УДК 343.9. 01
DOI https://doi.org/10.32782/2524-0374/2021-11/147

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ

CRIMINOLOGICAL CHARACTERISTICS OF CYBERCRIME

Дулепа В.П., студентка ІІ курсу
Інститут прокуратури та кримінальної юстиції
Національного юридичного університету імені Ярослава Мудрого

Статтю присвячено вивченню кримінологічної характеристики кіберзлочинності. Проаналізовано, що в умовах становлення інформаційного суспільства в Україні, коли комп'ютерні та телекомунікаційні технології поширюються всюди, виникають проблеми, пов'язані з безпекою у віртуальному просторі. Визначено, що з кіберзлочинністю потрібно боротися, адже це становить загрозу не лише для демократичних перетворень, а й для національної безпеки України. Проаналізовано, що в теорії немає єдиного визначення кіберзлочинності, тому наведено думки вчених щодо цього. Зазначено ознаки кіберзлочинності, її особливості, як-от транскордонний характер. Перелічено, які групи кіберзлочинів передбачені Конвенцією Ради Європи. Висвітлено стан нормативно-правого регулювання запобігання і протидії цьому явищу в Україні. Продемонстрована статистика облікованих злочинів у кіберпросторі та осіб, що їх учинили. Визначено, що ця статистика неповно відображає рівень кіберзлочинності, для якого властива висока латентність. Досліджено, що рівень кіберзлочинності останніми роками значно зріс, збільшилась його питома вага щодо інших видів злочинів. Установлено таке: хоча рівень злочинності зростає, кількість засуджених становить лише десятки осіб. Визначено, що шкода, заподіяна кіберзлочинами, є дуже значною. Проаналізовано, що серед кіберзлочинів найбільше переважають ті, які пов'язані з несанкціонованим втручанням у роботу комп'ютерів. Висвітлено позицію вченого щодо факторів латентності кіберзлочинців. Досліджуючи географію цього виду злочинності, ми встановили, що найбільше злочинів вчиняється в густонаселених містах. Установлено, що кіберзлочини найчастіше вчиняють 30–50-річні особи чоловічої статі, які мають повну вищу освіту та які на момент вчинення злочину були працездатними, але не працювали і не навчались, громадяни України, неодружені. Досліджено морально-психологічні якості таких осіб та мотиви вчинення злочину. Зазначено, що кримінологічна характеристика кіберзлочинності є одним зі складників теоретичного запобігання та протидії цьому явищу. Визначено, що для боротьби з цим явищем необхідно об'єднати зусилля правоохоронної, судової систем спецслужб, здійснивши при цьому належне кадрове та матеріально-технічне забезпечення.

Ключові слова: кібербезпека, кіберзлочинець, кіберпростір, віртуальний простір, характеристика, статистика, боротьба, протидія, злочинність.

The article is devoted to the study of the criminological characteristics of cybercrime. It is analyzed that in the conditions of formation of information society in Ukraine, while computer and telecommunication technologies are spread everywhere, there are problems related to security in cyberspace. It has been determined that cybercrime must be fought, as it poses a threat not only to democratic transformations, but also to Ukraine's national security. It is analyzed that in theory there is no single definition of cybercrime, so the opinions of scientists on this subject are given. Signs of cybercrime, are indicated, in particular it's cross-border nature. It lists which cybercrime groups are provided by the Council of Europe Convention. The state of normative legal regulation of prevention and counteraction of this phenomenon in Ukraine is highlighted. Statistics of reported crimes in cyberspace and those who committed them are demonstrated. Determined that these statistics do not fully reflect the level of cybercrime, which is characterized by high latency. Researched that the level of cybercrime has increased significantly in recent years compared to previous years, its share has increased compared to other types of crimes. It is determined that the damage caused by cybercrime is very significant. The position of the scientist about the latency factors of cybercriminals is highlighted. Examining the geography of this type of crime, it was found that most crimes are committed in densely populated cities. It is established that cybercrimes are most often committed by men, aged 30–50, with a complete higher education, at the time of the crime were able to work, but did not work or study, citizens of Ukraine, single. The moral and psychological qualities of such persons and the motives for committing the crime have been studied.

