DOI: https://doi.org/10.26642/jen-2025-1(111)-131-145
УДК 004:007:351.86

С.В. Корзун, аспірантка
Державний університет «Житомирська політехніка»

Понятійно-категоріальний апарат державної кримінально-правової політики протидії кіберзлочинам

У статті комплексно досліджується формування та ґенеза понятійно-категоріального апарату державної кримінально-правової політики протидії кіберзлочинам. Враховуючи наростаючу глобальну загрозу кіберзлочинності, найбільш ефективними є кримінальні засоби боротьби з нею, саме тому надзвичайно актуальним є уточнення понятійно-категоріального апарату.

Проаналізувавши науковий доробок попередніх років, дійшли до розуміння поняття «кіберзлочинність», «кіберзлочин» крізь призму багатовекторності, використовуючи різні підходи, в тому числі, розглядаючи міжнародне та національне законодавство. Особлива увага у статті присвячена виділенню ознак кіберзлочинів та їх класифікації, зокрема наведено приклади класифікацій різних вчених. Всебічно охарактеризовані види кіберзлочинів, що містяться в Конвенції Ради Європи про кіберзлочинність. На основі опрацьованого матеріалу розроблено власні підходи до класифікації кіберзлочинності для цілей державної кримінально-правової політики, що має багаторівневий характер.

Відносно визначених підходів до класифікації, ознак та змісту кіберзлочинності, виділено певні позиції щодо розгляду даних злочинів: по-перше, як суспільно небезпечне винне діяння, що полягає у виготовленні, фінансуванні, використанні, реалізації, обміні та розповсюдженні шкідливих програмних продуктів; по-друге, як суспільно небезпечне винне діяння, що скоєне з використанням інформаційно-комп'ютерних технологій.

Представлене дослідження полягає у аналізі понятійно-категоріального апарату державної кримінально-правової політики протидії кіберзлочинам, що дозволило сформувати сукупність теоретичних положень та є підґрунтям для формування й реалізації державної кримінально-правової політики протидії кіберзлочинності.

Ключові слова: *державна політика; кіберзлочинність; кіберпростір; протидія кіберзлочинності.*

Актуальність теми. Дослідження проблем державної політики в цілому та особливо кримінально-правової вимагає уточнення термінологічного апарату як власне для цілей дослідження, так і з позиції розширення теоретичних та методологічних положень і практики законотворчості. Державна кримінально-правова політика є складною динамічною системою, що охоплює сукупність сфер суспільних відносин, які проявляються як в кіберпросторі, так і в матеріальних соціально-економічних відносинах. Безумовно, що кримінально-правовий вплив на протидію кіберзлочинам є найбільш результативним та потребує постійного удосконалення, зважаючи на розвиток інформаційно-комп'ютерних технологій. «Політика в сфері протидії кіберзлочинності здійснюється різноманітними засобами. Найбільш ефективними у системі її протидії залишаються засоби кримінально-правового впливу. Діяльність з протидії кіберзлочинам засобами кримінально-правового впливу ґрунтується на їх криміналізації» [22]. Криміналізація кіберзлочинів вимагає уточнення понятійно-категоріального апарату, що стосується як власне понять «кіберзлочин» та «кіберзлочинність», так і суміжних понять, що поглиблює розуміння цього виду кримінальних правопорушень. «Кіберзлочинність – неминучий наслідок глобалізації інформаційних процесів і, як наслідок, є основною загрозою соціогуманітарної та інших компонентів. Зростаюча кількість кіберзлочинної діяльності на підприємствах, постійне вдосконалення інформаційних технологій і нові можливості «вдосконалення» інструментів їх скоєння створюють економічні загрози для глобальних інформаційних мереж» [36].

Аналіз останніх досліджень. Питання розвитку понятійно-категоріального апарату досліджували: Д.С. Азаров, О.Амелін, С.В. Бєлай, П.Д. Біленчук, В.М. Бутузов, В.О. Голубєв, Д.О. Грицишен, О.Ю. Довженко, О.П. Дзьобань, І.О. Драган, І.В. Європіна, М.В. Карчевський, М.О. Кравцова, В.В. Лісовий, О.В. Махницький, А.А. Музика, В.В. Пивоваров, В.Г. Пилипчук, Б.В. Романюк, С.О. Савчук, О.Столяр, К.В. Терещенко, В.С. Цимбалюк, К.В. Юртаєва та інші.

Викладення основного матеріалу. «Кіберзлочини є порівняно новим феноменом для кримінального права й криміналістики. Відсутнє навіть точне визначення цього поняття, проте наявне розуміння, що з'явилася нова категорія злочинів, що здійснюються в кіберпросторі та становлять не меншу загрозу, ніж "традиційні" злочини» [12].

«Поняття “кіберзлочинність” вперше з’явилося в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів відносно автоматизованих систем обробки даних. Поняття «кіберзлочинності як сукупності злочинів» поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, в якому відбуваються правопорушення, і засобом або знаряддям злочину» [36].

Сьогодні поняття «кіберзлочинність» має багатовекторне розуміння, що обумовлено його поширеністю в різних сферах суспільних відносин (економічна система, політична система, міжнародні відносини, соціальна сфера), різноманітними наслідками (економічні, соціальні, людські жертви, психологічні та інші) та впливом на національну безпеку (інформаційну, безпеку державного кордону, політичну, економічну, енергетичну, продовольчу та інші).

Денькович О. вказує, що «зрештою, відсутність єдності розуміння понять кіберзлочинності та кіберзлочину ілюструє загальносвітові тенденції. Зародження окремої категорії кіберзлочинів пов’язане з розвитком комп’ютерних технологій. Запровадження та поширення комп’ютерів на основі транзисторів у 1960-х роках створило передумови для появи нового виду злочинності. На цьому ранньому етапі кіберзлочини не виділялися в окрему групу, а обговорювались у контексті кримінальних правопорушень проти власності як правопорушення, які заподіюють фізичну шкоду комп’ютеру або розміщеній у ньому інформації. Однак вже у 1970-х роках акценти у визначенні кіберзлочину зміщуються. Незаконне використання комп’ютерних систем, маніпуляції з цифровими даними та перші шахрайські дії, вчинені з використанням комп’ютера, спричинили жваві дискусії у науковому середовищі щодо кримінально-правової оцінки таких діянь. У 1977 році у США було прийнято Федеральний закон про захист комп’ютерних систем, а пізніше інші держави також намагалися привести своє законодавство у відповідність до нових реалій та криміналізувати суспільно-небезпечні діяння, які вчинялися з використанням комп’ютерної системи чи мережі або у ній. Поява глобальної мережі “Інтернет” ще більше загострила проблему кіберзлочинності, й у 1989 році Європейський комітет з проблем злочинності Ради Європи надав низку рекомендацій національним законодавцям з приводу того, які діяння з комп’ютерними системами варто криміналізувати. А у 1994 році у межах ООН був розроблений “Посібник щодо попередження та контролю за комп’ютерними злочинами”, у якому констатовано, що міжнародного визначення поняття “комп’ютерного злочину” наразі не досягнуто. І хоча з моменту видання цього підручника минуло більше 20-ти років, єдиного уніфікованого міжнародного визначення поняття “кіберзлочину” досі немає» [9].

«Хоча поняття “кіберзлочинність”, “кіберзлочини” використовується як у міжнародному, так і у національному законодавстві, Кримінальний кодекс (далі – КК України) не містить визначення поняття “кіберзлочину”. В кримінально-правовій та кримінологічній доктрині дискутуються різні точки зору щодо їх поняття, видів та класифікації. Законодавча невизначеність понять породила дискусійність питання про тлумачення, що є кіберзлочинами, та умовно поділила науковців на дві групи. Перша група науковців відносить до кіберзлочинів дії, у яких комп’ютер є об’єктом або засобом посягання. Друга група визначає кіберзлочини як злочини, об’єктом посягання в яких є інформація, що обробляється в електронно-обчислювальній машині (комп’ютері) або в комп’ютерній системі, а засобом вчинення є електронно-обчислювальна машина (комп’ютер), тобто протизаконні дії у сфері автоматичної обробки інформації» [22].

