинності має досить пасивний характер – злочинцю достатньо розробити комп'ютерний алгоритм один раз, а потім отримувати багаторазові дивіденди. Це своєрідний пасивний злочинний дохід. Проте високий рівень захисту користувачів зменшив ризик полівіктимізації. Можливо, ті користувачі, які приділяють більше уваги аспектам захисту особистої інформації, дещо обережніші у своїй загальній онлайн-поведінці.

По-друге, офлайн-віктимізація має значення. Показово, що попередня кіберзлочинність є фактором ризику для широкого спектру онлайн-віктимізації, а також онлайн-полівіктимізації. Це ще більше підтверджує та доповнює результати попередніх досліджень, які відзначають, що онлайн- та офлайн-жертви не є повністю окремими групами жертв, а онлайн-середовище розширило середовище віктимізації серед тих, хто вже є жертвами в реальному житті [7, 15, 20, 21].

Отже, відбувається накопичення негативного досвіду як в офлайн-, так і в онлайн-контексті, де людина не є захищеною, навіть якщо правопорушник фізично відсутній. Нещодавні дослідження з'ясували, як примусовий контроль поширився на цифрові платформи та комунікаційні засоби [8, 13], що надалі надасть можливість для часткового пояснення збігу віктимізації від переслідувань в інтернеті, а також злому особистої електронної пошти чи облікового запису в соціальних мережах із віктимізацією насильства офлайн.

Однак здійснені висновки все ще викликають додаткові запитання, наприклад, чому минулий досвід віктимізації насильства підвищує ризик віктимізації щодо такої кількості різних типів онлайн-віктимізації та полівіктимізації? Чи це лише накопичення всіляких негативних переживань? Відповідно, існує потреба в подальших комплексних дослідженнях.

По-третє, різні типи кіберзлочинців мають різні фактори ризику. Незважаючи на те, що офлайн-віктимізація підвищувала ризик онлайн-віктимізації, роль різних соціально-економічних факторів у деяких випадках була іншою порівняно із факторами ризику щодо багатьох форм офлайн-віктимізації. Було виявлено, наприклад, що слабка фінансова ситуація є фактором ризику для багатьох типів офлайн-віктимізації [28]; однак хороша фінансова ситуація, фактично, збільшує ризик віктимізації зловмисного програмного забезпечення та різних форм переслідувань в інтернеті, а також полівіктимізації. Крім того, освіта не відіграє чіткої ролі, коли йдеться про онлайн-віктимізацію [4].

Цілком можливо, що ті, хто має кращий фінансовий стан, піддаються більшому ризику частково через те, що вони зазвичай є активнішими користувачами інтернету [27], й, отже, потенційно доступніші для широкого кола економічних кіберзлочинців. Водночас проблема також може полягати в тому, що вони мають більшу "поверхню атаки" або, іншими словами, мають більше пристроїв у своєму розпорядженні.

Крім того, в онлайн-контексті (потенційно захисний) ефект сусідства також зникає. Людина не має захисного фізичного оточення, наприклад, проживання в огороженому населеному пункті або проживання в іншому безпечному районі міста, отже, потенційно вирівнюючи умови для скоєння економічних злочинів. Це, безумовно, елементи, які вимагають подальших досліджень.

Визнано, що людина як кінцевий користувач може бути критичним компонентом у мережі [2]. Ученими в дослідженні був використаний поведінковий науковий підхід для визначення факторів, що формують поведінкові рішення користувачів щодо економічної кібербезпеки [1].

Результати свідчать про те, що сприйняття безпеки та загальні зовнішні фактори впливають на індивідуальну поведінку щодо економічної кібербезпеки, і ці фактори регулюються характеристиками користувачів (стать, вік) і робочим середовищем. Проведений огляд психологічних напрацювань дав змогу наголосити, що кілька кримінологічних теорій забезпечують важливі рамки, які скеровують емпіричні дослідження різних ситуацій в екосистемі кіберзалежної злочинності [18].

