Аналіз психологічних особливостей особистості, яка скоїла злочин у сфері використання комп'ютерних технологій, і визначення відповідних передумов

В.С. Савченко
здобувач,
Університет економіки та права «КРОК»

У статті досліджено психологію особистості комп'ютерного злочинця, тенденції до зміни її спрямованості, починаючи з 1980-х років, та її вплив на діяльність злочинних груп хакерів.

Ключові слова: *психологія особистості злочинця, профайлінг, розслідування злочину.*

В статье исследована психология личности компьютерного преступника, тенденции к изменению ее направленности, начиная с 1980-х годов, и ее влияние на деятельность преступных групп хакеров.

Ключевые слова: *психология личности преступника, профайлинг, расследование преступления.*

The research studies the psychology of computer criminal, tendency to change its direction, starting from the 1980s, and its influence on the activities of criminal groups of hackers.

Keywords: *offender psychology, profiling, the investigation of the crime.*

Постановка проблеми

XX ст., особливо останні його десятиріччя, позначилися стрімким науково-технічним прогресом, вінцем якого став прорив у світовому інформаційному просторі та водночас, як своєрідна плата за надбання людства, його масштабна криміналізація. Якісно нові злочини, що отримали назву кібернетичні, або комп'ютерні (від англомовних слів «computer crimes» і «Hi-tech crime»), викликали занепокоєння світової спільноти з огляду на їх зухвалість, організованість, технічну озброєність, широке використання найсучасніших досягнень науки й техніки, а головне – через неспроможність правоохоронних органів протистояти новоявленому феномену за допомогою правових та інших форм і методів діяльності, а так само неналежну психологічну підготовку. Відтак виникла нагальна потреба в напрацюванні нових знань та їх адаптації до потреб практики, що стало одним із пріоритетів сучасної науки, насамперед психології, що традиційно займається розробленням соціально-психологічних засобів, технологій, прийомів, методів, методик, рекомендацій, сприяючи в такий спосіб діяльності з розслідування чи попередження злочинів [1, с. 370].

Аналіз останніх досліджень і публікацій

Слід зауважити, що базові поняття проблематики теорії та практики розслідування злочинів у сфері використання комп'ютерних технологій досліджувалися ще в кінці 80-х – початку 90-х років XX ст., однак тільки зараз цей тип злочинів почав привертати серйозну увагу психологів, зокрема, Ю.М. Батуріна, П.Д. Біленчука, А.Б. Венгерова, М.В. Вєхова, Ю.В. Гавриліна, В.В. Голубєва, В.Г. Гончаренка, М.В. Карчевського, В.А. Колесника, В.В. Крилова, О.І. Мотляха, Л.П. Паламарчук, Д.В. Пашнєва, Є.Р. Росинської, М.Г. Щербаковського, М.П. Яблокова та інших. Слід зазначити, що переважна більшість учених, які займалися цією проблематикою, є за освітою юристами і не мають спеціальних знань, які допо-

могли б розглянути вказану проблематику з позиції розуміння психології особистості, яка скоїла злочин у сфері використання комп'ютерних технологій та психології її злочинної поведінки [1].

Не вирішені раніше частини загальної проблеми

Наслідки міжнародних злочинів та терактів у кіберпросторі початку XXI ст. змусили правоохоронців багатьох держав, у тому числі й України, звернути особливу увагу на проблему профайлінгу особистості кіберзлочинця. Останні події в українському сегменті всесвітньої мережі Інтернет демонструють неможливість відповідних органів вчасно реагувати на протиправну поведінку особи в Глобальній мережі без урахування психологічних знань про її особистість.

Формулювання цілей статті

Метою статті є висвітлення дослідження психологічних особливостей особистості, яка скоїла злочин у сфері використання комп'ютерних технологій.

Виклад основного матеріалу дослідження

Психологічні відомості про особу злочинця.

