goods, furniture, sports goods, musical instruments, cures etc.) provided in extra-judicial and extracontractual order; 2) alimony designated in the court decision or under the contract; 3) additional expenses imposed by the court or stipulated in the agreement on payment of alimony.

According with the way of determining the form and amount of means of maintenance as the subject of crime under Art. 164 of the Criminal Code of Ukraine they can be divided into three groups:1) the means, the forms and the amount of which are determined by the court (alimony designated in the court decision and court fees for additional costs); 2) means, the form and amount of which are defined in a contract (maintenance under the contract, additional expenses stipulated in the agreement on payment of alimony); 3) means, the form and amount of which are not determined either in court decision, or in contract.

Such classification is important for qualification of this crime in practice, since alimony designated in the court decision (the means of the first group) constitute a subject of persistent failure to pay contributions (alimony) for support of children, as prescribed by a court order (the first form of the researched crime), which is completed from the time of arrear of paying of such means in the amount that collects the sum of payments for three months of the corresponding payments; instead, additional expenses imposed by the court (the means of the first group), as well as the means of the second and third groups are the subject of parent's persistent failure to support dependent minors or children unable to work (the second form of the researched crime), which is completed since the act have acquired persistence.

Keywords: *crimes against family, failure to support of children, failure to pay alimony for support of children, subject of crime, alimony, maintenance.*

УДК 343.346.8

М. В. Карчевський

ОСНОВНІ ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАТИЗАЦІЇ

Здійснено спробу встановити зміни у сфері кримінально-правового регулювання, викликані інформатизацією та визначити основні напрями їх урахування в процесі подальшого вдосконалення законодавства та практики його використання. До означених змін віднесено формування нового предмета кримінально-правового регулювання (інформаційної безпеки) та появу нових видів матеріальних цінностей. Основні проблеми кримінально-правового регулювання відносин інформаційної безпеки – недостатня визначеність законодавства про «комп'ютерні» злочини, необгрунтовано розгалужену систему норм про злочини у сфері доступу до інформації, спірні нормативні рішення з питань формування інформаційного ресурсу. Проблеми кримінально-правового регулювання, пов'язані з появою нових видів матеріальних цінностей, стосуються розгляду безготівкових грошей, електронних грошей та криптовалюти в контексті злочинів проти власності.

Ключові слова: *інформаційна безпека, «комп'ютерний» злочин, блокування інтернет ресурсів, безготівкові гроші, електронні гроші, криптовалюта, майнінг криптовалюти.*

Постановка проблеми. Питання кримінально-правового відображення тенденцій інформатизації суспільства дедалі частіше стають предметом спеціальних досліджень. Це не дивно з огляду на зростання соціального значення відносин, пов'язаних з використанням інформаційних технологій, розширення сфери застосування комп'ютерної техніки та зростання небезпеки «комп'ютерних» злочинів. Через це потребує наукового аналізу питання змін, що відбулися в кримінально-правовому регулюванні інформаційних відносин. Чітке та послідовне визначення означених змін дозволить системно підходити до питання вдосконалення чинного законодавства та практики його використання.

Аналіз останніх досліджень і публікацій. Проблеми кримінально-правового відображення інформатизації суспільства розглядалися такими вітчизняними дослідниками, як Д. С. Азаров [1], П. П. Андрушко [2], Ю. А. Бельський [3], В. М. Бутузов [4], В. О. Голубєв [5], С. В. Дрьомов [6], М. В. Карчевський [8], О. О. Кирбят'єв [10], М. О. Кравцова [11], Т. В. Міхайліна [12], А. А. Музика [13], М. В. Плугатир [15], С. О. Орлов [14], Н. А. Розенфельд (Н. А. Савинова) [17], М. В. Рудик [18]. Водночас для ефективної організації наукового дискурсу з названої проблематики потрібним видається формулювання основних проблемних питань, «фокусів» подальшого дослідження кримінально-правого відображення інформатизації.