Варто зауважити, що необхідні додаткові дослідження в окресленій проблематиці, оскільки існує ймовірність, що незабаром кіберзлочинність вийде на передній план у кримінологічній та психологічній наукових сферах. Найпопулярніші кримінологічно-психологічні пояснення кіберзлочинності охоплюють теорію навчання, самоконтролю, нейтралізації та теорію рутинної діяльності [22].

Загалом їхні висновки підтверджують той факт, що інтеграція економічної кібербезпеки у психологічну просвіту відбувається не швидко, імовірно, через те, що кілька психологів вивчають психологічні особливості девіантних форм економічної поведінки особистості в кіберпросторі.

Звертаючись до важливості залучення людської поведінки до проектування та створення кібертехнологій [23], учені представили дві теми поведінкових аспектів:

- когнітивне навантаження, що може сприяти неуважній сліпоті, яка заважає користувачу кіберпростором помічати несподівані події, коли зосереджується на основній цілі перебування в онлайн-середовищі;
- упередження, які можуть допомогти психологам і розробникам безпеки передбачити сприйняття і враховувати їх у різноманітних просвітницьких заходах.

Обрана проблематика є настільки широкою, що потребує окреслення ключових питань для з'ясування першопричин, особливостей, розвитку особистості, схильної до девіантних форм економічної поведінки в кіберпросторі. Доцільним є визначення того, наскільки ці параметри залежать від країни проживання, рівня освіченості, виду зайнятості, наявності віктимного досвіду в реальному житті.

Висновки. Підводячи підсумок, варто зазначити, що особливості девіантних форм економічної поведінки особистості в кіберпросторі все ще недостатньо вивчені, а увага зосереджена більше на популярніших різновидах кібердевіантності. Однією із проблем є

складність проведення досліджень у разі звернення до різних теорій та з урахування ключової особливості кіберпростору – анонімності. Водночас головна мета психологічної науки полягає в тому, щоб надати інформацію про поточні проблеми, наприклад, особливості формування економічної кібердевіантності; виявлення схильності до такого виду поведінки; планування корекційної та просвітницької психологічної роботи з девіантами та жертвами економічної кіберзлочинності.

Слід зауважити, що відповідно до проаналізованих наукових досліджень існує значна кількість односторонніх вивчень обраної проблематики, комплексних і систематизованих робіт виявлено не було. Частина з обраних досліджень презентує напрацювання на американській, азійській та африканській аудиторіях, що характеризуються суттєвими відмінностями у соціальній, культурній та економічній площині формування особистості як майбутнього кіберпорушника, так і потенційної жертви. Це дає змогу констатувати низьку валідність і надійність отриманих результатів.

Оскільки питання девіантної та делінквентної поведінки перебувають на перетині наукових інтересів психології та кримінології, кібербезпеки, ІТ, це варто враховувати під час здійсненні планування дослідження, щоб задовольнити потреби всіх сфер.

