2. Бех І. Д. Виховання особистості / І. Д. Бех : [в 2-х кн. / Кн. 1.]. – К.: Либідь, 2003. – 280 с.
3. Братусь Б. С. Психологическое и нравственное пространство нормы / Братусь Б. С. // Журнал практикующего психолога. – Вып. 3. – 1997. – С. 6 – 17.
4. Леонтьев Д. А. Очерк психологии личности / Д. А. Леонтьев – М.: Смысл, 1993. – 64 с.
5. Ненастьев А. Н. Самоубийство как девиантное поведение : [Электронный ресурс] / А. Н. Ненастьев − Режим доступу к стат. : http://tzone.kulichki.com/religion/tanatos/suicide.html
6. Ручка А. А. Социальные ценности и нормы / Ручка А. А. – К.: Наук. думка, 1976. – 152 с.
7. Сухова Э. Психология самоубийства : [Электронный ресурс] / Э. Сухова // АиФ Долгожитель, 19.01.07. − Режим доступу к стат. :
8. http://www.polezen.ru/landd/psih.php
9. Узнадзе Д. Н. Установка у человека. Проблема объективации / Д. Н. Узнадзе // Психология личности в трудах отечественных психологов. – СПб.: Питер, 2000. – С. 87 – 91.
10. Франкл В. О смысле жизни: Психология личности. / В. Франкл. – Т. 1 / Под ред. Д. Я. Райгородского. – Самара: Бахрах-М, 2000. – 448 с.

УДК 343.95

Коваль О. Є.
к.пед.н., доцент кафедри психології та
соціальної роботи ЮФ ТНЕУ

ПСИХОЛОГІЧНИЙ ПОРТРЕТ КІБЕРЗЛОЧИНЦЯ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Поряд з перевагами, комп'ютеризація має низку негативних ефектів, одним із яких є кіберзлочинність. Наслідки цієї злочинності зачіпають не лише інтереси окремих осіб, що стали жертвами, але й компанії, організації та суспільство в цілому.

Теоретико-методичні та науково-практичні основи попередження дій кіберзлочинців були закладені у дослідженнях В. Голубєва, А. Долгової, О. Іванченко, М. Кастельса, Т. Кесаревої, М. Кравцової, Л. Куракова, А. Лукацького І. Рассолова, С. Смірнова [1]. Проте, не дивлячись на наявність значного масиву теоретико-практичних напрацювань з означеного напряму наукового пошуку, психологічні засади науково обґрунтованого дослідження портрету кіберзлочинця висвітлені неповно. Викладені обставини у своїй сукупності обґрунтовують актуальність наукових розвідок, позаяк ефективна та успішна боротьба з кіберзлочинами є неможливою без всебічного психологічного аналізу образу мислення та особи порушника.

Зазначимо, що кіберзлочин – це втручання в роботу телекомунікаційних мереж, комп'ютерних програм, що функціонують у їх середовищі, або несанкціонована модифікація комп'ютерних даних, зухвала дезорганізація роботи критично важливих елементів інфраструктури держави, що створює небезпеку загибелі людей, завдання значної майнової шкоди або настання інших суспільно небезпечних наслідків, здійснюване з метою порушення суспільної безпеки, залякування населення або впливу на ухвалення органами влади вигідних злочинцям рішень, задоволення їхніх майнових чи інших інтересів. Для повної ясності введемо поняття кіберзлочинця як висококваліфікованого фахівця у галузі інформаційних технологій, котрий здійснює дію з проникнення в інформаційну систему з метою порушення її цілісності або використання інформації у корисливих неправомірних цілях [4].

Залежно від віку виділяють дві групи кіберзлочинців: від 14 до 20 років та від 21 року і старші. До особливостей вчинення кіберзлочинів першою групою осіб належать: відсутність цілеспрямованої, продуманої підготовки до злочину; оригінальність способу; неприйняття заходів для приховування злочину; факти невмотивованого бешкетництва. Діяння осіб віком понад 21 рік, як правило, мають усвідомлений корисливий характер. Дослідження показують, що злочинці цієї групи, зазвичай, є членами добре організованих, мобільних і технічно оснащених висококласним обладнанням і спеціальною технікою (нерідко оперативно-технічного характеру) злочинних груп і співтовариств. Осіб, які входять до їх складу, загалом можна охарактеризувати як висококваліфікованих спеціалістів з вищою юридичною, економічною чи технічною освітою. Злочини носять багатоепізодний характер, обов'язково супроводжуються діями, спрямованими на приховування злочинів. Правоохоронна практика показує, що на долю цих злочинів припадає найбільша кількість посягань, які мають особливо небезпечний характер. За станом здоров'я такі особи частіше слабо розвинуті, мають певні особливості у фізичній конституції – худорлявість або зайву вагу. За ознакою зайнятості найбільше в Україні вчиняють злочини працездатні особи, які ніде не працюють і не навчаються (45-50%) [2].

Дослідники виділяють найбільш притаманні для типового кіберзлочинця індивідуально-психологічні риси: виражені порушення емоційно-вольової сфери, відхилення у психосексуальному розвитку, виражені аутичні прояви у сполученні із соціальним аутсайдерством, користолюбство, мстивість, антигуманна спрямованість, озлобленість, відчуття нерівності чи другорядності, боязкість і лякливість у соціальних та міжособистих стосунках, заглибленість у своїх думках, мріях, фантазіях, філософське сприйняття світу, відсутність буттєвих ціннісних орієнтацій, викривлена (збочена) система життєвих цінностей, тотальна недовірливість та виражений цинізм, прагнення уникнути перешкод у подоланні життєвих труднощів. Також зарубіжні вчені виділяють п'ять найпоширеніших мотивів скоєння комп'ютерних злочинів: корисливий мотив – 66%, політичні мотиви (шпигунство, злочини, спрямовані на підрив фінансової, кредитної політики уряду, дезорганізацію валютної системи країни) – 17%, дослідницький інтерес – 7%; хуліганські мотиви – 5%, помста – 3%.