Формування цілей. У роботі запропоновано спробу визначення змін, які відбулися в кримінально-правовому регулюванні через інформатизацію суспільства, та основних напрямів їх урахування в процесі подальшого вдосконалення законодавства й практики його використання.

Виклад основного матеріалу. Потреба кримінально-правового стимулювання позитивних та мінімізації негативних наслідків інформатизації обумовила *появу відносно самостійної групи суспільних відносин, які можна розглядати як новий родовий об'єкт злочину.* Для позначення цієї групи будемо використовувати термін «інформаційна безпека», визначивши його як систему суспільних відносин щодо реалізації інформаційної потреби особи, суспільства, держави. Складається така система з трьох взаємопов'язаних та взаємообумовлених елементів: відносини у сфері використання інформаційних технологій, відносини у сфері забезпечення доступу до інформації, відносини у сфері формування інформаційного ресурсу.

На сьогодні можна твердити про існування «класичних» проблем кримінально-правового регулювання кожної із зазначених груп. Ці проблемні аспекти досить добре досліджено та підтверджено емпіричними даними.

Що ж до так званих «*комп'ютерних злочинів*», посягань, що заподіюють шкоду відносинам інформаційної безпеки у сфері використання інформаційних технологій, *то головне питання полягає у відсутності чітких критеріїв суспільної небезпеки на рівні законодавчих визначень*. Через це в сфері дії кримінальної юстиції опиняються не тільки діяння, що дійсно є суспільно небезпечними, але й ті, які такими не є. Ефективність протидії кіберзлочинності зменшується. Через огром роботи щодо розслідування

діянь зі спірною суспільною небезпекою певною мірою втрачаються й перспективи вдосконалення діяльності правоохоронців. Красномовним тут буде порівняння даних про обліковані кримінальні правопорушення у сфері використання інформаційних технологій (ст.ст. 361 – 363-1 КК України) з кількістю вироків цієї категорії, представлених у Єдиному державному реєстрі судових рішень (таблиця 1). Для того, щоб мати можливість оцінити результати роботи правоохоронців у контексті темпів інформатизації, ми також додали дані щодо проникнення Інтернету. Цей показник є одним з універсальних маркерів інформатизації, обчислюється у відсотках та представляє собою частку населення країни, яка користується Інтернетом. Як можна побачити, із зростанням аудиторії Інтернету відбувається зростання кількості облікованих правопорушень, що цілком природньо, оскільки чим більше людей використовує сучасні інформаційні технології, тим більше «комп'ютерних» злочинів може бути вчинено. Але разом із зростанням кількості облікованих правопорушень спостерігається зменшення кількості судових вироків відповідної категорії. Можна говорити про рівень матеріально-технічного та кадрового забезпечення розслідування, брати до уваги необхідність спеціальних знань у суддів та прокурорів тощо, проте основна, фундаментальна причина ситуації, що склалася, саме в якості законодавства.

Таблиця 1

Статистичні дані щодо протидії злочинам у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку

Показник	2013	2014	2015	2016
Абсолютні дані				
Кількість вироків у Єдиному державному реєстрі судових рішень	56	40	39	25
Обліковано кримінальних правопорушень	568	418	556	912
Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	245	194	250	514
Проникнення Інтернету (КМІС)	49	54	57	62
Відносні дані (відсотки від базового рівня – 2013 р.)				
Кількість вироків у Єдиному державному реєстрі судових рішень	100	71	70	45
Обліковано кримінальних правопорушень	100	74	98	161
Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	100	79	102	210
Проникнення Інтернету (КМІС)	100	110	116	127

Проблеми кримінально-правового регулювання наступної групи відносин інформаційної безпеки – відносин у сфері забезпечення доступу до інформації – стосуються головно *розбалансованості законодавства, існуванні численних конкуруючих норм, надмірного рівня кількості кримінально-правових заборон у цій сфері*. Необхідною є оптимізація згаданої системи норм, заміни наявної розосередженої системи спеціальних кримінально-правових заборон такими, які б забезпечували регулювання більш широких сегментів інформаційної безпеки.

