УДК 343.9.01
DOI https://doi.org/10.32782/2524-0374/2025-3/87

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ОСОБИ ЗЛОЧИНЦЯ, ЩО ВЧИНЯЄ КРИМІНАЛЬНЕ ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНЕ СТ. 361 ККУ

CRIMINOLOGICAL CHARACTERISTICS OF AN OFFENDER COMMITTING A CRIMINAL OFFENSE UNDER ARTICLE 361 OF THE CRIMINAL CODE OF UKRAINE

Стручаєв М.Ф., аспірант кафедри кримінально-правової політики
Національний юридичний університет імені Ярослава Мудрого

У статті досліджується кримінологічна характеристика особи злочинця, який вчиняє кримінальне правопорушення, передбачене ст. 361 КК України – несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж.

На основі аналізу статистичних даних, наукових праць і судової практики визначено соціально-демографічні, психологічні та кримінологічні характеристики осіб, що вчиняють даний злочин. Досліджено статево-вікову диференціацію правопорушників, їхній освітній рівень, сімейний стан, соціальний статус, рівень зайнятості, а також індивідуально-психологічні риси. Окрему увагу приділено мотиваційним чинникам, які можуть спонукати злочинців до вчинення правопорушення.

Встановлено, що переважна більшість осіб, які вчиняють дане правопорушення, мають високий рівень інтелектуального розвитку, схильність до інтровертності, обмежену соціальну активність, а основним мотивом злочинної діяльності у більшості випадків є корисливість. Також проаналізовано роль психологічних факторів, що впливають на вибір злочинного способу дій.

Аналіз статистичних даних показав, що більшість правопорушників – є чоловіками віком від 18 до 39 років, але в останні роки зростає кількість жінок та неповнолітніх, залучених до злочинної діяльності. Більшість мають середню або вищу освіту, переважно не працюють та не навчаються. Також виявлено тенденцію до збільшення частки військовослужбовців серед суб'єктів даного правопорушення, що може бути пов'язано із низкою окреслених у статті чинників.

В свою чергу, дослідження психологічних характеристик показало, що для осіб, які вчиняють несанкціоноване втручання в інформаційні системи, не є характерними ті риси, що є притаманними для інших кіберзлочинців, зокрема це відхилення у психосексуальному розвитку, боязкість і лякливість, філософське сприйняття світу. Водночас у їх поведінці ярко простежується цинізм, недовіра до суспільства, високий рівень раціональності та прагматизму, а також високий інтелектуальний рівень у поєднанні з аутичними проявами та соціальним аутсайдерством.

Результати дослідження дають змогу детальніше вивчити соціально-демографічні та психологічні характеристики осіб, що вчиняють несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що є надзвичайно важливим для вдосконалення роботи правоохоронних органів та розробки ефективних заходів щодо запобігання та профілактики кіберзлочинності за статтею 361 Кримінального кодексу.

Ключові слова: особа злочинця, психологія кіберзлочинця, кіберзлочинність, несанкціоноване втручання, інформаційні технології, інформаційні злочини, боротьба з кіберзлочинністю.

The article examines the criminological characteristics of a person who commits a criminal offence under Article 361 of the Criminal Code of Ukraine – unauthorised interference with information (automated), electronic communication, information and communication systems and electronic communication networks.

Based on the analysis of statistical data, scientific works and court practice, the author identifies the socio-demographic, psychological and criminological characteristics of persons committing this crime. The author examines the gender and age differentiation of offenders, their educational level, marital status, social status, employment status, and individual psychological traits. Particular attention is paid to the motivational factors that may encourage offenders to commit an offence.

It is established that the vast majority of persons committing this offence have a high level of intellectual development, a tendency to introversion, limited social activity, and the main motive for criminal activity in most cases is self-interest. The author also analyses the role of psychological factors that influence the choice of a criminal course of action.

Analysis of statistical data has shown that most offenders are men aged 18 to 39, but in recent years the number of women and minors involved in criminal activity has been increasing. Most have secondary or higher education, and are mostly unemployed and uneducated. There is also a tendency to increase the proportion of military personnel among the perpetrators of this offence, which may be due to a number of factors outlined in the article.

