УДК 343:973

І. І. Васильковский
аспірант кафедри кримінального права,
процесу та криміналістики
ПВНЗ «Європейський університет»

ПОНЯТТЯ, КЛАСИФІКАЦІЯ ТА ХАРАКТЕРИСТИКА ОКРЕМИХ ВИДІВ КІБЕРЗЛОЧИНІВ

Кіберзлочини в Україні світі мають швидку динаміку розвитку, їх кількість і число потерпілих від дій кіберзлочинців постійно збільшується. Але суспільство не виробило проти такого виду злочинів ефективних заходів боротьби. Слід зазначити, кіберзлочини деякі вчені трактують як різні види (групи) злочинів у сфері високих комп'ютерних технологій, класифікація яких здійснювалася за різними ознаками. При цьому ознакою для «віднесення» окремих злочинів в сфері високих технологій до комп'ютерних в загальному вигляді є знаряддя скоєння злочину – комп'ютерна техніка, а ознакою для виділення кіберзлочини – специфічне середовище скоєння злочинів – кіберпростір (середовище комп'ютерних систем і мереж) [2, с. 18]. Безумовно, якщо розглядати групу злочинів, об'єднану в окремий розділ КК України – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» у відриві від інших форм прояву злочинної поведінки з використанням комп'ютерної техніки та високих технологій, при цьому допускаючи, що вони не перебувають (не включені) в єдину мережу, то дана класифікація має сенс. Однак, ми цілком погоджуємося з думкою автора про те, що їх включеність в мережі різних рівнів і створює можливість для здійснення діянь, що характеризуються підвищеною (кримінально караною) суспільною небезпекою [10, с. 321]. Проблема кіберзлочинності, хоч і взаємопов'язана з відносно недавно виникла сферою життєдіяльності людини, в порівнянні, наприклад, з організованою або службової, однак неодноразово знаходила відображення в роботах вітчизняних і зарубіжних криміналістів. Окремі питання кримінально правової характеристики та кваліфікації злочинів у сфері комп'ютерних технологій і напрямків протидії їм розглядалися як українськими вченими: Д. С. Азаровим, П. Д. Біленчуком, В. А. Глушковим, Н. А. Гуторовою, Н. В. Карчевський, П. І. Орловим, С. А. Орловим, Н. І. Хавронюком, так і зарубіжними криміналістами: В. І. Алескеровим, В. Б. Веховим, М. А. Єфремовою, Б. Д. Завидовою, Д. А. Зиковим, С. Я. Казанцевим, В. А. Кемпф, С. П. Кушніренком, А. Я. Мініним, Ю. І. Ляпуновим, В. А. Мазуровим, В. А. Мінаєвим, В. Б. Наумовим, В. Н. Черкасовим, В. Г. Щелкуновим і ін.

Мета даної статті полягає у тому, що незважаючи на досить широке коло досліджень, окремі аспекти даної проблеми залишаються розробленими недостатньо і вимагають подальших наукових пошуків. Перш за все це стосується виділення кіберзлочинності як самостійного виду злочинності, визначення її специфічних особливостей, кола діянь, характерних для даного виду злочинних проявів, класифікації комп'ютерних злочинів і об'єктів злочинних посягань даного виду.

Завдання полягає у формуванні визначення даної категорії злочинів та виділення її характеристики. На сьогодні в українському законодавстві відсутнє визначення поняття «кіберзлочин» або «кіберзлочинність», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку, зокрема:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 КК України);

– створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 3611 КК України);

– несанкціоновані 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 (стаття 361-2 КК України);

Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима обладнанням для їх виготовлення [11].

Питання пошуку шляхів протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги міжнародної спільноти. На даний час Будапештська конвенція є фундаментом для розробки законодавства у боротьбі з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства [16].

Будапештська Конвенція вимагає від держав:

– криміналізувати атаки на комп'ютерні дані і системи (тобто незаконний доступ, неле-

гальне перехоплення, втручання в дані, втручання у систему, зловживання пристроями), а також правопорушення з використанням комп'ютерів (підробка і шахрайство), правопорушення, пов'язані зі змістом (дитяча порнографія) та правопорушення у сфері авторських і суміжних прав;

– вдосконалювати законодавство для того, щоб компетентні органи змогли проводити розслідування кіберзлочинів і зберігати електронні докази найефективніше, включаючи термінове збереження комп'ютерних даних, термінове збереження і часткове розкриття даних про рух інформації, обшук і арешт комп'ютерних даних, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації;

– розширювати міжнародне співробітництво з іншими країнами-учасницями Конвенції через загальні (екстрадиція, взаємна допомога добровільне надання інформації тощо) і спеціальні заходи (термінове збереження та розкриття збережених даних про рух інформації, взаємна допомога щодо доступу до комп'ютерних даних, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж тощо) [16].