Основне питання кримінально-правового регулювання *у сфері формування інформаційного ресурсу полягає в чіткому та послідовному визначенні межі можливостей ефективного впливу на суспільні відносини засобами кримінального права.* У суспільно-політичному дискурсі, у науці небезпеки інформаційних впливів та зловживань обговорюються достатньо широко. Багатомірність і масштабність шкоди від неконтрольованого інформаційного простору не викликає сумнівів. Водночас розв'язання означених проблем через доповнення КК новими нормами навряд чи є доцільним. Неодноразово пропонувалося встановлювати покарання за різноманітні форми маніпуляції суспільною свідомістю. Такі пропозиції є спірними через прогнозовану неефективність і декларативність, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації. Крім того, поширення глобальних інформаційних технологій взагалі робить методи обмеження або заборони контенту все менш ефективними. Яскравим прикладом тут може слугувати відомий «ефект Стрейзанд». Розв'язання проблеми знаходиться поза межами кримінально-правового регулювання і, на нашу думку, передбачає, у першу чергу, системну роботу в галузі освіти та формуванні конкурентних інформаційних продуктів. Додатковими аргументами на користь освітнього вектору розв'язання наведених проблем інформаційної безпеки можуть свідчити й питання, які стали предметом суспільної уваги під час встановлення обставин загибелі учасників мережевої групи «Синій кит». Самостійним напрямом особистої інформаційної безпеки підлітків, який знову ж таки підтверджує тезу про обмежену ефективність кримінально-правових засобів, є протидія кібербулінгу. Зарубіжна практика свідчить про те, що негативні наслідки образ, цькування неповнолітніх за допомогою соціальних мереж або електронної пошти (власне кібербулінг) долаються головно через формування навичок безпечної комунікації.

У цьому контексті неможливо не згадати про рішення щодо обмеження доступу до певних російських сайтів та соціальних мереж. З одного боку маємо очевидні позитивні аспекти: тимчасове зменшення ефективності інформаційних операцій проти України та відчутні фінансові втрати російських ІТ-компаній (експертні оцінки втрат Яндекса - $124,4 млн.). З іншого – значні негативні наслідки як для інформаційної безпеки країни, так і громадян. По-перше, обмеження поведінки, що фактично є соціальною нормою, актуалізує питання *стимулювання правого нігілізму, веде до чергового «витку» інфляції нормативно-правових актів*. По-друге, *обмеження можливостей*

правоохоронних органів щодо оцінки, аналізу та контролю за антидержавною діяльністю з використанням заблокованих ресурсів. Сподіватися на те, що всі одразу перестануть користуватися забороненими ресурсами безвідповідально. Водночас кількісна та якісна оцінка цього процесу надзвичайно ускладнена, моніторинг національної аудиторії заборонених ресурсів став складним технічним завданням. По-третє, *створення «комфортної» «сірої зони» для інформаційних впливів через ускладнення їх правової оцінки*. Ще раз зазначимо, що величезна аудиторія не скоротиться миттєво. Про це наочно свідчать актуальні рейтинги найбільш відвідуваних мережевих ресурсів. Чи можна сьогодні розглядати пост у соціальних мережах, доступ до яких обмежено, як «публічний заклик» у контексті відомих статей Особливої частини КК? Непросте питання, яке може розглядатися як технологія ухилення від відповідальності. По-четверте, *нові небезпеки широкого розповсюдження шкідливого програмного забезпечення*, адже зловмисники (насамперед шахраї, «фішери») подістали значну цільову аудиторію. Потреба отримувати доступ до заблокованих ресурсів за наявності для цього достатньо простої технічної можливості створює попит на різноманітні програмні засоби. Під виглядом таких програмних засобів значна частка національної аудиторії заблокованих ресурсів може отримати «троянське» програмне забезпечення. У подальшому їхні комп'ютери та інтернет-пристрої можуть бути використані, наприклад, для масштабних атак відмови від обслуговування.