Key words: cybersecurity, cybercrime, cyberspace, characteristics, statistics, struggle, counteraction, crime.

Становлення інформаційного суспільства в Україні, розвиток та поширення комп'ютерних технологій та комп'ютерної техніки, використання телекомунікаційних мереж майже в усіх сферах життєдіяльності людини полегшило можливість передання інформації, створивши низку проблем, пов'язаних зі створенням безпечних умов використання віртуального простору. У період глобалізації швидкий розвиток інформаційних технологій та комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою та надає широкі можливості для вчинення традиційних злочинів, створюючи при цьому умови для реалізації зовсім нових схем і методів злочинної діяльності. Рівень можливостей, які отримують зловмисники, й тенденція до збільшення кількості злочинів у сфері комп'ютерних інформаційних технологій становлять загрозу не лише демократичним перетворенням та розвитку інформаційного суспільства в Україні, а й національній безпеці загалом.

Наразі терміни «кіберзлочин», «кіберзлочинець» чи «кіберзлочинність» так і не знайшли універсального визначення на конвенціональному рівні чи в інших міжнародних правових документах. Сама ж концепція була сформована завдяки діяльності правозахисних органів країн Європи та світу і поширюється на злочини у сфері комп'ютерної інформації та телекомунікацій, на обіг нелі-

цензованого програмного забезпечення для комп'ютерів, радіоелектронних і спеціальних технічних засобів, а також деяких інших видів злочинів. Проте в науці немає єдності щодо загальноприйнятої дефініції досліджуваного поняття. Наприклад, Б. Головкін стверджує, що кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [1]. М. Погорецький тут убачає злочини у сфері комп'ютерної інформації [2], тобто під час використання текстової, графічної чи будь-якої іншої інформації (даних), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватись, змінюватись чи використовуватись за допомогою АЕОМ. В. Болгов зазначає, що кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних, суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або

користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [3]. Попри відсутність єдиного підходу до розуміння кіберзлочинності, проблема запобігання і боротьби з нею залишається завжди актуальною, особливо в сучасних умовах.

Характеризуючи кіберзлочинність, можна виокремити низку її ознак:

1) такий тип злочинів вчиняється у віртуальному просторі або в межах комп'ютерних мереж;

2) вчинення кіберзлочинів, на відміну від інших, є більш доступним для людей із невисокими соціальними і віковими можливостями;

3) вчинення злочину у віртуальному просторі вимагає застосування певного комплексу знань, крім того, в суспільстві активно пропагується ідея «інтелектуальності» хакерів, роблячи цю субкультуру ще більш популярною;

4) кіберзлочини є анонімними та неперсоніфікованими;

5) цьому виду злочинності властивий високий рівень латентності [4].

Потрібно зазначити, що це явище за своєю природою є транскордонним. Можливість маніпуляцій з ідентичністю, глобальність і транскордонність комп'ютерних і телекомунікаційних мереж породжують ситуації, коли кіберзлочинець, перебуваючи на одному континенті, вчиняє злочин на іншому, негативні наслідки злочину виявляються на третьому, а всі ці події відбуваються у віртуальному просторі. Саме тому для забезпечення безпеки віртуального простору є необхідність мобілізації сил та ресурсів не лише на національному рівні, а й на міжнародному.

Є декілька підходів до класифікації кіберзлочинів, але ми розглянемо запропонований Конвенцією Ради Європи «Про кіберзлочинність», яка виокремлює такі п'ять груп злочинів:

- проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, як-от незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему;
- пов'язані з використанням комп'ютера як засобу скоєння злочинів, зокрема маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо);
- пов'язані з контентом (змістом даних), розміщеним у комп'ютерних мережах (зокрема, пов'язані з дитячою порнографією);
- пов'язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень унаслідено документом до компетенції національних законодавств держав;
- зафіксовані в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж) [5].