У Законі України «Про основі засади забезпечення кібербезпеки України» представлене таке визначення поняття «кіберзлочин (комп’ютерний злочин)»: «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України; кіберзлочинність – сукупність кіберзлочинів» [29].

Щодо наукової літератури, то можна виокремити такі підходи до розуміння зазначеного поняття, що має стати підґрунтям для формування його змістовного наповнення як об’єкта державної кримінально-правової політики:

– кримінальні правопорушення, що вчинені із використанням інформаційно-комп’ютерних технологій. Цієї точки зору притримуються В.Пивоваров та С.Лисенко, які наводять таке тлумачення кіберзлочинності: «кіберзлочинність – це сукупність злочинів, що вчиняються з використанням комп’ютерної системи, або комп’ютерної мережі, чи мережі електрозв’язку, у межах комп’ютерної системи або комп’ютерної мережі чи мережі електрозв’язку, чи проти комп’ютерної системи або комп’ютерної мережі чи мережі електрозв’язку» [26]. Матвійчук М. в цьому контексті дотримується вузького та широкого розуміння кіберзлочину: «кіберзлочин у вузькому сенсі (комп’ютерний злочин): будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є безпека комп’ютерних систем і оброблюваних ними даних; кіберзлочин у широкому розумінні: (як злочин, пов’язаний з комп’ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов’язане з комп’ютерами, комп’ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп’ютерних систем або мереж» [24]. Діордіца І. вказує,

що «кіберзлочинність – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж» [11]. Загуменний О. пропонує до розуміння досліджуваного поняття такий підхід: «кіберзлочинність – найбільш об'ємне та містке поняття для означення злочинів, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [15]. Бабанін С. вказує, що «кіберзлочинність – це сукупність злочинів, що вчиняються за допомогою комп'ютерної мережі чи мережі електрозв'язку, у межах комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку, чи проти комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку» [1]. Пфо О. зазначає, що «кіберзлочинність – незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей» [30];

– кримінальні правопорушення в сфері інформаційної безпеки, що викладені в працях: 1) Савчук Н.В.: «кіберзлочинність охоплює «комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо» [32]; 2) Карчевський М.: «кіберзлочин – однин з видів злочинів у сфері інформаційної безпеки, що передбачені КК України, суспільно небезпечні, винні, вчинені суб'єктом злочину діяння, які заподіюють шкоду, забезпеченим засобами обчислювальної техніки, відносинам у сфері реалізації інформаційної потреби» [17];

– кримінальні правопорушення, що пов'язані із протиправним втручання в роботу інформаційно-комп'ютерних систем та технологій. Такого підходу дотримується О.Копан зазначаючи, що «кіберзлочин – протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер, створення та використання в злочинних цілях певної кібернетичної системи, використання в злочинних цілях існуючих кібернетичних систем» [20]. Русецький А. та Куцолабський Д. в цьому контексті пропонують таке розуміння досліджуваного явища: «кіберзлочин – це протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створювати особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці» [31];

– суспільно небезпечні діяння, що шкодять відносинам, які регулюють поводження з інформацією. Загальний підхід до такого розуміння кіберзлочинів міститься в науковому дослідженні М.Думчикова, який вказує, що «кіберзлочини – це умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам, які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист у кіберпросторі» [14]. Досить оригінальний підхід до розуміння кіберзлочинів міститься в праці Ю.Бельського, зокрема: «кіберзлочини – це злочини, які вчиняються в процесі автоматизованої обробки інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації та інші суспільних відносин, у яких комп'ютер виступає кваліфікуючою ознакою вчинення злочину (наприклад, комп'ютерне шахрайство, або кібертероризм)» [2]. Кравцова М. доводить, що «кіберзлочинність – соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку» [21];

– злочинність, що скоєно в змодельованому комп'ютером інформаційному / віртуальному / кібернетичному просторі. Зокрема Д.Біленчук пропонує під кіберзлочинністю розуміти: «злочинність у змодельованому за допомогою комп'ютера інформаційному просторі, в якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді, й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі» [3]. Буяджи С.А. пропонує під вказаним поняттям розуміти «сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об'єктів, розташованих на ній, за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі й комп'ютерні дані» [5]. Також підходу дотримується О.Іванченко, зазначаючи, що «кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем, шляхом використання комп'ютерних мереж чи інших засобів віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних» [16]. Погорецький М. вказує, що «у широкому розумінні кіберзлочини – це: кримінальні посягання, об'єктивна сторона яких відбувається у кіберпросторі, а об'єктом посягання є суспільні відносини у різноманітних сферах людської діяльності, пов'язані з використанням ресурсів кіберпростору. У вузькому розумінні під кіберзлочинами пропонується розуміти кримінальні посягання з використанням кіберпростору на відносини керування певними процесами, пов'язаними з використанням комп'ютерних систем» [28].

Фоменко О. пропонує під кіберзлочином розуміти «суспільно-небезпечне діяння, яке вчиняється у віртуальному просторі й так чи інакше пов'язане з комп'ютерною системою» [34]. Ковальчук А.Ю. пропонує подібний підхід до розуміння досліджуваного поняття: «кіберзлочинність може бути визначена як сукупність злочинів, скоєних у кіберпросторі за допомогою комп'ютерних систем чи комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних» [18]. На характеристиці віртуального простору при визначенні змісту поняття кіберзлочинності наголошує С.Гавриш: «кіберзлочинність – це злочинність в так званому "віртуальному просторі". Віртуальний простір (або кіберпростір) – це модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді, що перебувають в процесі руху по локальних та глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки, передачі» [7]. Такого підходу дотримуються також А.Мокляк та О.Бабенко: «кіберзлочинність – сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору. Тобто кіберзлочинність – протиправні дії особи (чи групи осіб) у кібернетичному просторі» [25].

На нашу думку з позиції наукових досліджень у різних сферах суспільного життя, кіберзлочинність можна вивчати з позиції зазначених підходів, адже кожен із них характеризує не стільки зміст кіберзлочинності, а скільки її ознаки. Ознаки кіберзлочинності можуть стати основою класифікації як підґрунтя вивчення властивостей даного суспільного явища з позиції об'єкта державного управління в цілому та державної кримінально-правової політики зокрема.

Денькович О. пропонує вирізняти такі ознаки кіберзлочинів:

– комп'ютерними називають ті кримінальні правопорушення, які законодавець об'єднав у Розділі XVI Особливої частини КК. Умовно цей підхід можна назвати позитивістським, а ознакою, яка відрізняє кіберзлочини від інших та об'єднує їх у певну групу, є родовий об'єкт цих кримінальних правопорушень;

– комп'ютерним є кримінальне правопорушення, яке вчиняється з використанням ЕОМ, телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку. Тобто, на думку цих авторів, кіберзлочин відрізняється від інших видів кримінальних правопорушень знаряддям вчинення, яким є певна комп'ютерна система, комп'ютерна мережа чи мережа електрозв'язку;

– комп'ютерним є кримінальне правопорушення, предметом якого є комп'ютерна інформація, що обробляється в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку;

– кіберзлочином є кримінальне правопорушення, в якому комп'ютер є або предметом кримінального правопорушення, або знаряддям, або способом його вчинення;

– кіберзлочини – це кримінальне правопорушення, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення;

– кіберзлочин (комп'ютерне кримінальне правопорушення) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [9].

