Біленчук Петро Дмитрович,
професор кафедри кримінального права
і процесу Національного авіаційного
університету, кандидат юридичних наук,
доцент;
Малій Микола Іванович,
директор правничої компанії

КРИМІНОЛОГО-КРИМІНАЛІСТИЧНИЙ ПОРТРЕТ ЕЛЕКТРОННОГО ЗЛОВМИСНИКА

Проведений нами майже тридцятилітній соціально-правовий, психолого-кримінологічний та експертно-криміналістичний консолідований аналіз наукових досліджень та слідчої і судової практики (1991–2020 рр.) дозволяє зробити висновок, що серед електронних зловмисників[1] більшість становлять чоловіки [2]. Водночас останнім часом слідча і судова практика свідчить, що в цій структурі різко зросла частка жінок електронних зловмисників. Системний аналіз показує, що з позиції людських психофізіологічних характеристик – це яскрава, думаюча, творча особистість, професіонал своєї справи, готовий прийняти технологічний виклик, бажаний працівник. Як правило електронні зловмисники часто займають відповідальні керівні посади в установах та організаціях і озброєні спеціальними професійними знаннями, а також найновішими інноваційними грід-технологіями. Ці зловмисники мають доступ до комп'ютерних систем, мереж і електронних баз даних завдяки своєму службовому становищу. Одночасно – це людина, яка боїться втратити свій авторитет або ж певний професійний статус в рамках якоїсь соціальної групи, або ж боїться на роботі глузувань. Слідча і судова практика свідчить, що левова частка електронних злочинів здійснюється поодинці, самостійно. Водночас сьогодні має місце тенденція співучасті електронних зловмисників в групових (організованих) злочинних посяганнях. Доцільно звернути увагу і на те, що зовні поведінка таких людей особливо не відрізняється від установлених в суспільстві соціальних та правових норм. До того ж електронні зловмисники відзначаються високим професіоналізмом, уважністю і пильністю, а їх дії достатньо витончені, хитромудрі, супроводжуються відмінним маскуванням [3, с. 16; 6, с. 14–15].

Слід зазначити, що особливу групу електронних піратів становлять хакери і крекери[2]. Розглянемо їх особливі риси детальніше. Відомо, що дослівно «хакер» – це людина, яка проникає в чужі інформаційні мережі,

[1] Вважаємо, що доцільно використовувати термін «електронний зловмисник», оскільки термін «електронний злочинець» можна використовувати щодо конкретної особи лише після визнання особи винною за рішенням суду.

[2] Крекер – потужний викрадач чужої інформації (жарг. – злодій, взламувач).

комп'ютери, системи, електронні бази даних без злочинної мотивації. Хакери – це електронні корсари, комп'ютерні пірати, – так називають людей, які без дозволу господаря проникають в чужі інформаційні електронні мережі для забави, іноді з метою показу свого інтелектуального іміджу, зверхності, реваншу над іншими технократами. Слід зазначити, що хакери – це електронні хулігани, які отримують емоційне і психофізіологічне задоволення від непримітного вторгнення в чужий комп'ютер, інформаційну мережу, комп'ютерну систему, електронні бази даних. Очевидно, що хакери прекрасні телекомунікаційні професіонали – чудові знавці сучасної інформаційної та електронної техніки. Відомо, що за допомогою телефону (смартфону) і домашніх комп'ютерів вони підключаються до «всесвітньої павутини», електронних мереж, що передають дані, пов'язані майже з усіма великими електронними мережами і комп'ютерами світу, які діють в сфері економіки, фінансів, науково-дослідних центрів, банків, страхових компаній тощо [5, с.7].

Так, наприклад, американський хакер Річард Чешир, якого запросили в Мюнхен на нараду експертів з охорони відомостей в комп'ютерах практично на очах фахівців з кібербезпеки забезпечив собі доступ спочатку в німецьку мережу, потім просто завітав в американську інформаційну мережу, а звідти проник в один із найважливіших і найпотужніших стратегічних комп'ютерів США [3, с. 16].