Відомо, що особа злочинця досліджується різними науками. Кримінологічні дослідження обмежуються в основному тими особливостями людини, які необхідні для використання з метою кримінальної профілактики, попередження злочинів. Психологічний профайлінг за допомогою психологічних методів, методик оцінки і прогнозування вивчає поведінку злочинця. Окрім того юридична психологія також вивчає «професійні» звички злочинців, які проявляються в першу чергу в певних способах і прийомах вчинення злочину, у характерному почерку злочинця тощо. Виявлення на місці скоєння злочину речових доказів дає змогу визначити деякі особисті соціально-психологічні ознаки злочинця, його досвід, професію, соціальні знання, стать, вік, особливості взаємодії та взаємовідносин із потерпілими тощо.

Характеризуючи психологічні особливості особи, яка скоїла злочин у сфері використання комп'ютерних технологій, необхідно відмітити основну ознаку, а саме: у цю злочинну діяльність втягнуто широке коло осіб від дилетантів до професіоналів. Правопорушники мають різний соціальний статус, різний рівень освіти, навчання та виховання.

З дослідницької точки зору цікавим є той факт, що з кожної тисячі комп'ютерних злочинів, лише сім вчинені професійними програмістами. В окремих випадках особи вчиняли такі протиправні дії, взагалі не маючи технічного досвіду. Кевін Митник − знакова фігура в цьому вимірі. На його погляд, у будь-якій розмові можна підпорядкувати собі співрозмовника, якщо говорити авторитетним тоном знавця, навіть якщо в цій галузі ти нічого не тямиш. Час від часу він телефонував у відділ дистанційного зв'язку якої-небудь компанії і незадоволеним начальницьким голосом вимагав пояснити, чому той чи інший номер АТС не вдається набрати з міста. Наляканий оператор пояснював йому, як набрати номер, що цікавив Кевіна. Він вів спеціальну записну книжку, куди вписував імена та посади телефоністок і операторів різних фірм та їхніх начальників. Там же він позначав, новачки вони чи досвідчені робітники, наскільки добре поінформовані, мають схильність до розмов чи ні. Заносив у книжку й відомості, так би мовити, особистого характеру, здобуті протягом довгих годин розмов по телефону: їхні захоплення, імена дітей, улюблені види спорту і місця, де вони полюбляють бувати у відпустці чи на вихідні. Саме ці дрібні деталі, а також гнучкість пізнання особистості майбутньої жертви дали змогу Кевіну Митнику майже завжди отримувати своє. Тим не менш, згаданими прийомами користувалися не тільки хакери-чоловіки, а й представниці слабкої статі, тому досить цікавим є питання статевої приналежності особи злочинця. Частка участі чоловіків і жінок у комп'ютерних злочинах наближено має відповідну пропорцію з деяким відсотком переважання в бік сильної статі. Однак за критерієм злочинності та агресивності

у своїх діях значну перевагу отримують чоловіки. Жіноча злочинність більш продумана, чіткіше спланована, складніша у сприйнятті та розслідуванні. Доказом цього твердження є відома хакер Сюзен Сандер, яка на початку своєї кар'єри ще не мала достатньо досвіду і знань, щоб упоратися з комп'ютерами та мережами зв'язку Міністерства оборони США. І брак чисто технічних знань вона доповнила іншими навичками. Наприклад, стала їздити до військових баз і гуляти там біля офіцерських клубів, щоб звернути на себе увагу. Таким чином Сюзен знайомилася зі старшими офіцерами, спокушала їх і навідувалася до їхніх помешкань. Коли вони спали, жінка викрадала необхідні комп'ютерні паролі і коди доступу [1, с. 6].

У науковій літературі пропонуються різні класифікації комп'ютерних злочинців. Так, наприклад, О.І. Мотлях розмежовує дві категорії суб'єктів, які мають відношення до протиправних дій цього напряму: невиявлені (або невідомі) та виявлені (або відомі) [2, с. 65].

Свою увагу В.Б. Вехов зосередив на таких категоріях психологічних особливостей комп'ютерних злочинців: особи, які вирізняються з-поміж інших злочинців стійким поєднанням професіоналізму в галузі комп'ютерної техніки та програмування з елементами своєрідного фанатизму й винахідливості; особи, що страждають новим видом психічних захворювань – інформаційними хворобами чи комп'ютерними фобіями; професійні комп'ютерні злочинці з яскраво вираженими корисливими цілями [3, с. 31-40].