Варто зауважити, що проблематика інформаційної безпеки є однією з найбільш динамічних. Новітні технології розвиваються та поширюються досить швидко, а отже, викликають появу нових соціальних практик, формують нові потреби у правовому регулюванні. Тому, сформулювавши, як зазначалося вище, «класичні» проблеми інформаційної безпеки, вважаємо за потрібне звернути увагу на нові виклики, що виявились останнім часом досить рельєфно. Одним з них є *новітні можливості незаконних дій щодо матеріальних цінностей або з ними*.

Сферою широкого застосування комп'ютерної техніки є банківська діяльність та платіжні системи, тому велика частка злочинів проти власності так чи інакше пов'язана зі злочинами у сфері використання комп'ютерної техніки. Йдеться про «злам» електронної пошти для отримання реквізитів доступу до банківських рахунків (ст. 361 КК); блокування інтернет-ресурсу з метою вимагання (ст. 361 або 363-1 КК); використання «скімерів» (спеціальних пристроїв, що приховано встановлюються зловмисниками на банкомати) для отримання реквізитів платіжних карток або розробка та використання шкідливих програмних засобів, призначених для незаконного віддаленого доступу до бухгалтерського програмного забезпечення підприємств, установ чи організацій (ст. 361-1 КК); збут клієнтських баз даних скомпрометованих фінансових установ (ст. 361-2); введення банківськими працівниками до автоматизованих систем банківського обслуговування неправдивих відомостей щодо здійснених фінансових операцій (ст. 362 КК); невжиття потрібних технічних заходів інформаційної безпеки, що призвело до компрометації автоматизованої системи фінансової

установи (ст. 363 КК) тощо. Разом з оновленням способів вчинення та приховування слідів злочинів проти власності суттєві зміни спостерігаються й у питанні предмета злочину проти власності. Доволі дискусійним як для науковців, так і для практиків стало питання юридичного змісту таких категорій, як «*безготівкові гроші*», «*електронні гроші*», «*криптовалюта*».

Категорія «*безготівкові гроші*» найчастіше трапляється в контексті злочинів проти власності, що вчиняються з використанням платіжних карток або їх реквізитів. Фактично вони представляють собою зобов'язання банка-емітента платіжної картки, відомості про які обліковано на картковому рахунку держателя картки. У термінах розділу Особливої частини КК «Злочини проти власності» стосовно безготівкових грошей найбільш обґрунтовано використовувати поняття «право на майно». Тому переважна більшість посягань, пов'язаних з незаконними операціями з платіжними картками або їх реквізитами правильно розглядається як один з видів шахрайства, учиненого способом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК). Найбільш дискусійний момент такої кваліфікації полягає в питанні щодо можливості «ошукати комп'ютер». Проте наявний емпіричний матеріал та аналіз законодавства дозволяють сформулювати особливості об'єктивної сторони цього виду шахрайства. По-перше, надсилаючи несанкціонований законним держателем картки запит на здійснення платежу й використовуючи існуючу платіжну систему та встановлені в ній правила автоматизованої обробки запитів законних держателів карток, зловмисник ошуковує банківську установу (банк-емітент) щодо необхідності виконання останнім зобов'язань, обумовлених договором, укладеним між банком і законним держателем картки. По-друге, унаслідок введення в оману банк-емітент здійснює необґрунтоване списання безготівкових коштів з рахунку законного держателя картки, що призводить до заподіяння останньому збитків у вигляді зменшення кількості безготівкових грошових коштів, врахованих на картрахунку [7]. Варто зазначити, що не всі посягання у сфері використання платіжних систем, банкоматів потрібно кваліфікувати за ч. 3 ст. 190 КК. Наприклад, досить поширеним є заволодіння готівкою, що знаходиться в банкоматі, за допомогою спеціального пристрою («вилки»), або клейкої стрічки. Подібні випадки слід кваліфікувати як крадіжку, але такі винятки лише підтверджують правильність наведених раніше міркувань.

