УДК 159.99:343.982.323

О. О. Бабенко
головний судовий експерт
Полтавський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

А. С. Мокляк
головний судовий експерт
Полтавський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

ТЕОРЕТИЧНИЙ АНАЛІЗ ДОСЛІДЖЕННЯ ПСИХОЛОГІЧНОГО ПОРТРЕТА КІБЕРЗЛОЧИНЦЯ

У статті проаналізовані поняття «кіберзлочин» та «кіберзлочинець». Визначено основні типи кіберзлочинців. За допомогою соціальних і психологічних теорій особистості визначаються основні риси, притаманні кіберзлочинцям. Зауважено значення методу визначення психологічного портрета кіберзлочинця для попередження та розкриття кіберзлочинів.

Ключові слова: *кіберпростір, кіберзлочинність, кіберзлочинець, хакер, психологічний портрет, судово-психологічна експертиза.*

Постановка проблеми. Стрімкий розвиток комп'ютерних технологій і вдосконалення Інтернету породжує новий вид злочинності – «кіберзлочинність». У минулому кіберзлочини скоювали в основному окремі особи або невеликі групи осіб. Сьогодні ми спостерігаємо надзвичайно складні спільноти кіберзлочинців, що об'єднують людей у всьому світі в режимі реального часу, щоб вчинити злочини в безпрецедентному масштабі.

Самі злочини не обов'язково нові, а навпаки, звичні: крадіжка, шахрайство, гральний бізнес, продаж підроблених ліків, але вони розвиваються відповідно до можливостей, наданих Інтернетом, а отже, стають більш поширеними і шкідливими.

В українському суспільстві про реальну небезпеку, що можуть завдати кіберзлочини, почали говорити лише після вірусної атаки на мільйони серверів вірусу Петя.А (Petya.A) у 2017 р. Тому постало питання про ефективні методи боротьби з кіберзлочинністю.

Оскільки кіберзлочини спричиняються людьми, психологи не можуть залишатися осторонь. Можливість визначати мотивацію злочинців у кібернетичному просторі, зчитувати алгоритм і логіку протиправних дій суттєво допоможе кіберполіції в боротьбі з кіберзлочинністю.

Дослідженню питань протидії цьому виду злочинів присвятили свої роботи закордонні та вітчизняні науковці, зокрема: Ю. Батурин, В. Бутузов, В. Вєхов, Р. Калюжний, М. Карчевський, В. Козлов, Е. Рижков, Б. Романюк, І. Шинкаренко, В. Шеломенцев, Н. Шурухнов, G. Kirwan, A. Power, N. Nykodym, S. Ariss, K. Kurtz, J. Lickiewicz, P. Kwan, G. Stephens та інші.

Мета статті – проаналізувати наукову літературу щодо дослідження психологічного портрета кіберзлочинця та встановити наявні вітчизняні й закордонні методи профілювання злочинів у кіберпросторі.

Виклад основного матеріалу. Напевно, найбільш стрімко поширюється протиправна поведінка, пов'язана з розвитком Інтернету, що водночас створює нові види злочинів, як-от хакерство та розроблення шкідливих комп'ютерних програм. Цей новий тип злочинності найкраще вивчати і пояснювати через комбінацію теоретичних і емпіричних перспектив, зокрема й тих, що розроблені в кримінології, юридичній психології й інтернет-психології.

Термін «кіберзлочинність», хоча і здається досить зрозумілим, однак не має точного або універсального визначення. Все більше злочинців експлуатують швидкість, зручність і анонімність Інтернету для скоєння різноманітних правопорушень, які не мають кордонів, фізичних або віртуальних, завдають серйозної шкоди та створюють реальні загрози жертвам у всьому світі.

Найбільш широкого значення набуло поняття «кіберзлочинність» – сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору [1].

