

Назаркевич А. А.  
ст. гр. ПДЕБ зм– 11  
Тернопільський національний економічний університет

Каранетян О.М.  
к.е.н., доцент  
кафедри економічної безпеки та фінансових розслідувань  
Тернопільський національний економічний університет

## КОНЦЕПТУАЛІЗАЦІЯ КІБЕРЗЛОЧИННОСТІ В МІЖДИСЦИПЛІНАРНІЙ СФЕРІ НАУКОВОГО АНАЛІЗУ

На рубежі ХХ століття ознаменувався стрімким розвитком інформаційних технологій, що почали впроваджуватися в усі сфери життєдіяльності людей. Використання сучасних персональних комп'ютерів, інформаційно-обчислюваних мереж і комп'ютеризованих комунікаційних мереж забезпечило кожній особі можливості доступу до інформації, що зберігається у відповідних банках даних незалежно від доби і місцезнаходження абонента. Взаємопов'язаність інформаційної та комп'ютерної злочинності відображена на рис. 1.



Рис.1. Взаємопов'язаність інформаційної та комп'ютерної злочинності [1]

Поряд з перевагами, комп'ютеризація має ряд негативних наслідків, серед яких є поява якісно нового виду злочинності – кіберзлочинності. Наслідки цієї злочинності зачіпають не тільки інтереси окремих осіб, що стали жертвами, але

й компанії, організації, уряди і суспільство в цілому. Кіберзлочини найчастіше ставлять під загрозу життєво важливу інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства.

Під кіберзлочинністю слід розуміти сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом 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].

Дефініція «кіберзлочинність» часто вживається поряд з поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених, поняття «кіберзлочинність» є найширшим поняттям та охоплює найбільше коло злочинних посягань у віртуальному середовищі, а також його використання передбачає міжнародне законодавство. Так, Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність. Тому вважаємо обґрунтованим вживання саме цього терміну для кримінологічного дослідження цього різновиду злочинності.

Аналіз національного законодавства у сфері протидії кіберзлочинності показав, що в Україні не визначено ряд таких ключових понять як: кіберзлочинність, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист.

Разом з тим, застосовується диверсифікація дефініцій часто-густо не погоджених між собою. Так, в Законі України «Про національну безпеку України» згадуються «комп'ютерна злочинність» і «комп'ютерний тероризм», причому жоден з цих термінів не має свого визначення в даному нормативному документі [2]. У Законі України «Про боротьбу з тероризмом» не прописуються ключові поняття, зокрема «комп'ютерний тероризм». У рішенні Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» кібербезпека розглядається в контексті

необхідності розробки і впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, в тому числі відповідно до вимог ратифікованої Верховною Радою України Конвенції про кіберзлочинність.

Підґрунтям щодо кіберзлочинів є передбачені кримінальним законом суспільно небезпечні діяння і закріплені в окремому розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. З точки зору кримінального права до кіберзлочинів відносяться тільки злочину, передбачені розділом XVI КК України [3].

Разом з тим, кіберзлочинність набуває все більшого масштабу, новітні технології дозволяють злочинцям залишатися анонімними та сприяють швидкому збагаченню шляхом злочинної діяльності.

Можемо виділити наступні ознаки кіберзлочинності:

1. Ці злочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символічному чи іншому вигляді. Ці відомості знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі.

2. Кіберзлочини вчиняються за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину [3].

### Список літератури:

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. –2014. –№ 2. – С. 54-62
2. Про національну безпеку України [Електронний ресурс]: Закон України від 8 липня 2018 року №8068 // Верховна Рада України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/964-15>
3. Кримінальний кодекс України [Електронний ресурс] / Офіційний сайт Верховної Ради України. – Режим доступу: [http:// zakon1.rada.gov.ua](http://zakon1.rada.gov.ua)
4. Кузнецова С.А. Фінансовий моніторинг в Україні: якісний аспект. [Електронний ресурс] / С.А. Кузнецова. – Режим доступу: <http://bo0k.net/index.php?p=achapter&bid=5377&chapter=1>