Зупинимося більш детально на вказаних вище категоріях психологічних особливостей, використовуючи фактичний матеріал з кримінального минулого деяких «визнаних» злочинців.

До першої категорії можна віднести відомого хакера Роберта Таппана Морріса. Він є сином відомого математика Боба Морріса, який у свій час був штатним співробітником агентства криптологічної розвідки Сполучених Штатів Америки, що є частиною Міністерства оборони США і відповідає за збір та аналіз іноземної розвідувальної інформації та за захист інформаційних систем і комп'ютерних мереж уряду США. Мати бачила, що Роберт відчуває, що відрізняється від однолітків. Він розумів, що він інший, але не знав, чому. Одного разу він зізнався матері, що думає, що він «дивний». Мати пробувала з'ясувати, чи здогадується він, що його «ненормальність» полягає в його розумових здібностях. Однак навіть коли всім стало ясно, що Роберт розумніший за своїх однокласників, самого хлопця ця різниця тільки бентежила, а іноді дратувала. Стороннім могло навіть здатися, що Боб заохочує його займатися хакінгом. У 1982 р. Джина Колат, журналістка з Science, що працювала над статтею про комп'ютерну злочинність для журналу Smitsonian, брала у Боба Морріса інтерв'ю. Він упевнено заявив їй, що, швидко переглянувши вміст її сумки, знатиме про неї достатньо, щоб відгадати її комп'ютерний пароль. Після того, як написаний ним вірус rtm пошкодив більшість комп'ютерів Східного узбережжя США, Роберт представ перед судом. Під час останньої промови він заявив, що просто успадкував від батька любов до ігор чистого інтелекту.

До другої категорії належить один із найвідоміших комп'ютерних злочинців ФРН Карл Кох, більш відомий у світі хакерів як «Хагбард Сілайн». Сім'я Карла, як виявилося, розпалася дуже давно. Його батько залишив їх із сестрою на піклування матері, коли вони були ще маленькими. Мати захворіла на рак і померла на очах у Карла. Його батько, відомий ганноверський журналіст (і гіркий п'яниця), також помер від раку, Карлу тоді вже виповнилося шістнадцять. Спадщина становила 100 тис. марок, або близько 50 тис. доларів, що дало йому змогу купити відремонтований «Порше», зняти хорошу квартиру в Ганновері і почати вживати дорогий дурман. Студентом Карл приєднався до антиядерного руху і був навіть активістом (як і багато інших), однак зрештою залишив політику. У вільний від роботи час, здебільшого ночами сидів перед комп'ютером у кого-небудь на квартирі, гашиш забезпечував натхнення, а кокаїн з амфетаміном під-

тримував у фізичній кондиції. Зрештою, гроші зі спадщини швидко зникли і залишився тільки шлях криміналу, який Карл і обрав. І хоча Хагбард не був програмістом і, отже, повністю залежав від решти членів злочинної групи, які повинні були писати для нього програми, нескінченне терпіння і зацикленість на предметі занять робили його більш ефективним зломщиком, ніж багато інших. Після кількох сенсаційних прес-конференцій, на яких він у режимі реального часу проникав на комп'ютери держустанов США та ФРН, ним зацікавився Інтерпол. Тіло Карла Коха знайшли за містом, воно було опалене. За результатами слідство встановило, що це було самогубство.

Як приклад третьої категорії, якнайкраще підходить Ханс «Пенго» Хайнріх з тоді ще Західного Берліна. Вважаючи себе «технологічним партизаном» та маючи певні ліві політичні уявлення, він тим не менш за винагороду активно співпрацював з Представництвом КДБ СРСР при МДБ НДР. Передавши велику кількість цінного програмного забезпечення, Ханс майже встиг надати код найсучаснішої на той час операційної системи. На суді він вибудував лінію захисту на тому, що справжню загрозу становить не Радянський Союз, а промислове шпигунство, і шпигуни як американських, так і європейських корпорацій потихеньку зламують комп'ютери конкурентів у пошуках засекречених технологій і комерційної інформації.