Зазначений перелік є неповним, а тому потребує уточнення, що можливо шляхом вивчення підходів вчених до класифікації кіберзлочинів та кіберзлочинності. Питання класифікації кіберзлочинів як і власне злочинів та злочинності в цілому є досить важливим із таких позицій:

– по-перше, суспільних явищ, якими є кіберзлочини та кіберзлочинність, є вкрай важливим з позиції їх пізнання. Так класифікація є методом систематизації ознак суспільного явища, що дозволяє його пізнати як з точки зору об'єкта наукового пізнання, так і з точки зору об'єкта права, політики, економіки, державного управління, криміналістики та кримінології. У праці вітчизняного дослідника О.Ю. Довженка йдеться: «Це дає змогу встановити загальне уявлення про певну групу явищ, зіставити окремі явища та групи явищ між собою, виділити закономірності та прогнозувати можливості розвитку явищ, що розглядаються, в тому чи іншому напрямку. Отже, криміналістична класифікація дозволяє піднести розуміння об'єкта дослідження на новий рівень через проникнення до його сутності, забезпечує виявлення закономірностей, необхідних для його наукового обґрунтування та опису. Водночас вона дає змогу виявити малодосліджені та непізнані сторони системи, що розглядається, та слугує необхідною ланкою в розслідуванні протиправних діянь» [12];

– по-друге, якісна класифікація кіберзлочинів та їх наслідків є основою формування статистики кіберзлочинності, що є вкрай важливим в контексті розвитку кримінології. «В нашій країна взагалі відсутній відокремлений статистичний облік злочинів, віднесених до категорії кіберзлочинів. Разом з тим, наявні статистичні показники не враховують деякі «традиційні» злочини, вчинені з використанням автоматизованих технологій» [34]. Облік та статистика кіберзлочинів є вкрай важливою як з позиції постійної модернізації законодавства, так і з позиції їх вивчення та протидії;

– по-третє, кіберзлочини мають сукупність властивостей, які не притаманні традиційним злочинам, а отже потребують особливого підходу до класифікації. «Такий вид злочинності набуває все більшої популярності через свою специфіку. Дані злочини є доступними, їх можна вчиняти на великій відстані від об'єкта, і найголовніше, що при проведенні слідчих дій доволі важко виявити та вилучити інформацію, яку можна розцінювати як доказ. Також не можна забувати, що це неймовірно прибутковий вид злочинної діяльності, успіх якої не потребує великого ризику» [23].

У науковій літературі сьогодні існує декілька підходів до класифікації кіберзлочинів. Розглянемо їх з позиції формування державної кримінально-правової політики протидії кіберзлочинам.

Марків С.І. вивчаючи кримінологічні особливості кіберзлочинів наводить такі класифікаційні ознаки, що представлено в таблиці 1.

Таблиця 1

Класифікація кіберзлочинів за С.І. Марків [23]

За методами скоєння	
агресивні	**неагресивні**
Кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм	Кібертероризм, погроза фізичної розправи, кіберпереслідування, кіберсталкінг, дитяча порнографія
За напрямами злочинів	
традиційні злочини, що вчиняються за допомогою комп'ютерних технологій	**нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям**
Шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації тощо	Кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кардшаринг, соціальна інженерія, мальваре, протиправний контент, рефайлінг

Представлений підхід досить вузько характеризує властивості кіберзлочинів та не повною мірою дозволяє забезпечити системність і комплексність дослідження даного суспільного явища. Зокрема, потребує як розширення за методами, результатами та наслідками.

Дзюндзюк В.Б. виділяє такі види кіберзлочинів:

«– правопорушення проти конституційних прав та свобод людини та громадянина, які включають порушення недоторканності приватного життя, таємниці листування та інших повідомлень, а також порушення авторських прав;

– правопорушення проти життя та здоров'я, до яких належать рецепти виготовлення наркотичних речовин домашнім способом і їх поширення;

– правопорушення проти честі та гідності, враховуючи розповсюдження компрометуючої інформації та наклепи;

– правопорушення проти власності, зокрема кримінальні дії в сфері платіжних і банківських систем;

– правопорушення у сфері комп'ютерної інформації, які включають неправомірний доступ до інформації, створення та розповсюдження вірусів;

– правопорушення проти суспільної моралі;

– правопорушення проти безпеки держави, такі як незаконний доступ до державних секретів, що стає можливим через використання інтернету у державних структура» [10].

Голуб А. пропонує такий підхід до класифікації кіберзлочинів:

– кримінальні правопорушення у сфері комп'ютерної інформації, спрямовані проти інформаційних комп'ютерних відносин;

– кримінальні правопорушення у інформаційному комп'ютерному просторі, які впливають на відносини з реалізації прав на інформаційні ресурси;

– інші кримінальні правопорушення, характерні за умовами використання комп'ютерної інформації або її складових частин [8].

Бортнік П.Р. та Воєводін І.С. в своєму дослідженні з проблем правової природи кіберзлочинності наводять такий перелік її видів:

«– використання програм, що несуть загрозу;

– DOOS атаки (злочинець надсилає велику кількість запитів, що в результаті виводить з ладу об'єкт функціонування);

– комбінація соціальної інженерії і шкідливого коду (фішинг) – передбачає спонукання жертви до певних дій. Наприклад, відвідання сайту, натискання та вміст електронного листа, що в подальшому призводить до зараження системи;

– незаконна діяльність: домагання, поширення незаконного контенту. У цьому випадку зловмисники приховують свої сліди за допомогою анонімних профайлів, зашифрованих повідомлень та інших подібних технологій;

– незаконна діяльність з обчислювальними машинами та фінансовими апаратами» [4].

Васильковский І.І. на основі вивчення діяльності Національного банку України виділяє такі кіберзлочини:

«– банкоматне шахрайство: скімінг – виготовлення, збут та встановлення на банкомати пристроїв зчитування / копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї; використання «білого пластику» для «клонування» (підробки) платіжної картки та зняття готівки в банкоматах; Transaction Reversal Fraud – втручання в роботу банкомату при здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником; Cash Trapping – заклеювання диспенсера для привласнення зловмисником готівки, яка була списана з карткового рахунку законного держателя картки;

– шахрайство в торговельно-сервісних мережах: укладання фіктивних угод торговельного еквайрингу для обслуговування підроблених платіжних карток; викрадення реквізитів платіжних карток, у тому числі із застосуванням технічних засобів їх «клонування»; операції на суму нижче встановленого ліміту без проведення авторизації; використання втрачених/викрадених/підроблених платіжних карток;

– шахрайство в мережі Інтернет: викрадення реквізитів платіжних карток; проведення операцій із використанням викрадених реквізитів платіжних карток» [6].

У дослідженні О.Столяр міститься класифікація кіберзлочинів такого змісту:

«– злочини в сфері комп'ютерної інформації, які посягають на інформаційні комп'ютерні відносини, тобто стосунки, що виникають із приводу здійснення інформаційних процесів виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, поширення та споживання комп'ютерної інформації, створення і використання комп'ютерних технологій, і засобів їх забезпечення, а також захисту комп'ютерної інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації;

– злочини в інформаційному комп'ютерному просторі, які посягають на відносини реалізації прав на інформаційні ресурси, інформаційну інфраструктуру, та її складники;

– інші злочини для яких характерне використання комп'ютерної інформації або складових її елементів, інформаційного простору під час вчинення діянь, які посягають на інші правовідносини, що охороняються кримінальним законом» [33].

Піцик Ю.М. пропонує класифікувати кіберзлочини проти власності:

– кіберзлочини проти власності, що вчиняються шляхом психологічного впливу на людину з використанням комп'ютерної та іншої аналогічної техніки (обман, введення в оману, загрози);

– кіберзлочини проти власності, що вчиняються шляхом впливу на обладнання (комп'ютери, смартфони, маршрутизатори та інше обладнання) [27].

Кундеус В.Г. вказує, що залежно від об'єкту посягання кіберзлочини (комп'ютерні злочини) можна класифікувати за такими видами:

«– злочини, вчинені у кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами КК України. Такі злочини посягають на різні об'єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права на об'єкти інтелектуальної власності, власність, господарські відносини, права та свободи тощо. Ознакою віднесення цих злочинів до кіберзлочинів є те, що вони вчиняються з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. Наприклад: викрадення реквізитів платіжних карток (фішинг, вішинг, шимінг, скімінг); незаконні фінансові операції з використанням платіжних карток або їх реквізитів, які не ініційовані або не підтверджені її власником (кардинг); заволодіння коштами через фіктивні інтернет-магазини, інтернет-аукціони, сайти та інші засоби телекомунікації (онлайн-шахрайство); порушення авторського права і суміжних прав шляхом незаконного розповсюдження програмних продуктів через комп'ютерні мережі (піратство) тощо;

– злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що передбачені Розділом XVI КК України. Ознакою зарахування цих злочинів до комп'ютерних є те, що вони посягають на відносини, що виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [22].