In turn, the study of psychological characteristics has shown that persons who commit unauthorised interference with information systems do not have the features that are typical of other cybercriminals, in particular, deviations in psychosexual development, timidity and fearfulness, and a philosophical perception of the world. At the same time, their behaviour is marked by cynicism, distrust of society, a high level of rationality and pragmatism, as well as a high intellectual level combined with autistic manifestations and social outsiderism.

The results of the study make it possible to study in more detail the socio-demographic and psychological characteristics of persons who commit unauthorized interference with the operation of information (automated), electronic communication, information and communication systems, electronic communication networks, which is extremely important for improving the work of law enforcement agencies and developing effective measures to prevent and prevent cybercrime under Article 361 of the Criminal Code.

Key words: personality of a criminal, psychology of a cybercriminal, cybercrime, unauthorised interference, information technology, information crime, combating cybercrime.

Поява нових інформаційних технологій та їх тотальна інтеграція у повсякденне життя, разом із недостатньою адаптацією держав та міжнародної спільноти до викликів сьогодення, призвела до прогресивного зростання такого специфічного виду злочинності, як – кіберзлочинність [1, с. 81]. Наразі, в Кримінальному Кодексі України існує окремий Розділ XVI в якому переважно наведені ті кримінальні правопорушення, що і складають кіберзлочинність як таку.

Зокрема, до них належить і стаття 361 КК, яка передбачає кримінальну відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Аналіз статистичних даних Офісу Генеральної прокуратури за останнє десятиліття свідчить, що саме це правопорушення займає найбільшу питому вагу серед злочинів, передбачених Розділом XVI КК України, що в свою чергу вказує на його значну поширеність та необхідність розробки ефективних заходів його запобігання. Так, у 2024 році цей показник становив 48,2% та протягом останніх десяти

років варіюється у діапазоні від 41,1% (2022 р.) до 78,2% (2014 р.) кримінальних правопорушень за ст. 361 до загальної кількості облікованих правопорушень передбачених Розділом XVI, тобто переважна більшість [2].

У цьому контексті важливим напрямом кримінологічного аналізу стає дослідження особи злочинця, який вчиняє кримінальне правопорушення, передбачене статтею 361 КК України. Формування ефективних заходів протидії кіберзлочинності потребує всебічного дослідження соціально-демографічних, психологічних і кримінологічних характеристик осіб, які вчиняють подібні правопорушення, а також аналізу їх мотивацій і способу мислення.

Дослідженням особи кіберзлочинця займалася велика кількість вітчизняних науковців, зокрема: Б. М. Головкін, О. В. Ткачова та Науменко К. В., Т. В. Продан, О. М. Кравцова та інші. Проте, незважаючи на глибину праць вищезгаданих авторів, жодним з них не було розглянуто особу злочинця, що вчиняє конкретне кримінальне правопорушення проти основ кібербезпеки, у нашому випадку несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

З цього випливає мета нашого дослідження, яка полягає в проведенні кримінологічної характеристики особи злочинця, зокрема визначення її структури, індивідуальних ознак, якостей, властивостей, що характеризують особу злочинця з різних боків. Дане кримінологічне дослідження є одним з напрямів комплексного нормативного подолання загроз в інформаційній сфері та має важливе значення для розробки заходів запобігання та превенції кіберзлочиннів передбачених ст. 361 КК [3, с. 159].

Так найважливішим елементом в контексті кримінологічної характеристики є структура особи злочинця, яка визначається різними соціальними, демографічними та психічними ознаками, які при їх ретельному дослідженні дозволяють виявити певні закономірності у моделі злочинців та на основі цього сформувати портрет середньостатистичного правопорушника, що вчиняє несанкціоноване втручання в роботу інформаційних систем, тощо [4, с. 257].

Першою характерною демографічною ознакою особи злочинця, що вчиняє кримінальне правопорушення за ст. 361 є стать. Так, протягом 2017–2024 рр. було виявлено загалом 1127 осіб, що вчинили дане правопорушення, з яких 80,5% – чоловіки, а 18,5% – жінки. Варто зазначити, що незважаючи на стабільну більшість чоловіків, починаючи з 2021 року відбулось різке зростання жіночої злочинної активності у цій сфері. Наприклад, у 2020 році питома вага жінок до загальної кількості осіб, що вчинили цей злочин – становила 15%, а у 2021 р. зросла до 25% та продовжує коливатись в цих межах. На наш погляд, це може бути пов'язано із поступовим зменшенням гендерного дисбалансу в ІТ-сфері, зацікавленістю сучасних жінок у цифрових технологіях та дією інших зовнішніх і внутрішніх факторів.