У юридичній літературі дослідники визначають таких осіб, як порушники правил користування електронно-обчислювальними машинами; «білі комірці»; «комп'ютерні шпигуни»; «хакери», або «одержимі програмісти» [4, с. 168].

Класичною вважається класифікація В.Б. Вехова, основну ідею якої він запозичив у Ю.В. Гавриліна. Під категорією злочинних елементів цього напряму останній розуміє:

1. Осіб, які перебувають у трудових відносинах з підприємством, організацією, закладом, фірмою або компанією, де скоєний злочин (за цими даними, вони становлять більше 55 %), а саме: а) які безпосередньо займаються обслуговуванням ЕОМ (оператори, програмісти, інженери, персонал, що здійснює технічне обслуговування і ремонт комп'ютерних систем або обслуговуючий персонал комп'ютерної мережі); б) користувачі ЕОМ, що мають визначену підготовку та вільний доступ до комп'ютерної мережі; в) адміністративно-управляючий персонал (керівники, бухгалтери, економісти).

2. Громадян, які не перебувають у правовідносинах з підприємством, організацією, закладом, фірмою чи компанією, де скоєно злочин (близько 45%). Ними можуть бути: а) особи, що займаються перевіркою фінансово-господарської діяльності підприємства та ін.; б) користувачі та обслуговуючий персонал ЕОМ інших підприємств, що пов'язані з комп'ютерними мережами підприємства, на якому скоєно злочин; в) особи, які мають у своєму користуванні комп'ютерну техніку (у тому числі власники персональних ЕОМ, що отримали доступ до телекомунікаційних комп'ютерних мереж) [5, с. 38].

Подана класифікація не є вичерпною. Її можна доповнювати, видозмінювати та розширювати. Так, наприклад, коло осіб, що скоюють комп'ютерний злочин (той же Ю.В. Гаврилін) більш характеризує не як загальну класифікацію суб'єктів, а як категорії осіб, які мають доступ до засобів комп'ютерної техніки. Тобто, у полі зору перебувають внутрішні користувачі програмного забезпечення і обслуговуючий його персонал та зовнішні користувачі, які мають причетність до операційної комп'ютерної системи. При цьому не розглядається інша категорія осіб, що здійснює несанкціонований протиправний доступ до ЕОМ, АС мереж чи мереж зв'язку. Ті ж самі програмісти-любителі, професіонали-хакери і їх різновиди, хворі та психічно неврівноважені особи тощо. Хоча певною мірою можна погодитися з автором, на частку саме внутрішніх злочинців, як свідчить статистика США, припадає близько 80% усіх злочинів [6, с. 4].

Подібну, але дещо розширену класифікацію психології комп'ютерних злочинців за метою та сферою злочинної діяльності,

враховуючи наведені вище тенденції, дають у своїй роботі М.Г. Щербаковський і Д.В. Пашнєв. Так, групу зовнішніх суб'єктів вони поділяють на окремі підгрупи таким чином:

За психологією мети та сферою злочинної діяльності комп'ютерних злочинців зазвичай поділяють на окремі підгрупи:

1) хакери – отримують задоволення від вторгнення до великих комп'ютерних систем за допомогою телекомунікаційних технологій, зокрема комп'ютерних мереж. Це комп'ютерні хулігани, електронні «корсари», які без дозволу проникають у чужі інформаційні мережі задля розваги. Їх приваблює подолання труднощів: чим складніша система, тим привабливіша вона для хакера. Хакери – прекрасні знавці інформаційної техніки. За допомогою телекомунікаційного обладнання й домашніх комп'ютерів вони підключаються до мереж, які пов'язані з державними та банківськими установами, науково-дослідними та університетськими центрами, військовими об'єктами, отримують права доступу до них та до їхньої інформації. Хакери, як правило, не завдають шкоди системі та даним, отримуючи задоволення тільки від відчуття своєї влади над комп'ютерною системою;