Тобто кіберзлочинність – це протиправні дії особи (чи групи осіб) у кібернетичному просторі. Через різноманітні сценарії та середовища даний вид злочинності варіює в різних юрисдикціях і значною мірою відрізняється залежно від сприйняття тих, кого це стосується. Інтернет-простір забезпечує кіберзлочинцям високий ступінь анонімності і дозволяє винуватцям кіберзлочинів здебільшого залишатися безкарними.

Проблема кіберзлочинності сьогодні хвилює суспільства різних держав. Крім особистої інформації в соціальних мережах, у кіберпросторі зберігається і різного роду державна інформація, оприлюднення якої може призвести до інформаційного колапсу у світі. Звичайно, багато що в кіберпросторі зашифроване та закодоване, однак на противагу «бар'єрам» кіберпростору виникли і їх порушники, яких ми звикли узагальнювати єдиним терміном «кіберзлочинець».

З огляду на специфіку кіберзлочину, кіберзлочинець визначається як висококваліфікований фахівець у галузі інформаційних технологій, який проникає в інформаційну систему з метою порушення її цілісності або використання інформації в корисливих неправомірних цілях [2].

У результаті аналізу наукової літератури встановлено сім основних типів кіберзлочинців, а саме:

1. Скрипткіді (англ. *scriptkiddies*) – особи, що користуються скриптами або програмами, розробленими іншими, для атаки комп'ютерних систем і мереж, не розуміючи механізму їхньої дії. Зазвичай здатні лише атакувати дуже слабко захищені мережеві системи.

2. Спамери (англ. *scammers*) – ті, хто за допомогою спаму (масової розсилки кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати) вчиняє шахрайство (поширення порнографії, комп'ютерних вірусів, виманювання коштів, виведення поштової системи з ладу (відмова сервісу) тощо).

3. Групи хакерів (англ. *hacker groups*) – зазвичай працюють анонімно і створюють інструменти для злому в кіберпросторі. Вони часто зламують комп'ютери без кримінальних мотивів, а іноді їх наймають компанії, щоб перевірити власну систему захисту.

4. Фішери (англ. *phishers*) – шахраї, що мають на меті виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів, карткових рахунків. Фішери використовують усілякі пастки, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані, наприклад, надсилають електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого цілком копіює дизайн відомих ресурсів.

5. Політичні/релігійні/комерційні групи кіберзлочинців. Вони зазвичай не зацікавлені у фінансовій вигоді, розробляють шкідливі програми для політичних цілей. Наприклад вірус Стакснет (англ. *Stuxnet*). Є припущення, що саме цей вірус – спеціалізована розробка ізраїльських спецслужб, спрямована проти ядерного проекту Ірану.

6. Інсайдери (англ. *insiders*). Вони можуть становити лише 20% загрози, але завдають збитків на цілих 80%. Такі кіберзлочинці вважаються найвищим ризиком у кіберпросторі. Що ще гірше, як випливає з назви, вони часто перебувають у межах організації, де працюють.

7. Прояви стійкої загрози (англ. *Advanced persistent threat* (APT)). Йдеться про цілеспрямовані напади, що проводяться надзвичайно організованими групами, члени яких мають доступ до великих обчислювальних ресурсів і володіють глибокими технічними знаннями [3].

Також є класифікація А. Кузнєцова, згідно з якою кіберзлочинців можна розділити на три категорії:

– до першої групи належать особи, відмінною рисою яких є стійке поєднання професіоналізму в області комп'ютерної техніки і програмування з елементами своєрідного фанатизму і винахідливості. Вони сприймають засоби комп'ютерної техніки як виклик своїм творчим і професійним знанням, умінням і навичкам;

– друга група складається з осіб, які страждають на новий різновид психічних захворювань – інформаційну, або комп'ютерну залежність;

– до третьої групи входять професійні «комп'ютерні» злочинці з яскраво вираженими корисливими мотивами [4].

Серед мотивів кіберзлочинів М. Кравцова називає корисливі, ігрові, політичні та хуліганські (нігілістичні, самоствердження, помста). Отже, серед морально-психологічних рис кіберзлочинців, на її думку, переважають корисливість, авантюризм, правовий і моральний нігілізм, поєднані з детермінованим специфікою кіберпростору комплексом сваволі й ілюзій [3].