Довженко О.Ю. пропонує класифікувати кіберзлочини для криміналістичних цілей таким чином:

«– злочини проти конституційних прав і свобод людини і громадянина. До них можна віднести порушення права на особисте та сімейне життя, порушення таємниці листування, порушення авторських і суміжних прав, що скоюються за допомогою комп'ютерних технологій чи мережі "Інтернет";

– злочини проти життя та здоров'я населення, зокрема використання мережі "Інтернет" для розповсюдження заборонених чи обмежених у обігу речовин, таких як наркотики, психотропні речовини, ліки;

– злочини проти честі та гідності особи. До них можна віднести використання комп'ютерних технологій та мережі "Інтернет" для розповсюдження відомостей, що порочать честь та гідність особи;

– злочини проти власності. До них можна віднести викрадення грошових коштів з банківських рахунків, шахрайство та інші корисливі злочини, що ставлять за мету заволодіти власністю іншої особи з використанням комп'ютерних технологій і мережі "Інтернет";

– злочини в сфері комп'ютерної інформації, зокрема неправомірний доступ до інформації, а також створення та використання шкідливих комп'ютерних програм;

– злочини проти суспільної моралі (найбільш відомим прикладом є виготовлення, зберігання й поширення порнографії, в тому числі дитячої);

– злочини проти безпеки держави, в тому числі проти державної таємниці, скоєні з використанням комп'ютерних технологій чи мережі "Інтернет";

– злочини терористичного характеру, зокрема заклики до тероризму, фінансування тероризму та безпосередньо акти кібертероризму» [12].

Пфо О.М. пропонує класифікувати кіберзлочини в банківській сфері та виокремлює такі їх види:

«– шахрайство в мережі "Інтернет", зокрема: створення "фінансових пірамід" в мережі "Інтернет"; шахрайство при продажу товарів (послуг) через інтернет або на інтернет-аукціонах; діяльність по створенню програмних засобів з метою розкрадання фінансової, комерційної або персональної інформації (створення фіктивних вебсайтів, поширення комп'ютерних вірусів і троянських програм, перехоплення трафіку тощо);

– шахрайство в системах дистанційного банківського обслуговування (далі – ДБО), зокрема: створення комп'ютерних вірусів і троянських програм для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням ДБО; відкриття рахунків, проведення несанкціонованих операцій і отримання готівкових коштів у результаті несанкціонованих операцій у системах ДБО; отримання платежів від іноземних відправників через міжнародну систему SWIFT внаслідок втручання в роботу комп'ютерів і систем ДБО клієнтів іноземних банківських установ;

– підробка платіжних карток і банкоматне шахрайство, зокрема: використання втрачених / викрадених / підроблених платіжних карток; викрадення реквізитів платіжних карт, у тому числі із застосуванням технічних засобів їх "клонування"; скімінг – виготовлення, збут і установка на банкомати пристроїв читання / копіювання інформації з магнітної смуги платіжної карти та отримання ПІН-коду до неї; використання «білого пластику» для «клонування» (підробки) платіжної картки та зняття готівки в банкоматах; Transaction Reversal Fraud – втручання в роботу банкомату при здійсненні операцій видачі готівки, яка залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником; Cash Trapping – заклеювання диспенсера для присвоєння зловмисником готівки, яка була списана з карткового рахунки законного держателя картки» [30].

Савчук Н.В. наводить рейтинг десяти найбільш суттєвих кіберзлочинів:

– фальшові рахунки на оплату з інтернет-магазину (підроблені рахунки, які розсилаються електронною поштою, містять посилання на шкідливі програми);

– фальшиві повідомлення про доставку товару (злочинці часто видають себе за популярні поштові служби та розсилають листи, які під прикриттям повідомлення містять віруси);

– фішинг – заволодіння платіжними особистими даними користувачів шляхом обману на шахрайське їх використання, що пов'язано із електронною комерцією;

– компроментування популярних вебсайтів (кіберзлочинці атакують ті сайти, які відвідує найбільша кількість користувачів);

– крадіжка особистих даних через фальшиве анкетування (користувачі, які люблять заповнювати різного роду анкети в обмін на різні подарунки, потрапляють до групи ризику);

– відновлення результатів пошукових запитів (користувачам розсилаються посилання на вебсайти, при використанні яких комп'ютер отримує вірус, що призводить значних збитків);

– вірусна реклама;

– небезпечні привітальні листівки;

– підроблені сайти благодійних фондів;

– шахрайство на розпродажу (відвідавши сайт користувачі, клікнушви по банерній рекламі дешевого мобільного телефону, стають жертвами програми – троянський кінь) [32].

Переважно зазначенні вище підходи характеризується як перелік кіберзлочинів, а тому як класифікація не може бути застосований. Зокрема, окремі види характеризуються як наслідки, інші – як методи скоєння злочинів. Тобто не має можливості ідентифікувати властивості, які мають стати підґрунтям розвитку кримінального законодавства з одного боку та державної кримінально-правової політики з іншого. Це обумовлено насамперед відсутністю комплексного розуміння змісту, а також різновекторністю та міждисциплінарністю кіберзлочинів як об'єкта державного управління.

Досить цікавий підхід до групування кіберзлочинів міститься в науковому дослідженні зарубіжних вчених Dr. Mike McGuire and Samantha Dowling [37], зокрема автори пропонують вирізняти:

– кіберзалежні – це злочини, які вчиняються з використанням комп'ютерів, комп'ютерних мереж чи інших комунікаційних форм (поширення вірусів та інших шкідливих програм, хакерство, зламування

серверів для захоплення мережевої інфраструктури або вебсторінок). Такі злочини спрямовані на пошкодження комп'ютерів та джерел мережі, мають наслідки у вигляді, наприклад, шахрайства;

– кіберутворюючі злочини – це традиційні види злочинів, які стали кіберзлочинами через використання комп'ютерів, комп'ютерних мереж та інших видів комунікації. На відміну від кіберзалежних, вони можуть вчинятися і без застосування «комп'ютерного елементу» [37].

Денькович О. пропонує класифікувати кіберзлочини за двома типами:

«– кіберзлочини у власному розумінні, тобто ті, які неможливо вчинити без використання інформаційних (комп'ютерних) систем. Це прояви кримінально протиправної поведінки, які спрямовані проти інформаційних (комп'ютерних) систем або проти об'єктів чи предметів, які існують, зберігаються, передаються, обробляються у них (комп'ютерні програми, інформація тощо);

– пов'язані з інформаційними (комп'ютерними) системами кримінальні правопорушення, тобто ті, прояви кримінально протиправної поведінки, які вчиняються з використанням цих систем, але водночас можуть вчинятися і без них. Ці прояви кримінально протиправної поведінки можуть полягати, зокрема, у тому, що саме кримінально протиправне діяння вчиняється у кіберпросторі з використанням інформаційних технологій або ж інформаційні технології чи кіберпростір використовуються злочинцем на інших етапах реалізації кримінально протиправної діяльності як, наприклад, знаряддя чи засіб вчинення діяння» [9].