Електронні гроші «одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі» [16] Вони з'явилися як реакція ринку банківських послуг на проблеми безпеки використання платіжних карток та потребу в новому, більш гнучкому, зручному й захищеному платіжному інструменті для оплати товарів та послуг через Інтернет [19]. Цим зумовлюються особливості електронних грошей, які відрізняють їх від безготівкових: електронні гроші не є універсальними та приймаються лише користувачами відповідних платіжних систем; емісію грошей здійснює тільки НБ, а емісія

електронних грошей здійснюється банківськими установами; унаслідок переказу електронних грошей їх одержувач набуває право грошової вимоги до того ж суб'єкта, що й платник; електронні гроші існують у межах однієї платіжної системи й не можуть бути переведені до іншої платіжної системи в незмінному вигляді [більш докладно див. 20]. З огляду на вказані особливості електронних грошей питання кваліфікації незаконних дій щодо них мають розв'язуватися аналогічно з описаним раніше підходом щодо безготівкових грошей.

Криптовалюта являє собою подальший крок у розвитку технологій розрахунків з використанням сучасних інформаційних технологій. Найбільш відомою криптовалютою є Bitcoin. У науковій та популярній літературі представлено достатньо інформації щодо технічних та організаційних особливостей функціонування Bitcoin, ми ж зупинимося на тих, які вважаємо ключовими для відповіді на питання щодо можливостей кримінально-правового регулювання в цій сфері. По-перше, криптовалюта фізично являє собою певний набір даних, згенерованих на підставі складного математичного алгоритму. По-друге, платіжна система Bitcoin організована за принципом пірингової мережі (p2p, pear to pear – рівний рівному), записи щодо всіх транзакцій розподілені між усіма учасниками системи, єдиний центр координації мережі відсутній, у вільному доступі представлено інформацію щодо всіх здійснених транзакцій. Такий метод організації платіжної системи забезпечує майже абсолютний захист інформації щодо транзакцій, робить систему стабільною та надійною. По-третє, для реєстрації в платіжній системі не використовуються персональні дані, транзакції здійснюються між деперсоніфікованими «електронними гаманцями». По-четверте, Bitcoin - нефіатні гроші, їх вартість нічим не забезпечена й визначається ситуативно на підставі попиту та пропозиції, єдиний орган, що встановлює курс до національних валют, відсутній. Корисні властивості криптовалюти (захищеність, конфіденційність, децентралізація, майже миттєвий переказ у будь-яку частину світу) забезпечують стабільний попит на неї та стійке зростання курсу до національних валют. Лише з грудня 2016 року по вересень 2017 вартість Bitcoin зросла з 750 до 4250 доларів США.

За таких умов не дивно, що криптовалюта набуває значного поширення в Україні. При цьому Національний банк України (лист від 08 грудня 2014 року №29-208/72889) розглядає Bitcoin як «грошовий сурогат, який не має забезпечення реальною вартістю і не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це суперечить нормам українського законодавства». Маємо ситуацію, коли фактично існуючі та динамічні суспільні відносини опиняються поза межами правового регулювання за умови очевидної необхідності такого. Наприклад, особа вимагає певну суму у Bitcoin. Яким чином встановити ознаки предмета злочину? Чи можна розглядати відомості інтернет-джерел щодо курсу Bitcoin як достатній доказ для встановлення економічної ознаки відповідного предмета злочину? На сьогодні чіткої відповіді на поставлені запитання немає.

Варто звернути увагу й на питання, яке нещодавно активно обговорювалося в засобах масової інформації: кримінально-правова оцінка «майнінгу» криптовалюти в контексті ст. 200 КК. На нашу думку, відповідно до чинного законодавства «майнінг» криптовалюти не є випуском електронних грошей, такі дії не містять ознак складу злочину, передбаченого ст. 200 КК.