Світові правоохоронці, враховуючи мотиви злочину та специфіку скоєння таких злочинних дій, загалом визначають два основних типи кіберзлочинів, пов'язаних з інтернетом:

– розширені комп'ютерні злочини (або високотехнологічну злочинність) – вишукані напади на комп'ютерне обладнання та програмне забезпечення;

– злочинність, пов'язану з кіберзахопленням, адже багато традиційних злочинів вчиняються за допомогою Інтернету, як-от злочини проти неповнолітніх, фінансові злочини, тероризм [5].

Активно кіберзлочинність розглядається в психологічних теоріях особистості. Так, у психоаналітичній теорії зазначено, що в кожної людини є внутрішня моральна система (Супер-Его), яка розвивається через задовільні відносини батьківської фігури.

У психоаналізі злочинна поведінка є продуктом неадекватного Супер-Его. Сьогодні ми знаємо, що деякі хакери виходять із неблагополучних сімей, іноді хакери не мають батьківської фігури,

тому ми навіть можемо говорити про те, що деякі хакери мають слабке Супер-Его. Проте відсутність Супер-Его означала б відсутність структури й імпульсивності, тоді як хакерство – це запланована діяльність, де жертви попередньо обираються, а напад є навмисним. Отже, під час психологічного профілювання хакера психоаналітична теорія корисна тільки для розуміння одного злочину, але не здатна пояснити кіберзлочинної поведінки загалом [7].

За теорією морального розвитку Л. Кольберга, моральний розвиток людини проходить кілька стадій, від доморальних (фундамент – заохочення та покарання) до високоморальних (слідування самостійно виробленим моральним принципам). Кримінальна поведінка виникає тоді, коли відбувається затримка в розвитку моральних міркувань; тому людина не може контролювати бажання скоїти злочин. Одним із принципів теорії Л. Кольберга є гедонізм, і багато хто із засуджених хакерів більше зважає на задоволення власної потреби, ніж на наслідки власних дій.

З іншого боку, Інтернет повний хакерських маніфестів, які ставлять загальні етичні проблеми як основу їхньої діяльності. Тому можемо припустити, що принаймні щодо «етичних хакерів» є абстрактна необхідність морального кодексу, який не тільки враховує соціальне самопочуття й особисті права (що він робить корисного для суспільства?), але й підкреслює демократичні процеси, які дають кожному можливість виділитися, і визначає принципи рівності [8].

Теорія оперантного навчання Б.Ф. Скіннера пояснює, що поведінка людини детермінована, передбачена і контролюється оточенням. Якщо наслідки бажані, поведінка буде активнішою, якщо наслідки є небажаними, поведінка зменшиться в частоті. Отже, поведінка діє на навколишнє середовище для отримання результатів, які посилюють або знижують її активність. Оперантне навчання було використано для пояснення загальної злочинності, а не для зосередження уваги на конкретних злочинах. К.Р. Роджерс (2001 р.) констатує, що теорія оперантного наачіання Б.Ф. Скіннера може пояснити поведінку хакерів, однак не пояснює того, що хакери, які були спіймані та покарані, все ще цікавляться хакерською діяльністю [9].

Теорія соціального навчання пов'язана з роботою А. Бандури та його дослідженнями з моделювання й імітації. Теорія соціального навчання базується на тому, що поведінку можна вивчати шляхом спостереження. Як тільки поведінка вивчається та стає зрозумілою, нею стає легше керувати. Згідно з теорією соціального навчання, злочинна поведінка набувається шляхом спостереження за навчанням. Навчання відбувається в трьох контекстах: у сім'ї, субкультурі та соціальному середовищі.