Комплексний підхід до аналізу положень Кримінального кодексу України на предмет встановлення кримінальної відповідальності міститься в науковому дослідженні В.Г. Хахановського та В.Д. Гавловського [35]. Зокрема, авторами обґрунтовано можливість визначати як кіберзлочини кримінальні правопорушення, що визначені такими статтями Кримінального кодексу України:

– дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України);

– посягання на територіальну цілісність і недоторканність України (ст. 110);

– державна зрада (ст. 111);

– диверсія (ст. 113);

– шпигунство (ст. 114);

– розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132);

– незаконне розголошення лікарської таємниці (ст. 145);

– надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (ч. 1 ст. 158);

– порушення таємниці голосування (ст. 159);

– порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через інтернет) (ст. 161);

– порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163);

– розголошення таємниці усиновлення (удочеріння) (ст. 168);

– порушення недоторканності приватного життя (ст. 182);

– розголошення комерційної або банківської таємниці (ст. 232);

– завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259);

– незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (в частині збуту через інтернет) (ст. 263);

– заклики до вчинення дій, що загрожують громадському порядку (ст. 295);

– ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300);

– сутенерство або втягнення особи в заняття проституцією (ст. 303);

– незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307);

– викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через інтернет) (ст. 312);

– викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (в частині збуту через інтернет) (ст. 313);

– розголошення державної таємниці (ст. 328);

– передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330);

– погроза або насильство щодо працівника правоохоронного органу (ст. 345);

– погроза або насильство щодо журналіста (ст. 345–1);

– погроза або насильство щодо державного чи громадського діяча (ч. 1 ст. 346);

– погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (ч. 1 ст. 350);

– незаконне втручання в роботу автоматизованої системи документообігу суду (ч. 1 ст. 376);

– розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381);

– розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387);

– погроза або насильство щодо захисника чи представника особи (ч. 1 ст. 398);

– розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422);

– пропаганда війни (ст. 436);

– виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 4361) [35].

У системі нормативно-правового регулювання класифікація та виділення типів і видів кіберзлочинів міститься в міжнародних нормативно-правових актах. Зокрема в Конвенції Ради Європи про кіберзлочинність [19] вирізняють чотири групи злочинів (табл. 2).

Таблиця 2

Види кіберзлочинів, що містяться в Конвенції Ради Європи про кіберзлочинність [13]

Група	Вид кіберзлочину	Характеристика
Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем	*Незаконний доступ*	Навмисний доступ до цілої комп'ютерної системи або її частини без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою
	Нелегальне перехоплення	Протиправне перехоплення технічними засобами комп'ютерних даних
	Втручання в дані	Навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це
	Втручання в систему	Навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це
	Зловживання пристроями	А саме: їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином
Правопорушення, пов'язані з комп'ютерами	*Підробка, пов'язана з комп'ютерами*	Введення, зміна, знищення або приховування комп'ютерних даних, що призводить до створення недійсних даних з метою, щоб вони розглядалися, наче справжні, незалежно від того, можна чи ні їх прочитати чи зрозуміти
	Шахрайство з використанням комп'ютерів	Позбавлення іншої особи її власності шляхом введення, зміни, знищення чи приховування комп'ютерних даних або втручання у функціонування комп'ютерної системи
Правопорушення, пов'язані зі змістом (інформацією)	*Правопорушення, пов'язані з дитячою порнографією*	Вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації
Правопорушення, пов'язані з порушенням авторських і суміжних прав відповідно до чинних міжнародних угод		

Підводячи підсумок аналізу наукових джерел на предмет класифікації кіберзлочинності, варто наголосити на таких критичних моментах:

– кіберзлочинність характеризується розгалуженістю ознак та сферами впливу і наслідками, які в жодному разі не відображено в досліджених класифікаціях;

– класифікація кіберзлочинності не може бути сталою, що можливо пояснити постійним розвитком інформаційно-комп'ютерних технологій, а отже методів скоєння злочинів у кібернетичному просторі;

– представлені класифікації переважно визначалися технічними та технологічними особливостям, а також для цілей кримінології, а в окремих випадках криміналістики.

Для вирішення зазначеного пропонуємо такий підхід до класифікації кіберзлочинності (табл. 3).

Таблиця 3

Класифікація кіберзлочинності для цілей державної кримінально-правової політики

ЗАГАЛЬНІ ПІДХОДИ			
За обсягами наслідків			
– проти особистості	– проти інституції	– проти держави	– проти міжнародних відносин
За метою скоєння кіберзлочину			
– особисті	– економічні	– політичні	– релігійні
– психологічні	– націоналістичні	– без мети	– інші
За сукупністю осіб, задіяних в скоєнні злочину			
– особа	– держава		– група осіб
– транскордонне злочинне угрупування		– організоване злочинне угрупування	
За особою злочинця			
– замовник		– посередник	
– виконавиць		– підбурювач	
ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ, СИСТЕМИ ТА ІНФОРМАЦІЯ ЯК ОБ'ЄКТ ПОСЯГАННЯ			
Кіберзлочини, що пов'язані з поводженням зі шкідливими програмними продуктами			
– виготовлення шкідливих програмних продуктів	– фінансування виготовлення шкідливих програмних продуктів	– реалізація шкідливих програмних продуктів	– обмін шкідливий програмними продуктами
Втручання в функціонування інформаційних систем			
– фізичне втручання	– віртуальне втручання		– комбіноване втручання
За обсягами технічних наслідків			
– проти окремого комп'ютера	– проти локальної системи	– проти глобальної системи	– проти програмного продукту
За поводженням з інформацією			
– зміна та підробка інформації	– перехоплення інформації		– втручання в дані
– незаконний доступ до інформації	– утворення неправдивої інформації		– розповсюдження незаконно здобутої інформації
ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ СКОЄННЯ ЗЛОЧИНУ			
За об'єктом посягання			
– проти безпеки руху та експлуатації транспорту	– проти громадського порядку та моральності	– проти охорони державної таємниці	– проти статевої свободи та статевої недоторканності
– проти виборчих, трудових та інших особистих прав та свобод людини і громадянина	– проти органів державної влади, місцевого самоврядування, об'єднань громадян		– проти миру, безпеки людства та міжнародного правопорядку
– проти громадської безпеки	– проти безпеки виробництва	– проти життя та здоров'я особи	– проти господарської діяльності
– проти національної безпеки	– проти державних кордонів	– проти волі, честі та гідності	– проти службової діяльності
– проти правосуддя	– проти військової служби	– проти довкілля	– проти власності
За видами наслідків			
– економічні	– соціальні	– політичні	– інфраструктурні	– інші
За впливом на рівні безпеки			
– інфраструктурна	– державна	– регіональна	– глобальна
За впливом на види національної безпеки			
– інформаційна	– економічна	– енергетична	– продовольча
– соціальна	– воєнна	– екологічна	– політична

Представлена класифікаціє має багаторівневий характер, адже визначає групи класифікаційних ознак, зокрема: загальні підходи до класифікації кіберзлочинів; інформаційно-комп'ютерні технології, системи та інформація як об'єкт посягання; інформаційно-комп'ютерні технології як засіб скоєння злочину. До загальних класифікаційних ознак належить: за обсягами наслідків (проти особисті, проти інституції,

проти держави, проти міжнародних відносин); за метою скоєння кіберзлочину (особисті, економічні, політичні, релігійні, психологічні, націоналістичні, без мети, інші); за сукупністю осіб, задіяних в скоєнні злочину (особа, держава, група осіб, транскордонне злочинне угрупування, організоване злочинне угрупування); за особою злочинця (замовник, посередник, виконавиць, підбурювач). Інформаційно-комп'ютерні технології, системи та інформація як об'єкт посягання визначають такі класифікаційні ознаки: кіберзлочини, що пов'язані з поводженням зі шкідливими програмними продуктами (виготовлення шкідливих програмних продуктів, фінансування виготовлення шкідливих програмних продуктів, реалізація шкідливих програмних продуктів, обмін шкідливий програмними продуктами); втручання в функціонування інформаційних систем (фізичне втручання, віртуальне втручання, комбіноване втручання); за обсягами технічних наслідків (проти окремого комп'ютера, проти локальної системи, проти глобальної системи, проти програмного продукту); за поводженням з інформацією (зміна та підробка інформації, перехоплення інформації, втручання в дані, незаконний доступ до інформації, утворення неправдивою інформації, розповсюдження незаконно здобутої інформації). Інформаційно-комп'ютерні технології як засіб скоєння злочину передбачають такі класифікаційні ознаки кіберзлочинності: за об'єктом посягання (проти безпеки руху та експлуатації транспорту; проти громадського порядку та моральності; проти охорони державної таємниці; проти статевої свободи та статевої недоторканності; проти виборчих, трудових та інших особистих прав та свобод людини і громадянина; проти органів державної влади, місцевого самоврядування, об'єднань громадян; проти миру, безпеки людства та міжнародного правопорядку; проти громадської безпеки; проти безпеки виробництва; проти життя та здоров'я особи; проти господарської діяльності; проти національної безпеки; проти державних кордонів; проти волі, честі та гідності; проти службової діяльності; проти правосуддя; проти військової служби; проти довкілля; проти власності); за видами наслідків (економічні, соціальні, політичні, інфраструктурні, інші); за впливом на рівні безпеки (інфраструктурна, державна, регіональна, глобальна); за впливом на види національної безпеки (інформаційна, економічна, енергетична, продовольча, соціальна, воєнна, екологічна, політична).