Що стосується вікової диференціації, то найбільш кримінально активними виявились три вікових групи: від 18 до 28 років – 45% від загальної кількості протягом 2017–2024 рр.; від 29–39 років – 36,1%; 40–54 роки – 145 осіб. Інші вікові групи не є характерними для даного кримінального правопорушення, але в останні роки також спостерігається нова тенденція, так у 2024 р. відбулось різке збільшення кількості неповнолітніх осіб, що вчинили даний злочин, а саме 12 осіб 16–17 років та 3 особи 14–15 років. Звісно ця кількість є невеликою, що може бути пов'язано з відсутністю доступу до всіх механізмів його реалізації, наприклад спеціалізованої освіти, незалежних від батьків банківських рахунків, тощо, але сам факт зростання цієї кількості свідчить про деформації правосвідомості серед молоді та про поширення кіберзлочинності серед неповнолітніх. В свою чергу, та більшість осіб, що знаходяться у молодому, або середньому віці, можуть мати доступ до необхідного обладнання, певні навички користування ним, а також всі інші необхідні для здійснення кримінального правопорушення за ст. 361 КК засоби [5].

Надзвичайно важливою демографічною ознакою також є освітній рівень злочинців. Відповідно у період з 2017 по 2024 роки несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж вчинили: 62% осіб з повною середньою освітою, 21% осіб з вищою освітою, 16% осіб із професійно-технічною освітою (16%) та лише 1% із початковою освітою або без неї.

Отже, основну частку правопорушників становлять особи з повною середньою освітою, що може свідчити доступність даного виду злочинної діяльності для людей із базовими технологічними навичками. Особи з вищою освітою, маючи глибші знання та кваліфікацію, можуть бути залучені до більш складних та технічно оснащених злочинів, в той час як люди з низьким рівнем освіти не є характерними суб'єктами цього правопорушень в силу відсутності необхідних навичок [6, с. 116–120].

За сімейним станом більшість кіберзлочинців є неодруженими, деякі науковці пов'язують це з кількістю часу який правопорушники витрачають на отримання досвіду роботи з високими технологіями, що в свою чергу заважає своєчасній побудові особистого життя [4, с. 258].

Варто зазначити, що за ознакою громадянства 99,2% правопорушників є громадянами України (2017–2024 рр.) та лише 0,81% іноземні громадяни. Спостерігається також високий рівень урбанізації злочинності за статтею 361 Кримінального Кодексу, що збігається з загальною тенденцією розповсюдження злочинності по Україні. В даному випадку, простежуємо взаємозв'язок з тим, що жителі міст мають більшу інтеграцію в цифрові технології та контакт з ними, ніж особи з сільської місцевості.

Соціальні ознаки відображають соціально-економічний стан злочинців, рівень їхньої зайнятості, професійний статус, рівень доходів та інші характеристики. Серед осіб, які вчиняють несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж у 2024 році офіційно безробітними були 4 правопорушники, 244 – працездатними, які не працюють та не навчаються. На наш погляд, рівень зайнятості населення напряму впливає на злочинність у цьому секторі.

Що стосується, соціального статусу, то він переважно є середнім. Серед займаних посад – 1 депутат, 1 працівник правоохоронних органів та 1 державний службовець. Більш характерною соціальною групою є студенти, серед них 17 осіб вчинили дане кримінальне правопорушення у минулому році.

Аналіз статистичних даних також свідчить про поступове зростання частки військовослужбовців серед осіб, які вчиняють кримінальні правопорушення, передбачені ст. 361 КК України (40 осіб у 2024 році до 0 у 2017). Така тенденція може бути зумовлена низкою факторів, зокрема труднощами адаптації до цивільного життя, доступом до спеціалізованої інформації та технологій, впливом психологічного тиску і стресу під час проходження військової служби, матеріальними мотивами, зумовленими фінансовими труднощами, а також залученістю до інформаційних війн і кібератак. результати опитування, проведеного Українським Ветеранським Фондом, засвідчують, що серед ветеранів і ветеранок, які наразі не проходять службу в Силах оборони України, 56,16% респондентів зазначили про потребу у фінансовій підтримці, а 24,07% – у працевлаштуванні. Це свідчить про наявність соціально-економічних факторів, що можуть детермінувати вчинення правопорушень зазначеної категорії [7].