2) крекери – це більш серйозні порушники, здатні завдати будь-якої шкоди будь-якій комп'ютерній системі та програмі. На першому плані в них стоїть корислива мета, пов'язана з цінною комп'ютерною інформацією, заради якої й отримають доступ до будь-якого її виду. Це може бути програма, захищена авторським правом, інформація з обмеженим доступом, база даних або навіть загальнодоступна, але цінна для господаря інформація, що зберігається на домашньому комп'ютері. Вони викрадають, змінюють, перекручують та знищують комп'ютерну інформацію або навіть більше – вони залишають її на носії, але закривають до неї доступ. Усе це заради отримання винагороди за отриману інформацію або ж за її знищення чи заради вимагання викупу за коди доступу до інформації або за те, щоб вони залишили комп'ютерну систему у спокої. З технічного боку це набагато складніше від того, що роблять хакери. Отриману інформацію крекери потім продають іншим особам; досить часто контактують з організованою злочинністю. Популярним товаром є кредитна інформація, інформаційні бази правоохоронних органів та інших державних установ;

3) фріки – спеціалізуються на використанні телефонних систем з метою уникнення від оплати телекомунікаційних послуг. Вони теж отримують задоволення від подолання труднощів технічного плану. У своїй діяльності фріки використовують спеціальне обладнання, яке генерує спеціальні тони виклику для телефонних мереж. На сьогодні фріки орієнтуються переважно на отримання кодів доступу, крадіжки телефонних карток і номерів доступу з метою віднести платню за телефонні розмови та послуги Інтернет на рахунок іншого абонента. Досить часто вони займаються прослуховуванням телефонних розмов;

4) кібершахраї – це злочинці, які спеціалізуються на розрахунках. Вони використовують комп'ютери для заволодіння коштами та іншими цінностями шляхом використання номерів рахунків, кредитних карток та іншої інформації;

5) пірати – спеціалізуються на збиранні та торгівлі неліцензійним програмним забезпеченням. На сьогодні це велика група злочинців.

Внутрішні ж суб'єкти, виходячи з будови комп'ютерної системи та психології спрямованості на об'єкти злочинної дії, характеризуються дослідниками так:

1) оператори − використовуючи алгоритми, можуть активно впливати на ЕОМ із метою розкрадання грошових сум, товарів і послуг;

2) програмісти – мають можливість діяти у двох напрямах: по-перше, впроваджуючи в програмне забезпечення активно діючі компоненти (наприклад, команди), вони можуть учиняти розкрадання матеріальних цінностей, фінансів, послуг; по-друге, можуть уводити в програми неактуалізовані шкідливі компоненти і відповідно здійснювати шантаж адміністрації;

3) експлуатаційники (інженери та техні-

ки) – мають можливість несанкціонованого входу в комп'ютерну мережу з метою декодування інформації, її вилучення з подальшою реалізацією, несанкціонованого використання машинного часу [7, с. 31-33].

Наприкінці необхідно зазначити, що суттєву роль у структурі психологічної характеристики злочинів у сфері використання комп'ютерних технологій відіграють узагальнюючі відомості про потерпілих від злочинів. Подібна інформація дає змогу більш детально охарактеризувати особу злочинця, мотиви вчинення злочину і відповідно допомагає точніше окреслити коло осіб, серед яких потрібно шукати злочинця. Саме вивчення психологічних особливостей потерпілої сторони, її поведінки, дає можливість глибше розібратися в багатьох обставинах злочину, особливо тих, які вказують на своєрідність спрямування та мотиви поведінки злочинця, його загальні та індивідуальні риси. Між злочинцем і потерпілою стороною досить часто відслідковується певний психологічний зв'язок. Особливо це актуально щодо злочинів у сфері використання комп'ютерних технологій.

До факторів, які психологічно характеризують потерпілу сторону – юридичну особу або будь-яке інше утворення, необхідно підходити до кожної жертви вибірково. Однак усе ж найбільш загальними характеристиками є: вид діяльності; кадрове та матеріально-технічне забезпечення; фінансовий стан; досвід роботи працівників, у тому числі й досвід роботи з комп'ютерною технікою; система обліку і звітності; вид обчислювальної техніки, зв'язку та комунікацій, їхні технічні характеристики; наявність служби безпеки щодо захисту комп'ютерів та оперативного психолога в ній тощо [8, с. 50-52].