По-перше, відповідно до Закону України «Про платіжні системи та переказ коштів в Україні» електронні гроші являють собою «одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі». Натомість, як зазначалося раніше, криптовалюта не є грошовим зобов'язанням, її вартість нічим не забезпечена та визначається ситуативно на підставі попиту й пропозиції. Отже, згідно з чинним законодавством, криптовалюта не є електронними грошима за визначенням.

По-друге, «майнінг» представляє собою долучення до роботи системи криптовалюти через надання обчислювальних потужностей. Для підтримки системи функціонування криптовалюти потрібні надзвичайно значні обчислювальні потужності, тому алгоритм функціонування криптовалюти передбачає винагородження для учасників системи. У результаті «майнінгу» особи, які надають системі обчислювальні потужності, отримують винагороду у вигляді одиниць криптовалюти. Звичайно такі дії не можна розглядати як випуск електронних грошей, який відповідно до Положення про електронні гроші в Україні являє собою операцію з «надання електронних грошей користувачам або агентам в обмін на готівкові або безготівкові кошти».

Таким чином, відповідно до чинного законодавства «майнінг» криптовалюти не є випуском електронних грошей, оскільки криптовалюта не є електронними грошима, а в результаті «майнінгу» електронні гроші не надаються в обмін на готівкові або безготівкові.

Досвід зарубіжних країн дуже різноманітний і містить приклади від офіційного визнання криптовалюти (Японія, Німеччина) до аналогічного національному підходові ігнорування. Очевидно криптовалюти будуть дедалі частіше використовуватися для вчинення злочинів або ставати їх предметом. У таких умовах найбільш доцільно сформулювати прості та прозорі правила для сфери кримінально-правового регулювання, зокрема передбачити механізм оцінки. Представлення в процесуальній формі даних про криптовалюти створить нові умови для якісного оновлення діяльності правоохоронців. Виникнуть принципово нові види тактичних операцій, що збільшить можливості протидії злочинності. Варто зазначити, що ці питання потрібно розглядати як складові більш загальної проблеми – можливості використання технологій Big Data у правоохоронній діяльності [9].

Також відсутність правової визначеності щодо діяльності з використанням криптовалюти негативно позначається й на перспективах розвитку ІТ-сектору економіки. Цей сектор розвивається найбільш

динамічно і є перспективним з огляду на значні інвестиції в економіку України. Насамкінець зазначимо, що формалізована на рівні закону заборона використання криптовалюти в Україні не розв'яже означених проблемних питань, а лише створить нові. Криптовалюту будуть дедалі активніше використовувати злочинці та корупціонери саме через її позаправовий статус, водночас можливості правоохоронців, з цієї ж причини, будуть значно обмежені.

Висновки. Таким чином, *для продовження дискусії* щодо змісту обумовлених інформатизацією змін у сфері кримінально-правового регулювання можемо сформулювати такі положення:

- розпочалося та триває формування нового предмета кримінально-правового регулювання – інформаційної безпеки;
- «класичними» проблемами цього процесу є недостатність визначеності законів про кримінальну відповідальність за «комп'ютерні» злочини, потреба оптимізації системи кримінально-правого регулювання у сфері доступу до інформації, питання меж та доцільності кримінально-правового регулювання у сфері формування інформаційного ресурсу;
- існують складнощі кримінально-правового регулювання, обумовлені появою нових видів матеріальних цінностей; потребує розв'язання проблема правового регулювання використання криптовалюти.

Використані джерела:

1. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : Монографія / Д. С. Азаров. – К.: Атіка, 2007. – 304 с.

2. Андрушко П. П. Коментар до розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку» Особливої частини Кримінального кодексу України / П. П. Андрушко // Законодавство України. Науково-практичні коментарі. – № 1. – 2006. – С. 32–54.