Суб'єкти даного правопорушення досить часто ведуть відсторонений спосіб життя та не відрізняються високою соціальною активністю, деякий відсоток з них можуть бути членами так званих тематичних інтернет-ком'юніті, форумів із метою віртуального спілкування між однодумцями. Вважаємо, що це пов'язано з тим, що ці особи частіш за все є слабо розвинутими як на фізичному, так і ментально-психологічному рівні, мають певні особливості в фізичній конструкції, зокрема худорлявість або зайву вагу, проблеми з соціальною-адаптацією, також більшість з них є інтровертами.

Портрет кіберзлочинця у контексті ст. 361 КК України також включає низку індивідуально-психологічних рис, частіш за все це високий інтелектуальний рівень поєднаний із вираженими аутистичними проявами, соціальним аутсайдерством, цинізмом, недовірою до суспільства та відсутністю моральних обмежень, гордовитим, зневажливим ставленням до інших. Усвідомлення цих характеристик є важливим для правоохоронних органів та спеціалістів з кібербезпеки з метою розробки ефективних заходів протидії кіберзлочинності [8, с. 201]. Наприклад цинізм та відсутність моральних обмежень може виникнути у свідомості злочинця через високу латентність кіберзлочинів, яка варіюється від 90 до 95%. Крім того, деякі науковці вказують на взаємозв'язок злочинності та поведінкою жертви – віктимністю. Згідно з позицією Б. М. Головкіна, фізичний аспект віктимної поведінки полягає у недостатньому дотриманні норм особистої та майнової безпеки, що в контексті кіберзлочинності може виражатися через нехтування принципами кібербезпеки, прагнення до мінімізації зусиль і витрат, надмірну довірливість до сторонніх осіб, демонстративну активність у соціальних мережах тощо [9, с. 6–13]. Усвідомлення цих факторів потенційним злочинцем може сприяти формуванню у його психіці мотиву до скоєння правопорушення, а також зверхнє ставлення до інших людей, які не мають таких технологічних навичок, як вони.

Важливо зазначити, що на наш погляд, для осіб що вчиняють несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не є характерними всі індивідуальні-психологічні ознаки, які науковці виділяють серед кіберзлочинців. Зокрема, до менш характерних ознак можемо віднести відхилення у психосексуальному розвитку, боязкість і лякливість, а також філософське сприйняття світу.

Відсутність значної кореляції між кіберзлочинністю та відхиленнями у психосексуальному розвитку пояснюється тим, що такі порушення частіше виявляються серед осіб, залучених до сексуальних форм кіберзлочинності (наприклад, розповсюдження забороненого контенту, кібергрумінг), або серед осіб які вчиняють більш технічно складні кіберзлочини, а не серед правопорушників, які здійснюють втручання в інформаційні системи з метою отримання несанкціонованого доступу, тощо.

Щодо боязкості та лякливості, хоча деякі кіберзлочинці і можуть демонструвати соціальну замкненість, їхня діяльність не завжди свідчить про страх перед соціальними контактами. Навпаки, багато хто з них активно взаємодіє з потенційними жертвами з метою ввести їх в оману, втертись в довіру задля подальшого вчинення злочину. В свою чергу, філософське сприйняття світу, хоча й може бути притаманним частині кіберзлочинців (особливо серед ідеологічно мотивованих хактивістів), загалом не є визначальною рисою для осіб, що вчиняють несанкціоноване втручання в інформаційні системи. Більшість із них керується суто практичними мотивами – фінансовими або іншими вигодами, прагненням до змагання чи самоствердження у кіберсередовищі.

Тобто, аналіз психологічного профілю осіб, які вчиняють злочини, передбачені ст. 361 КК України, свідчить про необхідність диференційованого підходу до вивчення кіберзлочинності. Не всі загальні риси, характерні для кіберзлочинців у широкому сенсі, однаково притаманні особам, що здійснюють саме несанкціоноване втручання в інформаційні системи.

Особа злочинця також характеризується мотивом, якою вона керується на момент вчинення правопорушення. Так, аналіз 100 судових вироків за ст. 361 КК України, внесених до Єдиного реєстру судових рішень, показав, що у 74% випадків злочини вчинялися з корисливих мотивів, інші 17% – з хуліганськими мотивами, та 9% з метою помсти. У більшості вироків також фігурують статті 185, 190, 200 КК України, що свідчить про взаємозв'язок ст. 361 КК із іншими видами майнових правопорушень, що підтверджує вплив матеріальних факторів на злочинну поведінку та характеризує особу злочинця [10].