Відповідно до зазначеного та зважаючи на підходи вітчизняних вчених до ознак та змісту кіберзлочинності, вважаємо, що цей вид злочину варто розглядати з таких позицій:

– суспільно небезпечне винне діяння, що полягає у виготовленні, фінансуванні, використанні, реалізації, обміні та розповсюдженні шкідливих програмних продуктів (як на матеріальних, так і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивої інформації, розповсюдження незаконно здобутої інформації, та інших дій, що заборонено кримінальним законодавством України;

– суспільно небезпечне винне діяння, що скоєне з використанням інформаційно-комп'ютерних технологій проти особи, підприємства, органу державної влади, держави, міжнародних організацій, органів державного управління інших держав, що призводить до сукупності негативних наслідків економічного, соціального, політичного, інфраструктурного та іншого характеру та становить загрозу інформаційній, економічній, соціальній, продовольчій, енергетичній, воєнній, екологічній та політичній безпекам.

Відповідно до зазначеного кіберзлочинність є об'єктом державного управління за таких позицій:

– по-перше, формування правового поля використання інформації функціонування джерел його утворення, зберігання, розповсюдження, обміну;

– по-друге, формування системи регулювання виробництва, використання, реалізації та обміну інформаційними технологіями, системами та їх елементами;

– по-третє, модернізації кримінального законодавства на предмет протидії кіберзлочинності, встановлення кримінальної відповідальності та інше;

– по-четверте, формування суб'єктної структури державного управління в сфері протидії кіберзлочинності;

– по-п'яте, активізація діяльності в сфері міжнародної співпраці щодо протидії кіберзлочинності.

Висновки. Проведене дослідження дозволило сформувати сукупність теоретичних положень, що є підґрунтям формування та реалізації державної кримінально-правової політики протидії кіберзлочинності. Зокрема, розроблено багаторівневу класифікацію, що дозволило виявити більшість ознак кіберзлочинності як з позиції права, криміналістики, кримінології, так і з позиції державного управління та державної політики. Обґрунтовано необхідність двох підходів до тлумачення кіберзлочинності, а саме: 1) суспільно небезпечне винне діяння, що полягає у виготовленні, фінансуванні, використанні, реалізації, обміні та розповсюдженні шкідливих програмних продуктів (як на матеріальних, так і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивої інформації, розповсюдження незаконно здобутої інформації та інших дій, що заборонено кримінальним законодавством України; 2) суспільно небезпечне винне діяння, що скоєне з використанням інформаційно-комп'ютерних

технологій проти особи, підприємства, органу державної влади, держави, міжнародних організацій, органів державного управління інших держав, що призводить до сукупності негативних наслідків економічного, соціального, політичного, інфраструктурного та іншого характеру та становить загрозу інформаційній, економічній, соціальній, продовольчій, енергетичній, воєнній, екологічній та політичній безпекам. Це стало основою визначених підходів до характеристики напрямів розвитку державної кримінально-правової політики: 1) формування правового поля використання інформації функціонування джерел його утворення, зберігання, розповсюдження, обміну; 2) формування системи регулювання виробництва, використання, реалізації та обміну інформаційними технологіями, системами та їх елементами; 3) модернізації кримінального законодавства на предмет протидії кіберзлочинності, встановлення кримінальної відповідальності та інше; 4) формування суб'єктної структури державного управління в сфері протидії кіберзлочинності; 5) активізація діяльності в сфері міжнародної співпраці щодо протидії кіберзлочинності.

Список використаної літератури:

1. *Бабанін С.В.* Кіберзлочинність / *С.В. Бабанін* // Вісник Асоціації кримінального права. – 2016. – № 1 (6). – С. 468–470.
2. *Бельський Ю.* Щодо визначення поняття кіберзлочину / *Ю.Бельський* // Юридичний вісник. – 2014. – № 6. – С. 414–418.
3. *Біленчук Д.П.* Кібрешахраї – хто вони? / *Д.П. Біленчук* // Міліція України. – 1999. – № 7–8. – С. 32–34.
4. *Бортнік П.Р.* Правова природа та сутність кіберзлочинності / *П.Р. Бортнік, І.С. Воєводін* // Протидія кіберзагрозам та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф., 26 лист. – Харків : ХНУВС, 2019. – С. 36–38 [Електронний ресурс]. – Режим доступу : https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/8.pdf.
5. *Буяджи С.А.* Перспективи правового регулювання боротьби з кіберзлочинністю в Україні / *С.А. Буяджи* // Право України. – 2017. – № 9. – С. 245–251 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/prukr_2017_9_28.
6. *Васильковский І.І.* Поняття, класифікація та характеристика окремих видів кіберзлочинів / *І.І. Васильковский* // Прикарпатський юридичний вісник. – 2017. – Вип. 1 (16), Т. 2. – С. 196–201 [Електронний ресурс]. – Режим доступу : http://www.pjv.nuoua.od.ua/v1-2_2017/44.pdf.
7. *Гавриш С.Б.* Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / *С.Б. Гавриш* [Електронний ресурс]. – Режим доступу : http://www.irbis-nbuv.gov.ua.
8. *Голуб А.* Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби / *А.Голуб* [Електронний ресурс]. – Режим доступу : http://www.gurt.org.ua/articles/34602.
9. *Денькович О.* Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів / *О.Денькович* // Кіберзлочинність та електронні докази : навч. посібник / *Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан* ; за ред. канд. юрид. наук, доц. *О.Денькович*, д-р права, проф. *Г.Шмельцер*. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с.
10. *Дзюндзюк В.Б.* Поява і розвиток кіберзлочинності / *В.Б. Дзюндзюк* // Державне будівництво. – 2013. – № 1 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.
11. *Діордіца І.В.* Поняття та зміст кіберзлочинності / *І.В. Діордіца* // Глобальна організація союзницького лідерства [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti.
12. *Довженко О.Ю.* Класифікація кіберзлочинів у криміналістиці / *О.Ю. Довженко* // Південноукраїнський правничий часопис. – 2019. – № 1. – С. 19–22 [Електронний ресурс]. – Режим доступу : http://www.sulj.oduvs.od.ua/archive/2019/1/7.pdf.
13. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Протокол Ради Європи від 28.01.2003 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/994_687#Text.
14. *Думчиков М.О.* Кримінально-правова характеристика поняття та видів кіберзлочинів / *М.О. Думчиков* // Науковий вісник Міжнародного гуманітарного університету. Сер. : Юриспруденція. – 2022. – № 55. – С. 65–68.
15. *Загуменний О.О.* Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини» / *О.О. Загуменний* // Процесуальне та техніко-криміналістичне забезпечення досудового розслідування. – Харків, 2019. – С. 67–69.
16. *Іванченко О.Ю.* Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні / *О.Ю. Іванченко* // Актуальні проблеми вітчизняної юриспруденції. – 2016. – Вип. 3. – С. 172–177.
17. *Карчевський Н.В.* Кіберзлочин чи злочин у сфері використання інформаційних технологій / *Н.В. Карчевський* // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., 21 жовтня. – Одеса, 2016. – С. 10–15.
18. *Ковальчук А.Ю.* Кіберзлочини як загроза державній безпеці: кримінологічні та організаційні особливості обліку / *А.Ю. Ковальчук* // Інформація і право. – 2023. – № 4. – С. 187–196 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/ UJRN/Infpr_2023_4_20.
19. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/994_575.
20. *Копан О.В.* Словник термінів з кібербезпеки / *О.В. Копан*. – К. : Аванпост-Прим, 2012. – 214 с.
21. *Кравцова М.О.* Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08 / *М.О. Кравцова*. – Харків, 2016. – 16 с.