Слід зазначити, що Будапештська Конвенція, як основоположний документ у сфері боротьби з кіберзлочинністю, надає умовну класифікацію кіберзлочинів, що поділяються на наступні категорії: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем,правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів; правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія; правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

За інформацією Національного банку України, в банківській системі України найбільш розповсюдженими є наступні види кіберзлочинів:

– банкоматне шахрайство: скіминг – 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; TransactionReversalFraud – втручання в роботу банкомату при здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником; CashTrapping – заклеювання диспенсеру для привласнення зловмисником готівки, яка була списана з карткового рахунку законного держателя картки;

– шахрайство в торгівельно-сервісних мережах: укладання фіктивних угод торговельного еквайрінгу 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 [8].

Таким чином, стрімкий розвиток інформатизації в Україні несе за собою потенційну можливість використання комп'ютерних технологій з корисливих та інших мотивів, що певною мірою ставить під загрозу національну безпеку держави [12].

Разом з поширенням впровадження сучасних інформаційних технологій в Україні постійно зростає загроза як для державних комп'ютерних систем, так і для приватних організацій та окремих громадян. Особливої актуальності проблема кіберзлочинності набула в наш час. Соціологічні опитування в різних країнах, і насамперед, у високорозвинених, показують, що кіберзлочинність посідає одне з чільних місць серед тих проблем, які турбують людей. Більше того, на думку фахівців, сьогодні це явище становить значно серйознішу небезпеку ніж 5 років тому в силу використання зі злочинною метою новітніх інформаційних технологій, а також зростаючої уразливості сучасного індустріального суспільства. Незважаючи на зусилля держав, які спрямовані на боротьбу з кіберзлочинами, їх кількість у світі не зменшується, а, навпаки, постійно зростає. [5, с.17]

Таким чином, сучасний рівень інформатизації суспільства вимагає від України забезпечити належний та ефективний механізм боротьби із кіберзлочинами як однієї із серйозних загроз національній безпеці держави. Така потреба стає ще більш очевидною, враховуючи транснаціональний характер досліджуваних злочинів, що вимагає від правоохоронних органів України ще більш якісних технічного забезпечення та компетентності для здійснення якісної співпраці в як в рамках зокрема міжнародного співробітництва під час кримінальних проваджень даної категорії, так загалом у питаннях протидії кіберзлочинності.

Словник термінів із кібербезпеки за редакцією О. Копана надає два визначення поняттю кіберзлочину. Кіберзлочин (комп'ютерний злочин) – протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного шкідливого

програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо) [15].

Кіберзлочин (кібернетичний злочин) також визначено таким чином: 1. Кіберзлочин – злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин в кіберпросторі. На відміну від комп'ютерного злочину, поняття якого пов'язане з використанням будь-якої комп'ютерної техніки, кіберзлочин є більш вузьким поняттям, пов'язаним із функціонуванням саме кібернетичних комп'ютерних систем. До протиправного використання кібернетичних комп'ютерних мереж відносять несанкціоноване отримання прав керування такою системою (наприклад, використання шкідливого програмного забезпечення, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку тощо) та її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), а також створення та використання в злочинних цілях однієї кібернетичної комп'ютерної системи проти інших (наприклад, створення мережі зомбованих комп'ютерів для здійснення атак на веб-сайти, створення несанкціонованого робочого місця в системі електронного переказу коштів тощо) [15].

Кіберзлочин – найбільш небезпечне кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність. Також подаються визначення похідних понять від кіберзлочину. Кіберправопорушення – суспільно небезпечне діяння, що здійснюється з використанням технологій перетворення (створення, зберігання, обміну, обробки знищення) інформації, представленої у вигляді комп'ютерних даних, і тягне за собою юридичну відповідальність. Кіберправопорушення має всі загальні ознаки правопорушення, що виділяються в теорії права та вирізняються лише факультативною частиною юридичного складу, у якому кіберпростір виступає як засіб або мета здійснення правопорушення [15].

Кіберпроступки – кіберправопорушення, які не несуть суттєвої суспільної небезпеки, за які законодавством передбачена юридична відповідальність (крім кримінальної) [15].

Кіберпростір (кібернетичний простір) – 1) штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й обробки інформації та забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання послуг, ведення електронної комерції тощо); 2) простір, сформований інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну та знищення) інформації, представленої у вигляді електронних комп'ютерних даних.