3. Бельський Ю.А. Кримінальна відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку : Дис. ... канд. юрид. наук: 12.00.08 / Ю. А. Бельський. – К., 2017. – 253 с.

4. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КНТ, 2010. – 408 с.

5. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами / В. О. Голубєв. – Запоріжжя, 2003. – 250 с.

6. Дрьомов С. Комп'ютерна інформація як предмет злочину, передбаченого ст. 362 Кримінального кодексу України / С. Дрьомов // Підприємництво, господарство і право. – 2005. – № 4. – С. 129–132; Дрьомов С. Кримінально-правова характеристика перехоплення комп'ютерної інформації як форми об'єктивної сторони злочину, передбаченого статтею 362 КК України / С. Дрьомов // Юридичний журнал. – 2006. – № 6. – С. 54–56; Дрьомов, С. Несанкціоноване знищення інформації як форма об'єктивної сторони складу злочину, передбаченого ст. 362 КК України / С. Дрьомов, Т. Рендель // Вісник прокуратури. – 2006. – № 9. – С. 90–94; Дрьомов, С. Сутність копіювання як форми несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах,

комп'ютерних мережах або зберігається на носіях такої інформації / С. Дрьомов // Підприємництво, господарство і право. – 2005. – № 9.– С. 144–147; Дрьомов С. Умисел при вчиненні несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362 КК України) / С. Дрьомов // Підприємництво, господарство і право. – 2005. – № 7. – С. 115–119.

7. Дудоров О.О., Карчевський М.В. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки // Азовські правові читання – 2017: Матеріали міжнародної науково-практичної конференції, м. Бердянськ, 28–29 квітня 2017 р. – Бердянськ: ТОВ «Модем-1», 2017. – С. 5–12.

8. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж: монографія / М. В. Карчевський ; МВС України, Луг. акад. внутр. справ ім. 10-річчя незалежності України; [Наук. ред. Л.М. Кривоченко]. – Луганськ: РВВ ЛАВС, 2002. – 144 с.; Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України : Монографія. – Луганськ, 2012. – 528 с.

9. Карчевський М.В. Можливості Big Data та кримінально-правова комунікація // Матеріали Міжнародної науково-практичної конференції "Політика в сфері боротьби зі злочинністю" [Текст]. - Івано-Франківськ, 2017. – С. 52-58.

10. Кирбят'ев О. О. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : Дис. … канд. юрид. наук: 12.00.08 / О.О. Кирбят'єв. - Запоріжжя, 2015.- 200 с.

11. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08 / Кравцова М. О. ; Харків. нац. ун-т внутр. справ. - Харків, 2016. - 16 с.

12. Міхайліна, Т. В. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : Автореф. дис. … канд. юрид. наук : 12.00.08 / Т. В. Михайліна. – К., 2011. – 20 с.

13. Музика А.А., Азаров Д.С. Законодавство України про відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. – К.: Вид. Паливода А.В., 2005. – 120 с.

14. Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : Дис. ... канд. юрид. наук: 12.00.08 / С. О. Орлов. – Х., 2004. – 213 с.

15. Плугатир М. В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації : Автореф. дис. ... канд. юрид. наук: 12.00.08 / М. В. Плугатир. – К., 2010. – 18 с.

16. Положення про електронні гроші в Україні // Постанова Правління Національного банку України від 04.11.2010 № 481.

17. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : Дис. ... канд. юрид. наук: 12.00.08 / Н. А. Розенфельд. – К., 2003. – 222 с.; Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : Монографія / Н. А. Савінова. – К., 2012. – 340 с.

18. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : Дис. ... канд. юрид. наук: 12.00.08 / М. В. Рудик. – Х., 2007. – 229 с.

19. Фінансова грамотність : навч. посібник / авт. кол. ; за ред. д-ра екон. наук, проф. Т. С. Смовженко. – Вид. 2-ге, випр. і доп. – К., 2013. – С. 74.