Теорію соціального навчання А. Бандури можна застосувати до поведінки хакерів. Хакери зазвичай асоціюються з іншими хакерами в інтернет-середовищі або приєднуються до хакерської спільноти, і так вони набувають злочинних навичок. Поведінку хакерів можна активувати завдяки взаємодії із суспільством, наприклад, через розвиток спільних знань, здобуття престижу всередині громади або просто нагородження за зламану надійну систему безпеки. А хакери, що ототожнюють свою поведінку з іншими хакерами, пов'язані із субкультурою, що підсилює їхню приналежність до вищого рівня кіберзлочинців [10].

Досить цікавими дослідженнями в області кіберзлочинності є вивчення кіберзлочинця через психологічний портрет жертви інтернет-злочину. Варто пам'ятати, що через те, що правопорушення стається в Інтернеті, ще не означає, що потерпілий не може усвідомити когнітивні, емоційні та фізіологічні наслідки.

Отже, визначивши психологічні профілі кіберзлочинців і профілі їхніх жертв, психологи можуть сприяти попередженню подальших схожих за специфікою злочинних дій у кіберпросторі. Саморегуляція жертв кіберзлочинів напряму залежить від їхнього усвідомлення кібернетичної безпеки (окрім дітей і психічно нездорових осіб).

Зрозуміло, що перевіряти або досліджувати психологічний портрет кіберзлочинця – надскладне завдання для психологічної науки, однак є декілька досліджень, які розглядалися як методи вивчення психологічних профілів злочинців і можуть бути корисними у справах про кіберзлочинність. Гудайтіс (1998 р.) висвітлює потребу в багатовимірному методі профілювання для оцінки кіберзлочинців, а Нікодіметал (2005 р.) вказує на те, що профілювання злочинця може бути корисним для розслідування кіберзлочинів, особливо там, де підозрюється правопорушник, що є інсайдером, тобто перебуває в межах однієї компанії, яка зазнала хакерського впливу. Роджерс (2003 р.) зазначає, що профілювання злочинця може бути корисним для різних методів кібернетичного розслідування, включаючи допомогу психологів слідчим у більш ефективному пошуку злочинців: звуження потенційних підозрюваних, виявлення мотиву та визначення якостей жертв, які приваблюють правопорушників [11].

2006 р. Роджерс дослідив психологічні особливості, моральний вибір і експлуататорську маніпулятивну поведінку авторизованих комп'ютерних злочинців та некомерційних злочинців. Сімдесят сім студентів, які навчалися на програмістів, брали участь у веб-дослідженні, результати якого показали, що єдиною важливою змінною для прогнозування кримінальної / девіантної поведінки досліджуваних студентів була екстраверсія. Ті особи, яким притаманний кримінальний профіль, були

значно більш інтровертованими, ніж ті, кому кримінальний профіль не був притаманний [13].

Під час розгляду злочинів у фізичному світі юридичний психолог (судовий експерт-психолог) використовує індуктивний чи дедуктивний профіль злочинців, щоб зробити усвідомлене припущення про особистість злочинця.

Індуктивні кримінальні профілі розробляються шляхом вивчення статистичних даних із використанням відомих поведінкових моделей та демографічних характеристик злочинців.

Дедуктивний метод профілювання (визначення психологічного портрета злочинця) використовує цілу низку даних, серед яких криміналістичні докази, докази на місці злочину, віктимологія, особливості правопорушників тощо. Використання таких методів здається можливим у фізичному світі. Проте в кіберпросторі їх застосування може бути сумнівним. Цим і пояснюється той факт, що спеціалісти та деякі вчені називають метод встановлення психологічного портрета кіберзлочинця «перспективною, але незрілою наукою», та чомусь приділяють мало уваги профілям кіберзлочинців (Bednarz, 2004 p.). На відміну від фізичного світу, для розроблення профілів кіберзлочинців може знадобитися не лише знання про психологію, кримінологію та право, а й розуміння технологічних аспектів, пов'язаних із «місцем злочинності», тобто кіберпростором.