Проаналізувавши теоретичні та практичні дослідження в галузі визначення поняття кіберзлочину, можна дійти висновку, що серед сучасних українських науковців немає єдиного підходу до визначення поняття кіберзлочину. Причому підходи досить суттєво відрізняються, що може бути причиною неправильного трактування, а це у свою чергу може призвести до неправильної кваліфікацію злочинних дій, що створить проблеми не тільки на теоретичному, а й на практичному рівнях.

У чинному законодавстві України на сьогодні відсутнє нормативно-правове закріплення ключових термінів «кіберзлочин» і «кіберзлочинність», що спричиняє численні наукові дискусії серед дослідників сучасності. Науковці приділяють багато уваги дослідженню зазначеної проблематики та пропонують власні визначення цих понять. Так, кіберзлочином слід вважати втручання в роботу телекомунікаційних мереж, комп'ютерних програм, що функціонують в їх середовищі, або несанкціоновану модифікацію комп'ютерних даних, зухвалу дезорганізацію роботи критично важливих елементів інфраструктури держави, що створює небезпеку загибелі людей, завдання значної майнової шкоди або настання інших суспільно небезпечних наслідків, здійснювані з метою порушення суспільної безпеки, залякування населення або впливу на ухвалення органами влади вигідних злочинцям рішень, задоволення їхніх майнових або інших інтересів [13, с. 12].

Крім того, кіберзлочини визначають як сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення та 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 досто-

вірну й повну інформацію [1, с. 7]. Варто звернути увагу, що в науковій юридичній літературі наведені такі ознаки кіберзлочинів, що відрізняють їх від «звичайних» злочинних посягань і значно підвищують їх суспільну небезпечність. По-перше, кіберзлочин не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого. По-друге, кіберзлочин є «автоматизованим» злочином (суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч). По-третє, суб'єкт кіберзлочину не підвладний обмеженням, які існують у реальному, фізичному світі. Так, кіберзлочини можуть бути вчинені моментально, а тому потребують швидкої реакції на них. По-четверте, кіберзлочинність і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це можливо стосовно злочинів, що вчиняються у реальному, фізичному світі [6, с. 130]. Виходячи з наведеного, можна зробити висновок, що 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. Таким чином, кіберзлочинність – це 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 в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [3, с. 332].

Крім того, кіберзлочинність визначають як 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 [9, с. 12].

Сучасні дослідники нерідко вважають поняття «кіберзлочинність», «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність» синонімами, однак існують і інші точки зору, за якими поняття «кіберзлочинність» є найширшим та охоплює найбільшу кількість злочинних посягань у віртуальному середовищі. Також використання поняття саме «кіберзлочинність» передбачає міжнародне законодавство [7, с. 173].

Щодо класифікації кіберзлочинів, то вона також не має чіткого нормативно-правового закріплення. Так, відповідно до розділу XVI Кримінального кодексу України [11], який має назву «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», основними такими злочинами є: несанкціоноване втручання в роботу електроннообчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 3611); несанкціоновані 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. 3612); 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); 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 оброблюється (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 3631). Відповідно до Конвенції Ради Європи про кіберзлочинність кіберзлочини можна умовно поділити на чотири групи: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення комп'ютерних даних, втручання в дані, втручання в систему, зловживання пристроями); 2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, та шахрайство, пов'язане з комп'ютерами); 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією); 4) правопорушення, пов'язані з порушенням авторських і суміжних прав [8]. Деякі науковці пропонують поділити кіберзлочини на агресивні та неагресивні. Так, до першої групи належать кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга

група охоплює кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм [3, с. 333]. Дуже цікавою, на нашу думку, є класифікація кіберзлочинів, запропонована В. Б. Дзюндзюком і Б. В. Дзюндзюком: 1) злочини проти конституційних прав і свобод людини та громадянина, такі як порушення недоторканості приватного житла, порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, порушення авторських і суміжних прав; 2) злочини проти життя та здоров'я. Загрозливих масштабів у мережі Інтернет набуває наявність сайтів, які пропагують наркоманію, публікують технологію виготовлення наркотичних препаратів у домашніх чи промислових масштабах або які розповсюджують наркотичні засоби, психотропні речовини та їх аналоги; 3) злочини проти честі та гідності особи. Анонімність і широка аудиторія користувачів Інтернету дають безмежні можливості для розповсюдження інформації будь-яких видів, у тому числі наклепницької, такої, що порочить честь і гідність особи; 4) злочини проти власності. Одним із найпоширеніших видів злочинів на сьогодні є інтернет-шахрайство, нові форми, види і способи якого з'являються кожного дня; 5) злочини у сфері комп'ютерної інформації, такі як неправомірний доступ до інформації, створення, використання та розповсюдження шкідливих програм; 6) злочини проти суспільної моральності; 7) злочини проти безпеки держави. Із зростанням використання мережі Інтернет у державних структурах стає можливим нелегально дістати доступ не лише до приватної та корпоративної інформації, а й до інформації, що є державною таємницею, також стає можливим скоювати такі злочини, як шпигунство, державна зрада або розголошення державної таємниці.

