Б. М. Орловський
д. ю. н., доц., доц. кафедри кримінального права,
кримінального процесу та криміналістики,
Одеський національний університет імені І. І. Мечникова

ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ У КРИМІНОЛОГІЧНІЙ НАУЦІ

Кіберзлочинність є одним із найскладніших різновидів злочинності в кримінології, що має високу латентність та складний механізм скоєння злочинних діянь. Виникнення та розвиток кіберзлочинності обумовлюється рядом причин, умов і факторів, що у сучасній кримінологічній науці називаються детермінантами кіберзлочинності. Варто розуміти, що з точки зору транснаціональності кіберзлочини займають третє місце у світовій злочинності, одразу після продажу зброї та продажу наркотичних засобів. Щорічно вони заподіюють значні за розміром збитки підприємствам, громадянам, державам за рахунок розкрадань і шахрайських дій, що вчиняються з використанням комп'ютерних технологій. Тому встановлення переліку детермінант кіберзлочинності має важливе значення для зупинення розвитку кіберзлочинності і мінімізації її наслідків у життєдіяльності суспільства.

Детермінанти кіберзлочинності – це комплекс взаємопов'язаних між собою факторів, причин та умов, які сприяють розвитку та поширенню кіберзлочинів у суспільстві, стимулюючи виникнення кіберзлочинних форм поведінки, що пов'язані із використанням комп'ютерних технологій та мережі Інтернет.

Детермінанти кіберзлочинності можна об'єднати у однотипні групи за певними сферами їх виникнення та розвитку і саме такий підхід використовується у сучасній кримінології. Детермінанти кіберзлочинності в Україні можна поділити на:

1) технологічні (технічні), які пов'язані із можливостями використання недоліків сучасних інформаційних технологій, без яких неможливо було б скоювати кіберправопорушення. Це: а) пряма залежність бізнесу та населення від інформаційних технологій, необхідність підприємств, установ, організацій мати

власні інтернет-сайти, без яких неможливо вести господарську діяльність; б) проведення фінансових розрахунків у інтернет-мережах через електронні гаманці та віртуальні рахунки, у зв'язку з чим виникає можливість викрадення паролів, пін-кодів власників гаманців (рахунків) тощо; в) неможливість встановити територію скоєння кіберзлочину або кібервтручання; г) низький рівень кібернетичної культури користувачів, невміння безпечно проводити операції з картками та гаманцями в мережі Інтернет; д) поширення персональних даних у соціальних мережах, які дозволяють ідентифікувати особу, розшифрувати її паролі та отримати конфіденційну інформацію, необхідну для зламу гаманця; е) використання застарілого та неліцензійного програмного забезпечення у комп'ютерних системах, що зменшує рівень їх захисту; є) розвиток криптовалюти як анонімного засобу платежу, який дозволяє переводити реальні грошові кошти, викрадені з рахунків чи гаманців користувачів у електронну валюту, яка не має жодного контролю за обігом і не підлягає ідентифікації; ж) використання публічних Wi-Fi мереж та хмарних технологій із вразливими умовами підключення, що дозволяють перехоплювати та викрадати персональні дані користувачів під час їх надходження до технічних засобів з'єднання (маршрутизаторів тощо); з) високий рівень технічної кваліфікації кіберзлочинців, який передбачає вміння скористатися незначними прогалинами у системі захисту мережі або гаманця [1, с. 120];

2) економічні: а) висока прибутковість кіберзлочинності, що може приносити мільйонні прибутки; б) економічна криза та зростання безробіття у суспільстві, що породжує пошук альтернативних «безпечних» способів заробітку; в) відставання країни у економічному рівні життя, що призводить до зубожіння населення; г) розвиток «тіньової» економіки, яка породжує тіньові незахищені операції, відтік технічних кадрів із легального сектору економіки до тіньових структур, що беруть участь у кіберзлочинності [3, с. 83];

3) соціальні: а) перехід суспільної активності у віртуальні соціальні мережі (Інстаграм, Фейсбук, Телеграм), де користувачі зберігають свої персональні дані; б) пріоритетність мобільних

телефонів у житті, використання їх у незахищених операціях; в) глобальна участь всього населення в Інтернет-мережах, що дозволяє кіберзлочинцям залишатися непомітними серед мільярдів користувачів мережі; г) наявність соціальних груп (пенсіонерів, інвалідів), які мають високу кібервіктимність через технічну неграмотність;

4) правові: а) складність документування та доведення кіберзлочину, проблеми збирання доказів; б) необхідність постійних змін в розділі XVI КК України, виникнення нових форм кіберправопорушень; в) недостатня технічна оснащеність та недостатня кваліфікація працівників правоохоронних органів;

5) психологічні та ідеологічні: а) почуття «необмеженої» свободи у кіберзлочинця; б) відсутність «візуального» контакту із жертвою, нерозуміння тяжкості наслідків; в) розвиток субкультури «хакерів» та «хактивістів» тощо [2, с. 247].

Висновки. Отже, за результатами проведеного кримінологічного дослідження, були виділені та розкриті основні групи детермінант кіберзлочинності, серед яких превуалюють технологічні (технічні), які вказують на найбільш типові незахищенності комп'ютерних систем та мереж. Розуміння такої системи детермінант кіберзлочинності на сучасному етапі є важливим для розробки та формування ефективних засобів її протидії.

Література

1. Боженко В. В., Кушнерьов О. С., Кільдей А. Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум*. 2021. № 4. С. 116– 121.
2. Бондаренко О. С., Рєпін Д. А. Кіберзлочинність в Україні : причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246– 248.
3. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах. *Журнал східноєвропейського права*. 2016. №. 31. С. 80– 86.