Очевидно, що для вирішення такої проблеми треба застосовувати міждисциплінарний підхід

Висновки. Кіберзлочинність у сучасному світі є новітнім способом скоєння правопорушень і, як показує практика, досить популярним, оскільки система кіберпростору дозволяє таким злочинцям довгий час, а то і назавжди, залишатися безкарними.

Основною проблемою визначення психологічного портрета кіберзлочинця є перебування його протиправних дій у кібернетичному просторі та відсутність фізичних дій. Важливість проведення більш масштабних досліджень використання методу визначення психологічного портрета кіберзлочинця є очевидною, оскільки визначення особи (або окремих її індивідуально-психологічних характеристик) є єдиним засобом відстеження злочинця за відсутності фізичних доказів.

Література:

1. Кримінологія: Загальна та Особлива частини: підручник для студ. юридич. спец. вищ. навч. закл. / за ред. І. Даньшина. Нац. юридична академія ім. Ярослава Мудрого. Харків: Право, 2003. 352 с.
2. Пилипчук В., Дзьобань О. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети.* 2011. № 4(21). С. 12–17.
3. Кравцова М. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.08. Харків, 2016. 16 с.
4. Романюк Б., Гавловський В., Гуцалюк М., Бутузов В. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посібник / за заг. ред. Я. Кондратьєва. К.: Вид. А.В. Паливода, 2004. 144 с.
5. Александров А. Новая теория доказательств. *Уголовная юстиция: связь времен:* доклады и сообщения на конференции. URL: http://www.iuaj.net/node/406.
6. Shinder D. (2010) Profiling and categorizing cyber criminals. Retrieved on 6th July 2016. URL: http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069.
7. Kirwan G., Power A. (2013). Cybercrime: Psychology of cybercrime. Dublin: Dun Laoghaire Institute of Art, Design and Technology.
8. Nykodym N., Ariss S., Kurtz K. Computer addiction and cybercrime. Journal of Leader ship, Accountability and Ethics. 2008. № 35. P. 55–59.
9. Lickiewicz J. Cybercrime psychology-proposal of anoffender psychological profile. Problems of forensic sciences. 2011. № 2(3). P. 239–252.
10. Kwan L., Ray P., Stephens G. (2008). Towards a Methodology for Profiling Cyber Criminals. IEEE Computer Society. Proceedings of the 41st Hawaii International Conference on System Sciences.
11. Rogers M. A two-dimensional circum plex approach to the development of a hacker taxonomy. Digital Investigation. 2006. № 3 (2). P. 97–102.
12. Alison L., Goodwill A., Almond Louise, Heuvel C., Winter J. Pragmatic solutions to offender profiling and behavior investigative advice. Legal and criminological psychology. 2010. № 15. P. 115–132.
13. Tompsett E.C., Marshall A.M., Semmens C.N. (2005). Cyberprofiling: Offender Profiling and Geographic Profiling of Crime on the Internet. Computer Network Forensics Research Workshop.

Бабенко О. А., Мокляк А. С. Теоретический анализ исследования психологического портрета киберпреступников

В статье проанализированы понятия «киберпреступление» и «киберпреступник». Определены основные типы киберпреступников. С помощью социальных и психологических теорий личности проанализированы основные черты, присущие киберпреступникам. Определено значение метода установления психологического портрета киберпреступника для предупреждения и раскрытия киберпреступлений.

Ключевые слова: *киберпространство, киберпреступность, киберпреступник, хакер, психологический портрет, судебно-психологическая экспертиза.*

Babenko O. O., Mokliak A. S. Theoretical analysis of research of psychological portrait of cyber criminals

In the article concepts are analysed "cyber-crime" and "cyber criminals". The basic types of cyber criminals are certain. By means of social and psychological theories of personality, the basic personal touches are analysed, that inherent to cyber criminals. The role of method of establishment of psychological portrait of cyber criminals is determined in warning and opening of cyber criminals.

Key word: *cyberspace, cybercrime, cybercriminals, hacker, psychological portrait, judicial-psychological examination.*