Злочини, передбачені ст. 361 КК України, у переважній більшості вчиняються умисно, що свідчить про усвідомлену протиправну поведінку правопорушників. Аналіз статистичних даних також вказує на значну поширеність рецидиву: у 2024 р. серед підозрюваних 361 особа мала попередній досвід вчинення кримінальних правопорушень. Також 179 злочинів були вчинені групою осіб. Ці дані, на наш погляд, підтверджують тенденцію до високого рівня організованості та повторюваності злочинної діяльності в сфері несанкціонованого втручання в роботу інформаційних (автоматизованих) систем і мереж.

Отже, в процесі дослідження, нами було проведено кримінологічну характеристику особи злочинця, що вчиняє кримінальне правопорушення за ст. 361 КК, визначено структуру особи злочинця, її демографічні, соціальні, індивідуально-психологічні ознаки. Так, аналіз статистичних даних свідчить, що основну частку правопорушників становлять чоловіки віком від 18 до 39 років, хоча з 2021 року спостерігається зростання кількості жінок серед правопорушників. Також простежується тенденція до залучення до кіберзлочинної діяльності неповнолітніх осіб, що може бути наслідком зростаючого впливу цифрового середовища на молодь.

Щодо освітнього рівня, переважна більшість злочинців мають повну середню або вищу освіту, що підтверджує важливість базових технологічних знань для вчинення таких правопорушень. Крім того, значний відсоток злочинців є працездатними, але офіційно не працюють або не навчаються, що вказує на зв'язок між соціально-економічним станом населення та кіберзлочинністю. Про це також свідчить наявність корисливого мотиву у 74% облікованих правопорушень.

Дослідження психологічних характеристик показало, що для осіб, які вчиняють несанкціоноване втручання в інформаційні системи, не є характерними такі риси, як відхилення у психосексуальному розвитку, боязкість і лякливість, філософське сприйняття світу. Натомість у їхньому поведінковому профілі домінують цинізм, недовіра до суспільства, високий рівень раціональності та прагматизму, а також високий інтелектуальний рівень у поєднанні з аутичними проявами та соціальним аутсайдерством.

Таким чином, результати дослідження дозволяють глибше зрозуміти соціально-демографічні та психологічні характеристики осіб, які вчиняють злочини, передбачені ст. 361 КК України, що має важливе значення для правоохоронної діяльності. Отримані дані можуть бути використані для розробки ефективних заходів запобігання та превенції кіберзлочиннів за ст. 361 Кримінального Кодексу.

ЛІТЕРАТУРА

1. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах. Журнал східноєвропейського права. 2016. № 31. С. 80–86.

2. Єдиний звіт про кримінальні правопорушення (2014-2024). Офіс Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovanikriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

3. Таволжанський, О. В. Основи державної кіберполітики України: формування та реалізація. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право. 2017. № 4. С. 158–164.

4. Кримінологія: підручник / Б. М. Головкін, В. В. Голіна, О. Ю . Шостко та ін.; за ред. Б. М. Головкіна. Харків: Право. 2020. 384 с.

5. Єдиний звіт про осіб, що вчинили кримінальні правопорушення (2014-2024). Офіс Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-osibyaki-vchinili-kriminalni-pravoporushennya-2

6. Стручаєв М. Ф. Кримінологічний аналіз злочинності за ст. 361 КК України: статистичні закономірності та тенденції. The 3rd International Scientific and Practical Conference «Scientific Exploration: Bridging Theory and Practice» (March 24–26, 2025. Berlin, Germany). *European Open Science Space*. 2025. С. 116–120.

7. Потреби ветеранів 2023. Український ветеранський фонд. Інтернет-ресурс: https://veteranfund.com.ua/analitics/needs-of-veterans-2023/

8. Ткачова О. В., Науменко К. В. Кримінологічна характеристика кіберзлочинця. *Юридичний науковий електронний журнал*. 2018. № 2. С. 200–204.

9. Головкін Б. М. Віктимність як основна категорія віктимології. Журнал східноєвропейського права. 2015. № 20. С. 6–13.

10. Єдиний реєстр судових рішень. URL: https://reyestr.court.gov.ua/