Ще одним важливим питанням, яке потребує висвітлення, є нормативне регулювання запобігання та протидії кіберзлочинності в Україні. Указом Президента України від 26 серпня 2021 року № 447/2021 затверджено Стратегію кібербезпеки, де зазначається, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки [6]. У 2017 році ухвалено профільний Закон України «Про основні засади забезпечення кібербезпеки України» [7]. Крім цього, у 2005 році відбулась ратифікація Будапештської конвенції Ради Європи «Про кіберзлочинність», про яку зазначалось вище [5]. Аналіз нормативної бази вказує на те, що Україна на законодавчому рівні вже зробила перші кроки у сфері боротьби і протидії кіберзлочинності.

Переходячи до кримінологічної характеристики, проаналізуємо показники рівня та динаміки зазначених кіберзлочинів (розділ XVI КК України) за останні 7 років, звернувшись до офіційної статистики. Нині офіційна державна статистика містить відомості про вчинені кримінальні правопорушення, передбачені Розділом XVI КК України, які відображаються у звітах Офісу Генерального прокурора України (далі – ОГП) [8] та у відомчій статистичній звітності Національної поліції України.

Таблиця 1

(за даними Офісу Генерального прокурора)

Рік	Обліковані кримінальні правопорушення	Кількість осіб, яким вручено повідомлення про підозру
2014 р.	443	207
2015 р.	598	263
2016 р.	865	472
2017 р.	2573	1272
2018 р.	2301	1608
2019 р.	2204	1481
2020 р.	2498	1675
2021 р. (станом на жовтень)	2790	2034

Характеризуючи наведені статистичні дані, потрібно вказати на їхні особливості:

1) статистична інформація, яка надається ОГП, стосується лише злочинів, обмежених Розділом XVI КК України. При цьому не можна встановити кількість інших «традиційних» кіберзлочинів, як-от кібершахрайства та ін., адже вони містяться в інших розділах і об'єднані в спільну статистичну інформацію зі злочинами певного розділу;

2) надана статистика не здатна повно та достовірно відобразити стан кіберзлочинності в Україні, адже такий вид злочинної діяльності, як уже зазначалось, характеризується високим рівнем латентності.

Отже, щодо *рівня кіберзлочинності*, то станом на 2014 рік він становив 443 зареєстрованих злочини, де повідомлення про підозру отримало 207 осіб, а станом на 2021 рік (на жовтень) обліковано 2 498 злочинів, із яких 2 034 особам вручено підозру. Можна побачити й значний приріст у *динаміці* досліджуваного виду злочинності в Україні за останні 7 років. Порівняно з 2014 роком кількість виявлених злочинів збільшилась майже в шість разів. Питома вага злочинності у сфері електронно-обчислюваних машин у структурі злочинності в Україні за 2014 рік становила приблизно 0,08%, у 2015 р – 0,01%, у 2016 р. – 0,15%, у 2017 р. – 0,49%, у 2018 р. – 0,5%, у 2019 р. – 0,49%, у 2020 р. – 0,7%, а у 2021 р. (станом на жовтень) – 0,93% [8]. *Рівень судимості* за 2014 рік склав 37 осіб, за 2015 – 31 особу, за 2016 – 24 особи, за 2017 – 42 особи, за 2018 – 49 осіб, за 2019 – 50 осіб, за 2020 – 56 осіб. Отже, зазначений показник є досить мізерним порівняно з кількістю облікованих щорічно злочинів [9]. За звітними даними Голови Національної поліції України, *ціна кіберзлочинності* в Україні за 2019 рік становила 28 мільйонів гривень, а станом на 2020 рік зросла до 241 мільйона гривень [10]. Американська компанія McAfee, яка спеціалізується на комп'ютерній безпеці, та Центр стратегічних і міжнародних досліджень (CSIS) стверджують, що хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів, або 820 мільярдів євро [11].

Аналізуючи дані за 2020 рік *щодо структури*, можемо дійти висновку, що найбільшу питому вагу серед злочинів, передбачених розділом XVI КК України (49%) становлять дії з несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ); 5% – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збуту (ст. 361^{-1} ККУ); 3% – несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^{-2} ККУ);

42% – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 ККУ); 0,6% – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363 ККУ); 0,4% – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку через масове розповсюдження повідомлень електрозв'язку (ст. 363^{-1} ККУ).