22. *Кундеус В.Г.* Поняття та види кіберзлочинів / *В.Г. Кундеус* // Держава і злочинність. Нові виклики в епоху постмодерну : зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака, 23 квіт. – Харків : ХНУВС, 2019. – С. 44–45 [Електронний ресурс]. – Режим доступу : https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content.
23. *Марків С.І.* Кіберзлочинність. Нова кримінальна загроза / *С.І. Марків* // Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід : матеріали II Міжнар. наук.-практ. конф. – Тернопіль : Економічна думка, 2017. – С. 360–362 [Електронний ресурс]. – Режим доступу : http://dspace.wunu.edu.ua/bitstream/ 316497/21460/1/360-362.pdf.
24. *Матвійчук М.П.* Кіберзлочини: поняття та види / *М.П. Матвійчук* // Кримінальне право в умовах глобалізації : матер. Міжнар. наук.-практ. конфер., 25 травня. – Одеса : НУ «Одеська юридична академія», кафедра кримінального права, 2018. – С. 236–238.
25. *Мокляк А.* Теоретичний аналіз дослідження психологічного портрета кіберзлочинця / *А.Мокляк, О.Бабенко* // Теорія та практика сучасної психології. – 2018. – № 2. – С. 89–93.
26. *Пивоваров В.В.* Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання / *В.В. Пивоваров, С.Ю. Лисенко* // Право і суспільство. – 2016. – № 3 (2). – С. 177–182 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/ Pis_2016_3%282%29__32.
27. *Піцик Ю.М.* Класифікація кіберзлочинів проти власності / *Ю.М. Піцик* // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. – 2017. – Вип. 30 (2). – С. 65–68 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_30%282%29__18.
28. *Погорецький М.А.* Кіберзлочини: до визначення поняття / *М.А. Погорецький* // Вісник прокуратури. – 2012. – № 8. – С. 89–96.
29. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII ; станом на 28 черв. 2024 р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.
30. *Пфо О.М.* Основні поняття і класифікація кіберзлочинності / *О.М. Пфо* // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., 23–25 листоп. – Кропивницький : КНТУ, 2016. – С. 33–34 [Електронний ресурс]. – Режим доступу : https://core.ac.uk/download/pdf/84825482.pd.
31. *Русецький А.А.* Теоретико-правовий аналіз понять кіберзлочин і кіберзлочинність / *А.А. Русецький, Д.А. Куцолабський* // Право і безпека. – 2017. – № 1 (64). – С. 74–75.
32. *Савчук Н.В.* Кіберзлочинність: зміст та методи боротьби / *Н.В. Савчук* [Електронний ресурс]. – Режим доступу : http://tppe.econom.univ.kiev.ua/ data/2009_19/zb19_48.pdf.
33. *Столяр О.* Міжнародно-правові проблеми визначення та класифікації «кіберзлочинів» / *О.Столяр* // Jurnalul juridic naţional: teorie şi practică. – 2017. – № 4. – С. 190–193 [Електронний ресурс]. – Режим доступу : http://www.jurnaluljuridic.in.ua/ archive/2017/4/43.pdf.
34. *Фоменко О.В.* Кіберзлочинність: сучасний стан та особливості віктимологічної профілактики / *О.В. Фоменко* // Юридичний науковий електронний журнал. – 2017. – № 6. – С. 328–330 [Електронний ресурс]. – Режим доступу : http://lsej.org.ua/6_2017/97.pdf.
35. *Хахановський В.Г.* Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів / *В.Г. Хахановський, В.Д. Гавловський* // Інформація і право. – 2020. – № 2 (33). – С. 99–109.
36. *Шемчук В.В.* Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні / *В.В. Шемчук* // Вчені записки ТНУ імені В.І. Вернадського. Серія : Юридичні науки. – 2018. – № 6. – Т. 29 (68). – С. 119–124 [Електронний ресурс]. – Режим доступу : https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf.
37. *McGuire M.* Cybercrime: A review of the evidence Summary of key findings and implications : Home Office Research Report 75 / *M.McGuire, S.Dowling*. – University of Surrey, 2013. – October. – 29 p.

References:

1. Babanin, S.V. (2016), «Kiberzlochynnist», *Visnyk Asotsiatsii kryminalnoho prava*, No. 1 (6), pp. 468–470.
2. Belskyi, Yu. (2014), «Shchodo vyznachennia poniattia kiberzlochynu», *Yurydychnyi visnyk*, No. 6, pp. 414–418.
3. Bilenchuk, D.P. (1999), «Kibreshakhrai – khto vony?», *Militsiia Ukrainy*, No. 7–8, pp. 32–34.
4. Bortnik, P.R. and Voievodin, I.S. (2019), «Pravova pryroda ta sutnist kiberzlochynnosti», *Protydiia kiberzahrozam ta torhivli liudmy*, zb. materialiv Mizhnar. nauk.-prakt. konf., 26 lyst., KhNUVS, Kharkiv, pp. 36–38, [Online], available at: https://univd.edu.ua/general/publishing/konf/ 26_11_2019/pdf/8.pdf
5. Buiadzhy, S.A. (2017), «Perspektyvy pravovoho rehuliuvannia borotby z kiberzlochynnistiu v Ukraini», *Pravo Ukrainy*, No. 9, pp. 245–251, [Online], available at: http://nbuv.gov.ua/UJRN/prukr_2017_9_28
6. Vasylkovskyi, I.I. (2017), «Poniattia, klasyfikatsiia ta kharakterystyka okremykh vydiv kiberzlochyniv», *Prykarpatskyi yurydychnyi visnyk*, Issue 1 (16), Vol. 2, pp. 196–201, [Online], available at: http://www.pjv.nuoua.od.ua/v1-2_2017/44.pdf
7. Havrysh, S.B., «Kompiuternyi teroryzm: suchasnyi stan, prohnozy rozvytku ta shliakhy protydii», [Online], available at: http://www.irbis-nbuv.gov.ua
8. Holub, A., «Kiberzlochynnist u vsikh yii proiavakh: vydy, naslidky ta sposoby borotby», [Online], available at: http://www.gurt.org.ua/articles/34602
9. Denkovych, O. (2022), «Poniattia kiberzlochynnosti ta yii mistse v zahalnii strukturi zlochynnosti. Vydy kiberzlochyniv», Holovkin, B.M., Denkovych, O.I., Lutsyk, V.V. and Tsekhan, D.M., in kand. yuryd. nauk, dots. Denkovych, O. and d-r prava, prof. Shmeltser, H. (ed.), *Kiberzlochynnist ta elektronni dokazy*, navch. posibnyk, LNU im. Ivana Franka, Lviv, 298 p.