Список використаних джерел

- Addae J. H., Sun X., Towey D., Radenkovic M. Exploring user behavioral data for adaptive cybersecurity. *User Model User-Adap Inter.* 2019. № 29 (3). P. 701–750.
- Ahram T., Karwowski W. Advances in Human Factors in Cybersecurity. *AHFE: international conference on applied human factors and ergonomics*. Springer. Washington D. C. 2019. P. 66–96.
- Atwai A. Youth cybercrime influenced by peers youth today. University of Liverpool. 2011. URL: <http://www.youthtoday.org/viewarticle.cfm?articleid=4859>.
- Bergmann M. C., Dreißigacker A., von Skarzynski B., Wollinger G. R. Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking*, 2018. № 21 (2). P. 84–90.
- Branley D. B., Covey J. Is exposure to online content depicting risky behavior related to viewers own risky behavior offline? *Computers in Human Behavior*. 2017. № 75. P. 283–287.
- Burton V. S. Jr., Evans T. D., Cullen G. T., Olivares K. M. Age, self-control, operationalization theories and adult criminality. *Journal of qualitative criminology*. 1999. № 10. P. 213–239.
- Choi K., Cho S., Lee J. R. Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior*. 2019. № 100. P. 1–10.
- Dragiewicz M., Burgess J., Matamoros-Fernández A., Salter M., Suzor N. P., Woodlock D., Harris B. Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*. 2018. № 18 (4). P. 609–625.
- Duff A. The Normative Crisis of the Information Society. *Cyberpsychology: Journal of psychosocial research on cyberspace*. 2008. № 2 (1). 3 p.
- Duffield G., Grabosky P. The psychology of fraud, trends and issues in crime and criminal justice. *Australian Institute of Criminology*. 2001. № 199. P. 1–6.
- Graham R. S., Smith S. K. Cybercrime and digital deviance. New York, NY: Taylor and Francis; Routledge. 2019. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9781351238090/cybercrime-digital-deviance-roderick-graham-shawn-smith>.
- Hargittai E. Digital na (t) ives? variation in internet skills and uses among members of the "Net Generation". *Sociological Inquiry*. 2010. № 80 (1). P. 92–113.
- Harris B. A., Woodlock D. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*. 2019. № 59 (3). P. 530–550.
- Holt T. J. Low self-control, deviant peer associations, and juvenile cybercrime. *American journal of criminal justice*. 2011. URL: <https://news.msu.edu/medial/06/963e40c7-08ff-411d-af1-fe7563496f89.pdf>
- Ioannou M., Synnott J., Reynolds A., Pearson J. A comparison of online and offline grooming characteristics: An application of the victim roles model. *Computers in Human Behavior*. 2018. № 85. P. 291–297.
- Jewkes Y., Yar M. Handbook of internet crime. London ; New York, NY: Taylor and Francis; Routledge. 2013. URL: <https://books.google.ro/books?>
- Leukfeldt E. R., Yar, M. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*. 2016. № 37 (3). P. 263–280.
- Maimon D., Louderback E. R. Cyber-Dependent Crimes: An interdisciplinary review. *Ann Rev Criminol*. 2019. № 2 (1). P. 191–216.
- Matveev V., Nykytchenko N., Stefanova N., Khrypko S., Ishchuk A., Pasko K. Cybercrime in the economic space: psychological motivation and semantic-terminological specifics. *International journal of computer science and network security*. 2021. № 21 (8). P. 203–211.
- Mitchell K. J., Finkelhor D., Wolak J., Ybarra M. L., Turner H. Youth internet victimization in a broader victimization context. *Journal of Adolescent Health*. 2011. № 48 (2). P. 128–134.
- Oksanen A., Keipi T. Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies*. 2013. № 8 (4). P. 298–309.
- Payne B. K., Hadzhidimova L. Cyber security and criminal justice programs in the United States: Exploring the intersections. *Int J Crim Justice Sci*. 2018. № 13 (2). P. 385–404.
- Pfleeger S. L., Caputo D. D. Leveraging behavioral science to mitigate cyber security risk. *Comput Secur*. 2012. № 31 (4). P. 597–611.
- Reyns B. W., Fisher B. S., Bossler A. M., Holt, T. J. Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*. 2019. № 44 (1). P. 63–82.
- Roberta B. Where political extremists and greedy criminals meet: A comparative study of financial crimes and criminal networks in the United States. *A dissertation submitted to the Graduate Faculty in Criminal Justice in partial fulfillment of the requirements for the degree of Doctor of Philosophy*. The City University of New York. 2011. URL: <https://www.cjg.gov/pdffiles1/nij/grants/234524.pdf>.
- Singh S., Silakari S. A survey of cyber-attack detection systems. *International. Journal of computer science and network security*. 2022. № 5. P. 1–10.
- Statistics Finland. Use of information and communications technology by individuals. 2018. URL: http://www.stat.fi/ti/sutivi/2018/sutivi_2018_2018-12-04_tie_001_en.html. Accessed 10th of March 2020.
- Tilley N., Tseloni A., Farrell G. Income disparities of burglary risk: Security availability during the crime drop. *The British Journal of Criminology*. 2011. № 51 (2). P. 296–313.
- Yar M., Steinmetz K. F. Cybercrime and Society. Thousand Oaks, CA: SAGE Publications, 2019. 368 p.