Що стосується *рівня латентності* кіберзлочинів, то він становить близько 90–95%. Б.М. Головкін зазначає, що факторами латентності тут є такі:

- високотехнологічність вчинення кіберзлочинів, що перебуває на межі різних сфер життєдіяльності, тоді як недотримання загальних правил безпеки під час використання комп'ютера більшістю потенційних жертв кіберзлочинів, нехтування своєю безпекою;
- негативна поведінка жертв злочину або очевидців (у деяких випадках жертві не зовсім відомо про те, що стосовно неї було скоєно злочин, у інших – неповідомлення потерпілим особам про факти вчинення таких злочинів;
- недоліки в роботі правоохоронних органів стосовно реагування на звернення та повідомлення про кіберзлочини [12].

Аналіз *географії кіберзлочинності* в Україні виявив її залежність від чинника урбанізації. З огляду на це, найбільша кіберкримінальна активність прослідковується в м. Києві, у Харківській, Миколаївській, Одеській, Запорізькій, Черкаській та Львівській областях, найнижча – у Чернівецькій, Херсонській, Сумській і Кіровоградській. Проте надані географічні особливості кіберзлочинності доцільно розглядати не стільки через призму густоти населення, скільки через фінансовий та промисловий розвиток тієї чи іншої області, адже саме технічний розвиток є неможливим без залучення сучасних інформаційних технологій, середовище яких і є середовищем кіберзлочинності [13].

Вивчення *особи кіберзлочинця* також має вагоме значення в контексті виявлення закономірностей злочинної поведінки, розуміння способу мислення злочинця, а також для належної організації та профілактики протидії кримінальним правопорушенням.

Щодо *статі*, то злочини цього виду найчастіше вчиняються чоловіками, але протягом останніх років спостерігаємо тенденцію до збільшення питомої ваги жінок, адже вони вчиняють близько третини кіберзлочинів. Пояснити це можна так:

- по-перше, злочинність у кіберпросторі не потребує фізичної активності та підготовки, що дозволяє жінкам на рівні з чоловіками «працювати» в цій сфері, використовуючи злочинні форми поведінки;
- по-друге, результати науково-технічного прогресу почали користуватись підвищеним інтересом із боку жінок.

Аналіз даних судової статистики про склад засуджених в Україні за 2014–2019 роки за злочини, передбачені ст. 361–363-1 КК України, показав, що найбільше злочинів цього виду вчиняється 30–50-річними особами, на другому місці перебувають особи від 25 до 30 років, на третьому – від 18 до 25 років. Починаючи з 2020 року, вік кіберзлочинців почав зменшуватися, тому тепер найбільше злочинів у віртуальному просторі, передбачених розділом XVI КК України, вчиняється особами від 18 до 25 років [14]. Згідно з кримінологічними та соціологічними дослідженнями, проведеними вітчизняними й зарубіжними науковцями, за віковими ознаками можна виокремити три категорії кіберзлочинців. Перша – молодь віком від 13 до 17 років, яка займається переважно злочинами з використанням кредитних карток, телефонних номерів, підбираючи при цьому коди й паролі. Для цієї групи характерними є відсутність продуманої, цілеспрямованої підготовки до злочину; оригінальність способу; факти невмотивованого бешкетництва, неприйняття заходів для приховування злочину. Друга група – 18–25-річні особи, які займаються комп'ютерним хакерством. Це студенти, які встановлюють тісні стосунки з хакерами інших країн для підвищення свого пізнавального рівня і за допомогою електронних мереж BBS обмінюються з ними інформацією, викрадаючи її з різних банків даних. До третьої категорії належать 30–45-річні особи, які вчиняють злочини з корисливою метою [15, с. 107; 16, с. 477].

Статистичні дані вказують на те, що близько 60% осіб на момент вчинення злочину були працездатними, але не навчались і не працювали. За *освітнім рівнем* більшість кіберзлочинців характеризуються наявністю повної вищої, повної загальної середньої чи професійно-технічної освіти.