За метою та сферою злочинної діяльності комп'ютерних злочинців можна поділити на окремі підгрупи [2]:

1. Хакери (hacker) отримують задоволення від вторгнення та вивчення великих ЕОМ за допомогою телефонних ліній та комп'ютерних мереж. Це комп'ютерні хулігани, електронні корсари, які без дозволу проникають в чужі інформаційні мережі для забави. У значній мірі їх тягне до себе подолання труднощів: чим складніша система, тим привабливіша вона для хакера. За допомогою телефону і домашніх комп'ютерів вони підключаються до мереж, які пов'язані з державними та банківськими установами, науково-дослідними та університетськими центрами, військовими об'єктами. Хакери, як правило, не роблять шкоди системі та даним, отримуючи насолоду тільки від почуття своєї влади над комп'ютерною системою.

2. Крекери (cracker) – більш серйозні порушники, ніж хакери, здатні спричинити будь-яку шкоду системі. Вони викрадають інформацію, викачуючи за допомогою комп'ютера цілі інформаційні банки, змінюють та псують файли.

3. Фрікери (phone+break=phreak) спеціалізуються на використанні телефонних систем з метою уникнення від оплати телекомунікаційних послуг. Також отримують насолоду від подолання труднощів технічного плану. У своїй діяльності фрікери використовують спеціальне обладнання («чорні» та «блакитні» скрині), яке генерує спеціальні тони виклику для телефонних мереж.

4. Колекціонери (codeskids) використовують програми, які перехоплюють різні паролі, а також коди телефонного виклику та номери приватних телефонних компаній, які мають вихід до загальної мережі. Як правило, вони молодші за хакерів та фрікерів. Обмінюються програмним забезпеченням, паролями, номерами, але не торгують ними.

5. Кіберплути (cybercrooks) – це злочинці, які спеціалізуються на розрахунках, використовують комп'ютери для крадіжки грошей, отримання номерів кредитних карток та іншої цінної інформації. Отриману інформацію потім продають іншим особам, досить часто контактують з організованою злочинністю. Популярними товарами для них є кредитна інформація, інформаційні бази правоохоронних органів та інших державних установ.

6. Торгаші або пірати (waresdudes) спеціалізуються на збиранні та торгівлі піратським програмним забезпеченням.

Досить цікавими виявилися результати дослідження М. Кравцової [3], яка встановила, що у своїй більшості кіберзлочинці – це працездатні, але не працюючі (43,7 %), неодружені (58 %) або одружені, але такі, що з родиною не живуть (16 %), чоловіки (90,8 %), віком 30–50 років (43,1 %), громадяни України (95,5 %), які мають вищу освіту (48,1 %). За розподілом засуджених через вчинення кіберзлочинів за родом їх занять виявлено, що першою за поширеністю після працездатних непрацюючих осіб є група службовців, на частку яких припадає 17 % (з них 1,7 % – державні службовці). Другою – робітники (16,1 %) та приватні підприємці (11,4 %). На третьому місці за поширеністю перебувають особи, які навчаються – 7,4 % (6,9 % складають студенти навчальних закладів, 0,5 % – учні шкіл, ліцеїв, коледжів, гімназій). На четвертому – працівники господарських товариств (3,3 %), на п'ятому – пенсіонери (1,1 %). Питома вага осіб, які на момент вчинення кіберзлочину мали не зняту та непогашену судимість, у структурі засуджених є відносно сталою протягом останніх 5 років та складає 5,8 %. З них 5 % мають одну, 0,8 % – дві судимості. Основну частину цих осіб складають такі, попередня судимість яких пов'язана із вчиненням злочинів проти власності (67 %),

злочинів у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів (27 %), злочинів проти життя та здоров'я особи (3 %), проти громадського порядку та моральності (2 %), інших злочинів – 1 %. У результаті дослідження науковець не виявила жодного кіберзлочинця, який би вчиняв злочини у стані сп'яніння. Серед мотивів кіберзлочинів М. Кравцова називає корисливі, ігрові, політичні та хуліганські (нігілістичні, самоствердження, помста). Відтак, серед морально-психологічних рис кіберзлочинців, на її думку, переважають корисливість, авантюризм, правовий та моральний нігілізм, поєднані з детермінованим специфікою кіберпростору комплексом сваволі та ілюзій.

Виходячи із вищевикладеного, висновуємо, що необхідність запобігання кіберзлочинам є дуже актуальною сьогодні. Вважаємо, що базовим елементом у боротьбі із кіберзлочинністю є підвищення рівня правосвідомості громадян, проведення віктимологічної профілактики, спрямованої на підвищення психологічної грамотності інтернет-користувачів, які не застосовують засобів захисту або не знають про існування таких та професійних користувачів, яким необхідно отримувати інформацію про нові впровадження у сфері комп'ютерної безпеки.

ЛІТЕРАТУРА:

1. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності / В. Б. Дзюндзюк, Б. В. Дзюндзюк. // Державне будівництво. – 2013. – № 1. – Режим доступу: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3
2. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні / О. Ю. Іванченко // Актуальні проблеми вітчизняної юриспруденції. – 2016. – Вип. 3. – С. 172–177.
3. Кравцова М. О. Кіберзлочинність : кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис ... канд. юрид. наук: 12.00.08 / Марина Олександрівна Кравцова. – Харків, 2016. – 16 с.
4. Пилипчук В. Г. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації / В. Г. Пилипчук, О. П. Дзьобань // Стратегічна пріоритети. – №4 (21), 2011. – С. 12–17