Найпоширенішими видами кіберзлочинів у сучасному світі є: – кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу, «трояни», «боти»); – фішинг – клієнтам платіжних систем надсилаються повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи із проханням вказати свої рахунки та паролі; – вішинг – у повідомленнях міститься прохання зателефонувати на певний міський номер, а під час розмови запитуються конфіденційні дані власника картки; – онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку; – піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті; – кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення; – соціальна інженерія – технологія управління людьми в інтернет-просторі; – мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення; – протиправний контент – контент, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства; – рефайлінг – незаконна підміна телефонного трафіка [3]. Варто взяти до уваги, що головне місце серед кіберзлочинів посідає кібертероризм як самостійний вид злочинної діяльності, який відрізняється від кіберзлочинності передусім своєю політичною спрямованістю, властивою тероризму в цілому [13, с. 12]. Під кібертероризмом слід розуміти навмисну політично вмотивовану атаку на об'єкти інформаційного простору (інформацію, що обробляється, комп'ютерну систему, мережу, а також на людину), що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної або суспільної безпеки, залякування населення, провокації військового конфлікту, чи загрозу вчинення таких дій [13, с. 13]. Отже, така значна кількість видів кіберзлочинів свідчить про те, що масштаби кіберзлочинності збільшуються. Тим самим зростає необхідність взаємодії держави із суспільством і міжнародною спільнотою з метою подолання цього негативного явища.

Література

1. Амелін О. Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. 2016. № 3. С. 1–10. URL: http://www.chasopysnapu.gp.gov.ua/ua/pdf/11-2016.

2. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність» / В. М. Бутузов // Інформацій на безпека людини, суспільства, держави. – 2010. – № 1 (3). – С. 18., с. 18.

3. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с, с. 332

4. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // Ресурсний центр ГУРТ: сайт. URL: http://www.gurt.org.ua/articles/34602.

5. Голубєв В.О. Комп'ютерні злочини в банківській діяльності. – З.: Павел, 1997. – С.16-18., с. 17.

6. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. 2010. № 3 (19). С. 129–136., с. 130].

7. Іванченко О. М. Кримінологічна характеристика кіберзлочинності, запобіганні кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. № 3. С. 172–177., с. 173.

8. Конвенція про кіберзлочинність: від 23.11.2001 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/994_575

9. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.08. Харків, 2016. 16 с.

10. Кравцова М.А. Понятие киберпреступности и ее признаки//Часопис Київського університету права. № 2015/2. С. 320–324, с. 321.

11. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-ІІІ // БД«ЗаконодавствоУкраїни» / ВРУкраїни.URL:http://zakon.rada.gov.ua/laws/show/2341-14

12. Пивоваров В.В., Терещенко К. В.: Шахрайство її банківськими картками: окремі питання віктимологічної профілактики // Карпатський приватний часопис № 10 – 2015.

13. Пилипчук В. Г., Дзьобань О. П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. Стратегічні пріоритети. 2011. № 4 (21). С. 12–17., с. 12

14. Пилипчук В. Г., Дзьобань О. П. Теоретичні та державно-правові аспекти протидії

15. Про боротьбу з тероризмом : Закон України // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180., с. 85

16. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року.

Анотація

Васильковский І. І. **Поняття, класифікація та характеристика окремих видів кіберзлочинів.** – Стаття.

Стаття присвячена визначенню основних понять кіберзлочинності та класифікації кіберзлочнів, їх характеристиці, які виникають у результаті здійснення даного виду діяльності та аналізу понять.

Ключові слова: кіберзлочинність, кіберзлочини, розслідування, кримінальне провадження.

Аннотация

Васильковский И. И. **Понятие, классификация и характеристика отдельных видов киберпреступлений.** – Статья.

Статья посвящена определению основных понятий киберпреступности и классификации киберзлочнив, их характеристике, которые возникают в результате осуществления данного вида деятельности и анализа понятий.

Ключевые слова: киберпреступность, киберпреступления, расследование, уголовное производство.

Summary

Vasylkovskyi I. I. **Concept, classification and characterization of certain types of cybercrime.** – Article.

The article is devoted to the definition of the basic concepts of cybercrime and the classification of cyber-bulbs, their characteristics, which arise as a result of the implementation of this type of activity and analysis of concepts.

Key words: cybercrime, cybercrime, investigation, criminal proceedings.