Серед засуджених є близько 98% громадян України, тобто лише 2% становлять громадяни інших держав.

Специфіка діяльності кіберзлочинців негативно відбивається на особистому житті, тому за *сімейним станом* це неодружені особи або одружені, які проживають окремо від сім'ї.

У структурі *морально-психологічних* якостей таких осіб переважають: авантюризм, порушення емоційно-вольової сфери, антигуманна спрямованість, правовий нігілізм, викривлена система життєвих цінностей, виражений цинізм, корисливість, заглибленість у своїх думках, мріях, фантазіях [12].

Мотивами кіберзлочинів є такі: користь, ігрові, політичні, хуліганські мотиви, помста.

Таким чином, кримінологічна характеристика кіберзлочинності є одним із теоретичних складників запобігання та протидії злочинності, адже на теоретичному рівні (за допомогою даних офіційної статистики) вона дозволяє виокремити низку властивостей, які притаманні цьому виду злочинності, а також сформувати наближений портрет кіберзлочинця. Це має позитивно відзначатися на ефективності розслідування кіберзлочинів та притягненні винних осіб до відповідальності. Як уже зазначалось раніше, кількість облікованих кіберзлочинів та засуджених осіб, які їх вчинили, суттєво різняться, тому ще є над чим працювати. Причинами такого низького рівня судимості може бути недостатнє фінансове та технічне забезпечення органів, що здійснюють розслідування, і, як наслідок, відсутність технічних можливостей для пошуку й притягнення винних осіб до відповідальності. Окрім цього, чинником, що впливає на результативність розслідування, може бути недостатня кількість знань та досвіду в спеціалістів у галузі комп'ютерних технологій та телекомунікаційних мереж, які залучаються до розслідування кіберзлочинів.

Отже, стверджуємо, що в епоху інформаційних технологій слід більше уваги приділяти безпеці у віртуальному просторі. Адже швидкими темпами науково-технічного прогресу людська спільнота все більше і більше сфер суспільного життя переносить у кіберпростір, що надає злочинцям широке коло можливостей для реалізації своїх протиправних дій. З огляду на курс України на входження у світовий інформаційний простір, ми переконані, що потребує побудови національна модель забезпечення кібербезпеки держави, громадян, а також підприємств, установ і організацій. Для цього необхідна координація зусиль та взаємодія правоохоронних органів, судової системи, спецслужб, а також їх належне кадрове і матеріально-технічне забезпечення.

ЛІТЕРТУРА

1. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини. Навчальний посібник. Харків : Право, 2014. 284 с.
2. Погорецький М.А. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.
3. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : науково-практичний посібник. Київ : Національна академія прокуратури України, 2015. 202 с.
4. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. С. 4–12
5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021 / *Верховна Рада України*. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 17.10.2021)
6. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 року № 2824-IV / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 17.10.2021)
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-VII / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 18.10.2021).
8. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування : Єдиний звіт Офісу Генерального прокурора. URL: https://www.gp.gov.ua/ua/stat_n_st?dir_id=113653&libid=100820 (дата звернення: 18.10.2021)
9. Судова статистика. Форма № 7 «Звіт про склад засуджених»: URL: http://court.gov.ua/inshe/sudova_statystyka/.
10. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf (дата звернення: 18.10.2021)
11. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://tsn.ua/groshi/kiberzlochinci-u-2020-roci-zavdali-u-sviti-zbitkiv-na-trilyon-dolariv-doslidzhennya-1683076.html (дата звернення: 18.10.2021)
12. Головкін Б.М., Голіна В.В., Лисодєд О.В. Кримінологія : підручник. Право, 2020. 259 с.
13. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації Україн*и. 2018. № 2(19). С. 155–166.
14. Судова статистика. Форма № 7 «Звіт про склад засуджених»: URL: http://court.gov.ua/inshe/sudova_statystyka/
15. Комп'ютерна злочинність : навчальний посібник / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. Київ : Атіка, 2002. 240 с.
16. Протидія кіберзлочинності в Україні: правові та організаційні засади : навчальний посібник / О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін. Київ : Видавничий дім «Скіф», 2012. 728 с