Потерпілих від злочинів у сфері використання комп'ютерних технологій також можна класифікувати за особливостями діяльності. Найчастіше їх умовно поділяють на три групи: власники комп'ютерних систем; клієнти, що користуються їхніми послугами; інші особи [9]. При цьому слід ураховувати, що перша група осіб часто не повідомляє правоохоронні органи про факт скоєння злочину, тому подібні останні й мають високий рівень латентності порівняно з іншими видами злочинів, що у свою чергу суттєво ускладнює процес їх розкриття та профілактики.

Висновки

У дослідженні зроблено спробу простежити шляхи розвитку комп'ютерного андеграунду і відтворити, ґрунтуючись на реальних фактах, психологію сучасного кіберзлочинця. Вона, частіше за все, визначається як химерна суміш найсучасніших технічних знань та моралі ізгоя. Як правило, у засобах масової інформації, особливо соціальних мережах, розповідається про талановитих комп'ютерників-бунтарів, що відмовляються коритися встановленим порядкам, причому події зазвичай розгортаються на тлі якогось нечіткого майбутнього, у світі, де панують високі технології, а гігантські міста перенаселені і занепадають. У такому світі все вирішує безмежна міць комп'ютерів. На думку ж професіоналів, величезні комп'ютерні мережі утворюють новий всесвіт, на просторах якого мешкають електронні особистості, які майже завжди не аутентичні собі в реальному житті. Лабіринтами цих мереж нишпорять перехоплювачі інформації. Багато з них живуть тим, що скуповують, перепродують або просто крадуть інформацію − валюту електронного майбутнього.

Психологічні передумови протиправної поведінки у сфері використання комп'ютерних технологій постають перед нами в риторичному запитанні: «А як же насправді – чи дійсно таку серйозну загрозу становлять юнаки та дівчата, що нелегально підключаються до чужих комп'ютерів?» Соціальне напруження та економічні кризи завжди штовхали людей у прірву криміналу, але не слід забувати, що одержимі комп'ютерами та комп'ютерними мережами особи стають хакерами, коли їхня одержимість вже почала переходити межі того, що комп'ютерники-професіонали вважають допустимим з точки зору моралі, а юристи − з точки зору закону.

Дослідженнями встановлено, що злочини у сфері використання комп'ютерних технологій являють собою одне з найскладніших антисоціальних явищ у суспільстві. Грамотне розслідування злочинів, зокрема визначення психологічного портрета особи злочинця – одне з ключових питань для будь-якого правоохоронного органу держави, у тому числі й для України. Міжнародний характер протидії цьому феномену сучасності – запорука подальшої стабільності та розвитку всіх сфер людського буття.

Література

1. *Марков Д.* Хакеры / Д. Марков, К. Хэфнер. – К. : Полиграфкнига, 1996. − 92 с.
2. *Мотлях О. І.* Методика розслідування комп'ютерних злочинів : Монографія / О. І. Мотлях. − К. : Освіта України, 2010. – 236 с.
3. *Вехов В. Б.* Компьютерные преступления : Способы совершения и раскрытия / В. Б. Вехов / Под ред. акад. Б. П. Смагоринского. − М. : Право и Закон, 1996. – 182 с.
4. *Зинченко К. Е.* Компьютерные технологии в юридической деятельности: учеб. и практ. пособие / К. Е. Зинченко, Л. Ю. Исмаилова, К. Е. Караханьян, Б. В. Киселев. − М. : БЕК, 1994. – 303 с.
5. *Гаврилин Ю. В*. Рассследование неправомерного доступа к компьютерной информации. Учеб. пособие / Ю. В. Гаврилин. –М. : Книжный мир, 2001. – 88 с.
6. Компьютерная преступность в США // Проблемы преступности в капиталистических странах. – 1990. – № 9. – С. 3-5.
7. *Щербаковський М. Г.* Розслідування комп'ютерних злочинів : посібник / М. Г. Щербаковський, Д. В. Пашнєв. – Харків : ХНУВС, 2010. – 112 с.
8. *Паламарчук Л. П.* Розслідування злочинів у сфері використання комп'ютерних технологій : Монографія / Л. П. Паламарчук. – К. : Експрес-Поліграф, 2007. – 144 с.
9. Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65. – С. 107.