References

- Addae J. H., Sun X., Towey D., Radenkovic M. Exploring user behavioral data for adaptive cybersecurity. *User Model User-Adap Inter.* 2019. № 29 (3). P. 701–750.
- Ahram T., Karwowski W. Advances in Human Factors in Cybersecurity. *AHFE: international conference on applied human factors and ergonomics*. Springer. Washington D. C. 2019. P. 66–96.
- Atwai A. Youth cybercrime influenced by peers youth today. University of Liverpool. 2011. URL: <http://www.youthtoday.org/viewarticle.cfm?articleid=4859>.
- Bergmann M. C., Dreißigacker A., von Skarzynski B., Wollinger G. R. Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking*, 2018. № 21 (2). P. 84–90.
- Branley D. B., Covey J. Is exposure to online content depicting risky behavior related to viewers own risky behavior offline? *Computers in Human Behavior*. 2017. № 75. P. 283–287.
- Burton V. S. Jr., Evans T. D., Cullen G. T., Olivares K. M. Age, self-control, operationalization theories and adult criminality. *Journal of qualitative criminology*. 1999. № 10. P. 213–239.
- Choi K., Cho S., Lee J. R. Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior*. 2019. № 100. P. 1–10.
- Dragiewicz M., Burgess J., Matamoros-Fernández A., Salter M., Suzor N. P., Woodlock D., Harris B. Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*. 2018. № 18 (4). P. 609–625.
- Duff A. The Normative Crisis of the Information Society. *Cyberpsychology: Journal of psychosocial research on cyberspace*. 2008. № 2 (1). 3 p.
- Duffield G., Grabosky P. The psychology of fraud, trends and issues in crime and criminal justice. *Australian Institute of Criminology*. 2001. № 199. P. 1–6.
- Graham R. S., Smith S. K. Cybercrime and digital deviance. New York, NY: Taylor and Francis; Routledge. 2019. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9781351238090/cybercrime-digital-deviance-roderick-graham-shawn-smith>.
- Hargittai E. Digital na (t) ives? variation in internet skills and uses among members of the "Net Generation". *Sociological Inquiry*. 2010. № 80 (1). P. 92–113.
- Harris B. A., Woodlock D. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology*. 2019. № 59 (3). P. 530–550.
- Holt T. J. Low self-control, deviant peer associations, and juvenile cybercrime. *American journal of criminal justice*. 2011. URL: <https://news.msu.edu/medial/06/963e40c7-08ff-411d-af1-fe7563496f89.pdf>
- Ioannou M., Synnott J., Reynolds A., Pearson J. A comparison of online and offline grooming characteristics: An application of the victim roles model. *Computers in Human Behavior*. 2018. № 85. P. 291–297.