Особливим різновидом хакерів є крекери. Фактично ці надзвичайно потужні електронні зловмисники крадуть найважливішу електронну інформацію, викачуючи за допомогою комп'ютера та електронних мереж цілі закриті для звичайних користувачів інформаційні банки даних. Зрозуміло, що технічно це набагато складніше здійснити ніж те, що роблять звичайні хакери.

Практика показала, що за декілька годин, не докладаючи особливих зусиль, будь-який технік середньої руки може пограбувати недоступний електронний банк даних французького комісаріату з атомної енергії і отримати найконфіденційніші засекречені відомості, або, наприклад, таємний проект створення лазера чи програму будівництва ядерного реактора [1, с.30].

Слідча і судова практика свідчить, що серед електронних зловмисників є представники усіх груп традиційної кримінально-правової класифікації та кваліфікації: білокомірцевого, організованого і загальнокримінального злочинного світу. Причому вони працюють як в самих організаціях та установах, проти яких скоюють злочинні діяння, так і поза їх межами, поодинці і в групі потужних технічно озброєних співучасників. Одні технічно оснащені слабо, а інші мають дорогі, престижні науковомісткі могутні комп'ютерні системи,а також стаціонарні та пересувні портативні пристрої [3, с.16–17].

Важливо звернути увагу, що провідне місце сьогодні де професійно працюють крекери посідає організована електронна злочинність [7, с. 144–147]. Це обумовлено тим, що, по-перше, діяльність

мафіозних структур є часткою великомасштабного електронного злочинного бізнесу. По-друге, із організацій, що використовують комп'ютери та електронні мережі, значно простіше і зручніше «витягувати» гроші, ресурси, інформацію та потужні бази даних. Електронні зловмисники скоюють це за допомогою звичайних смартфонів, мобільних телефонів, комп'ютерів та різного роду електронних пристроїв та новітніх технологій. Нарешті, по-третє, оскільки сили кібербезпеки і кіберполіції також використовують комп'ютерні системи, електронні мережі, смартфони для боротьби із електронною злочинністю, то, відповідно, щоб попередити стеження і розгадати плани противника, організована електронна злочинність використовує таку могутню зброю, як сучасний мобільний телефон, смартфон чи комп'ютер [4, с. 138].

Підводячи підсумки можна стверджувати наступне:електронні зловмисники – це особи, які як правило, являються фахівцями-професіоналами своєї сфери, відмінно знають сучасну електронну обчислювальну техніку, віртуозно володіють програмуванням. Їхні дії достатньо сплановані, витончені і розумно опрацьовані.

Список використаних джерел

1. Батурин Ю.М. Право и политика в компьютерном круге. М.: Наука, 1987. 111 с.
2. Біленчук П.Д., Малій М.І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів*:матеріали Міжнародної науково-практичної конференції (м. Київ, 30 жовтня 2020 року).К.: Державний науково-дослідний інститут МВС України2020. С.10.
3. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навчальний посібник.Київ: Українська академія внутрішніх справ, 1994.72с.
4. Біленчук П.Д. Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: навчальний посібник. Київ: Атіка, 2002. 240с.
5. Біленчук П.Д., Береський Я.О., Кобилянський О.Л., Малій М.І., Перелигіна Р.В. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: монографія; за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2019.416 с.
6. Біленчук П.Д., Малій М.І. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Юридичний Вісник України*. 2019. № 40. С. 14–15.
7. Біленчук П.Д., Перелигіна Р.В., Малій М.І. Кримінологічна характеристика особи комп'ютерного злочинця. *Кримінологічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення*: матеріали міжвузів. наук.-практ. Круглого столу (Київ, 22 березня 2019 р.) [редкол. В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ: Нац. акад. внутр. справ, 2019. С.144–147.