10. Dziundziuk, V.B. (2013), «Poiava i rozvytok kiberzlochynnosti», *Derzhavne budivnytstvo*, No. 1, [Online], available at: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3
11. Diorditsa, I.V., «Poniattia ta zmist kiberzlochynnosti», Hlobalna orhanizatsiia soiuznytskoho liderstva, [Online], available at: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti
12. Dovzhenko, O.Yu. (2019), «Klasyfikatsiia kiberzlochyniv u kryminalistytsi», *Pivdennoukrainskyi pravnychyi chasopys*, No. 1, pp. 19–22, [Online], available at: http://www.sulj.oduvs.od.ua/archive/2019/1/7.pdf
13. Rada Yevropy (2003), *Dodatkovyi protokol do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy*, Protokol vid 28.01.2003, [Online], available at: https://zakon.rada.gov.ua/laws/show/994_687#Text
14. Dumchykov, M.O. (2022), «Kryminalno-pravova kharakterystyka poniattia ta vydiv kiberzlochyniv», *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*. Ser. *Yurysprudentsiia*, No. 55, pp. 65–68.
15. Zahumennyi, O.O. (2019), «Spivvidnoshennia poniat "kiberzlochynnist" i "kompiuterni zlochyny"», *Protsesualne ta tekhniko-kryminalistychne zabezpechennia dosudovoho rozsliduvannia*, Kharkiv, pp. 67–69.
16. Ivanchenko, O.Yu. (2016), «Kryminolohichna kharakterystyka kiberzlochynnosti, zapobihannia kiberzlochynnosti na natsionalnomu rivni», *Aktualni problemy vitchyznianoi yurysprudentsi*, Issue 3, pp. 172–177.
17. Karchevskyi, N.V. (2016), «Kiberzlochyn chy zlochyn u sferi vykorystannia informatsiinykh tekhnolohii», *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia*, materialy vseukr. nauk.-prakt. konf., 21 zhovtnia, Odesa, pp. 10–15.
18. Kovalchuk, A.Yu. (2023), «Kiberzlochyny yak zahroza derzhavnii bezpetsi: kryminolohichni ta orhanizatsiini osoblyvosti obliku», *Informatsiia i pravo*, No. 4, pp. 187–196, [Online], available at: http://nbuv.gov.ua/UJRN/Infpr_2023_4_20
19. Rada Yevropy (2001), *Konventsiia pro kiberzlochynnist*, Konventsiia vid 23.11.2001, [Online], available at: https://zakon.rada.gov.ua/laws/show/994_575
20. Kopan, O.V. (2012), *Slovnyk terminiv z kiberbezpeky*, Avanpost-Prym, K., 214 p.
21. Kravtsova, M.O. (2016), «Kiberzlochynnist: kryminolohichna kharakterystyka ta zapobihannia orhanamy vnutrishnikh sprav», Abstract of Ph.D. dissertation, 12.00.08, Kharkiv, 16 p.
22. Kundeus, V.H. (2019), «Poniattia ta vydy kiberzlochyniv», *Derzhava i zlochynnist. Novi vyklyky v epokhu postmodernu*, zb. tez dop. nauk.-prakt. konf., prysviach. pamiati vitse-prezydenta Kryminolohichnoi asotsiatsii Ukrainy, profesora O.M. Lytvaka, 23 kvit., KhNUVS, Kharkiv, pp. 44–45, [Online], available at: https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content
23. Markiv, S.I. (2017), «Kiberzlochynnist. Nova kryminalna zahroza», *Ukraina v umovakh reformuvannia pravovoi systemy: suchasni realii ta mizhnarodnyi dosvid*, materialy II Mizhnar. nauk.-prakt. konf., Ekonomichna dumka, Ternopil, pp. 360–362, [Online], available at: http://dspace.wunu.edu.ua/bitstream/ 316497/21460/1/360-362.pdf
24. Matviichuk, M.P. (2018), «Kiberzlochyny: poniattia ta vydy», *Kryminalne pravo v umovakh hlobalizatsii*, mater. Mizhnar. nauk.-prakt. konfer., 25 travnia, NU «Odeska yurydychna akademiia», kafedra kryminalnoho prava, Odesa, pp. 236–238.
25. Mokliak, A. and Babenko, O. (2018), «Teoretychnyi analiz doslidzhennia psykholohichnoho portreta kibezlochyntsia», *Teoriia ta praktyka suchasnoi psykholohii*, No. 2, pp. 89–93.
26. Pyvovarov, V.V. and Lysenko, S.Yu. (2016), «Kiberzlochynnist: kryminolohichnyi pohliad na henezys yavyshcha ta shliakhy zapobihannia», *Pravo i suspilstvo*, No. 3 (2), pp. 177–182, [Online], available at: http://nbuv.gov.ua/UJRN/ Pis_2016_3%282%29__32
27. Pitsyk, Yu.M. (2017), «Klasyfikatsiia kiberzlochyniv proty vlasnosti», *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*. Seriia. *Yurysprudentsiia*, Issue 30 (2), pp. 65–68, [Online], available at: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_30%282%29__18
28. Pohoretskyi, M.A. (2012), «Kiberzlochyny: do vyznachennia poniattia», *Visnyk prokuratury*, No. 8, pp. 89–96.
29. Verkhovna Rada Ukrainy (2024), *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy*, Zakon Ukrainy vid 05.10.2017 No. 2163-VIII, stanom na 28 cherv. 2024 r., [Online], available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text
30. Pfo, O.M. (2016), «Osnovni poniattia i klasyfikatsiia kiberzlochynnosti», *Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky*, materialy Vseukr. nauk.-prakt. konf., 23–25 lystop., KNTU, Kropyvnytskyi, pp. 33–34, [Online], available at: https://core.ac.uk/download/pdf/84825482.pdf
31. Rusetskyi, A.A. and Kutsolabskyi, D.A. (2017), «Teoretyko-pravovyi analiz poniat kiberzlochyn i kiberzlochynnist», *Pravo i bezpeka*, No. 1 (64), pp. 74–75.
32. Savchuk, N.V., «Kiberzlochynnist: zmist ta metody borotby», [Online], available at: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf
33. Stoliar, O. (2017), «Mizhnarodno-pravovi problemy vyznachennia ta klasyfikatsii "kiberzlochyniv"», *Jurnalul juridic naţional: teorie şi practică*, No. 4, pp. 190–193, [Online], available at: http://www.jurnaluljuridic.in.ua/archive/2017/4/43.pdf
34. Fomenko, O.V. (2017), «Kiberzlochynnist: suchasnyi stan ta osoblyvosti viktymolohichnoi profilaktyky», *Yurydychnyi naukovyi elektronnyi zhurnal*, No. 6, pp. 328–330, [Online], available at: http://lsej.org.ua/6_2017/97.pdf
35. Khakhanovskyi, V.H. and Havlovskyi, V.D. (2020), «Tlumachennia ta klasyfikatsiia kryminalnykh pravoporushen yak kiberzlochyniv», *Informatsiia i pravo*, No. 2 (33), pp. 99–109.
36. Shemchuk, V.V. (2018), «Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini», *Vcheni zapysky TNU imeni V.I. Vernadskoho*. Seriia. *Yurydychni nauky*, No. 6, Vol. 29 (68), pp. 119–124, [Online], available at: https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf
37. McGuire, M. and Dowling, S. (2013), *Cybercrime: A review of the evidence Summary of key findings and implications*, Home Office Research Report 75, University of Surrey, October, 29 p.

Корзун Світлана Вікторівна – аспірантка Державного університету «Житомирська політехніка».
Наукові інтереси:
– протидія кіберзлочинності.

Korzun S.V.

Conceptual and categorical apparatus of the state criminal and legal policy of countering cybercrimes

The article comprehensively examines the formation and genesis of the conceptual and categorical apparatus of the state criminal and legal policy of countering cybercrimes. Given the growing global threat of cybercrime, the most effective are criminal means of combating it, which is why the clarification of the conceptual and categorical apparatus is extremely relevant.

Having analyzed the scientific achievements of previous years, we have come to an understanding of the concepts of «cybercrime», «cybercrime» through the prism of multi-vectority, using various approaches, including considering international and national legislation. Special attention in the article is devoted to the identification of signs of cybercrimes and their classification, in particular, examples of classifications of various scientists are given. The types of cybercrimes contained in the Council of Europe Convention on Cybercrime are comprehensively characterized. Based on the processed material, our own approaches to the classification of cybercrime for the purposes of state criminal and legal policy, which has a multi-level nature, have been developed.

Regarding the identified approaches to the classification, signs and content of cybercrime, certain positions have been highlighted regarding the consideration of these crimes: first, as a socially dangerous criminal act consisting in the manufacture, financing, use, sale, exchange and distribution of malicious software products; second, as a socially dangerous criminal act committed with the use of information and computer technologies.

The presented study consists in the analysis of the conceptual and categorical apparatus of the state criminal law policy to combat cybercrime, which allowed to form a set of theoretical provisions and is the basis for the formation and implementation of the state criminal law policy to combat cybercrime.

Keywords: state policy; cybercrime; cyberspace; combating cybercrime.

Стаття надійшла до редакції 10.02.2025.