16. Jewkes Y., Yar M. Handbook of internet crime. London ; New York, NY: Taylor and Francis; Routledge. 2013. URL: <https://books.google.ro/books?>
17. Leukfeldt E. R., Yar, M. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*. 2016. № 37 (3). P. 263–280.
18. Maimon D., Louderback E. R. Cyber-Dependent Crimes: An interdisciplinary review. *Ann Rev Criminol*. 2019. № 2 (1). P. 191–216.
19. Matveev V., Nykytchenko N., Stefanova N., Khrypko S., Ishchuk A., Pasko K. Cybercrime in the economic space: psychological motivation and semantic-terminological specifics. *International journal of computer science and network security*. 2021. № 21 (8). P. 203–211.
20. Mitchell K. J., Finkelhor D., Wolak J., Ybarra M. L., Turner H. Youth internet victimization in a broader victimization context. *Journal of Adolescent Health*. 2011. № 48 (2). P. 128–134.
21. Oksanen A., Keipi T. Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies*. 2013. № 8 (4). P. 298–309.
22. Payne B. K., Hadzhidimova L. Cyber security and criminal justice programs in the United States: Exploring the intersections. *Int J Crim Justice Sci*. 2018. № 13 (2). P. 385–404.
23. Pfleeger S. L., Caputo D. D. Leveraging behavioral science to mitigate cyber security risk. *Comput Secur*. 2012. № 31 (4). P. 597–611.
24. Reyns B. W., Fisher B. S., Bossler A. M., Holt, T. J. Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*. 2019. № 44 (1). P. 63–82.
25. Roberta B. Where political extremists and greedy criminals meet: A comparative study of financial crimes and criminal networks in the United States. *A dissertation submitted to the Graduate Faculty in Criminal Justice in partial fulfillment of the requirements for the degree of Doctor of Philosophy*. The City University of New York. 2011. URL: <https://www.ojp.gov/pdffiles1/nij/grants/234524.pdf>.
26. Singh S., Silakari S. A survey of cyber-attack detection systems. International. *Journal of computer science and network security*. 2022. № 5. P. 1–10.
27. Statistics Finland. Use of information and communications technology by individuals. 2018. URL: http://www.stat.fi/til/sutivi/2018/sutivi_2018_2018-12-04_tie_001_en.html. Accessed 10th of March 2020.
28. Tilley N., Tseloni A., Farrell G. Income disparities of burglary risk: Security availability during the crime drop. *The British Journal of Criminology*. 2011. № 51 (2). P. 296–313.
29. Yar M., Steinmetz K. F. Cybercrime and Society. Thousand Oaks, CA: SAGE Publications, 2019. 368 p.

Надійшла до редколегії 25.08.22
Рекомендована до друку 30.11.22

Hanna Koval, PhD (Psychology), Associate Prof.

ORCID: 0000-0003-0291-7501

Odessa I. I. Mechnikov National University, Odessa, Ukraine

PSYCHOLOGY OF THE DEVIANT FORMS OF ECONOMIC PERSONAL BEHAVIOR IN THE CYBERSPACE

The author achieved the defined goal of the research - the psychological features of the deviant forms of economic behavior of an individual in cyberspace were considered. When writing the article, we used a classic set of philosophical and worldview, general scientific methods to implement the problematic completeness of our research and obtain scientifically based and reliable results and general conclusions: synthesis, logic and structure of the presentation, analysis and generalization of the problems of scientific sources. Linguistic methodology and the method of cognition were used to study the problematic issues of this work in the unity of their visual and factual perception, social content, legal and terminological form of representation. The systemic-structural approach made it possible to conceptually form, implement the theoretical foundations and model the complexity of the research discourse. It was noted that crime and delinquency are related to both internal factors that mediate criminal tendencies and external factors such as interaction with other types of crime, age, gender, material values, and the influence of peers. It is concluded that the specifics of deviant forms of individual economic behavior in cyberspace are still not sufficiently studied, and attention is focused more on more popular types of cyber deviance. It was noted that one of the problems is the difficulty of conducting research when referring to various theories and taking into account the key feature of cyberspace – anonymity. At the same time, it is emphasized that the main goal of psychological science is to provide information about current problems, for example, the peculiarities of the formation of economic cyber deviance; detection of a tendency to this type of behavior; planning correctional and educational psychological work with deviants and victims of economic cybercrime.

Keywords: personality of the criminal; cybercrime; transformation of the socio-economic system; combating cybercrime, security; cyber deviance; online victimization.