20. Шимон С. Електронні гроші: форма грошей чи майнові права вимоги? / С. Шимон // Юридична Україна. – 2015. – № 9. – С. 36–41; Куцевич М. Неправомірний випуск й використання електронних грошей, що вчиняються у системах інтернет-розрахунків (проблеми кримінально-правової кваліфікації) / М. Куцевич, П. Берзін // Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. - 2013. - Вип. 4. - С. 13-16.

Стаття надійшла до редколегії 23.08.2017

Карчевский Н. В. Основные проблемы уголовно-правового регулирования в сфере информатизации

Предпринимается попытка установить изменения в сфере уголовно-правового регулирования, вызванные информатизацией и определить основные направления их учета при дальнейшем совершенствовании законодательства и практики его применения. К указанным изменениям отнесены формирование нового предмета уголовно-правового регулирования (информационной безопасности) и появление новых видов материальных ценностей. Основные проблемы уголовно-правового регулирования отношений информационной безопасности – недостаточная определенность законодательства о «компьютерных» преступлениях, необоснованно разветвленная система норм о преступлениях в сфере доступа к информации, спорные нормативные решения по вопросам формирования информационного ресурса. Проблемы уголовно-правового регулирования, связанные с появлением новых видов материальных ценностей, касаются рассмотрения безналичных денег, электронных денег и криптовалюты в контексте преступлений против собственности.

Ключевые слова: *информационная безопасность, «компьютерное» преступление, блокирование интернет-ресурсов, безналичные деньги, электронные деньги, криптовалюта, майнинг криптовалюты.*

Karchevskyi M. The Main Problems of Criminal Law Regulation in the Field of Informatization

An attempt is being made to introduce changes in the field of criminal law regulation caused by informatization and to determine the main directions of their consideration in the process of further improvement of legislation and practice of its use.

The necessity of criminal legal stimulation of the positive and minimization of the negative consequences of informatization led to the emergence of a relatively independent group of social relations, which can be considered as a new subject of criminal law regulation. To designate this group, the term "information security" - the system of public relations for the implementation of the information needs of the individual, society, and state - is used. This system consists of three interconnected and interdependent elements: relations in the sphere of information technology use, relations in the field of providing access to information, relations in the field of formation of information resources.

In the case of so-called "computer crimes", the main point is the lack of clear criteria for public danger at the level of legislative definitions. So there are not only acts that are really socially dangerous in the field of criminal justice, but also those that are not. The effectiveness of cybercrime abatement is reduced.

The problems of criminal law regulation of the next group of relations of information security - relations in the field of providing access to information - relate mainly to the imbalance of legislation, the existence of numerous competing norms, the excessive amount of criminal law prohibitions in this area.

The primal question of criminal law regulation in the area of information resource formation is the clear and consistent definition of the limits of the possibilities of effective influence on social relations by means of criminal law. It is substantiated that solving problems of counteracting manipulative influences on public consciousness by supplementing the Criminal Code with new norms is not expedient. The effectiveness of restricting access to Internet resources is critically evaluated.

A separate basket is related to the renewal of property crimes. Criminal-legal aspects of illegal actions with non-cash and electronic money, crypto-currency are considered. The conclusion is based on the fact that at the present time in Ukraine there is a situation where actual existing and dynamic social relations are outside the limits of legal regulation upon condition of the obvious necessity of such.

Key words: *information security, "computer" crime, blocking of Internet resources, non-cash money, electronic money, cryptocurrency, cryptocurrency mining.*

УДК 343.122

А. О. Коваленко

ТИМЧАСОВИЙ ДОСТУП ДО РЕЧЕЙ І ДОКУМЕНТІВ У СИСТЕМІ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ ЦИВІЛЬНОГО ПОЗОВУ

Статтю присвячено окремим теоретичним і прикладним аспектам здійснення тимчасового доступу до речей і документів як одного з видів заходу забезпечення цивільного позову в кримінальному провадженні. Визначено, що в практичній площині найдієвішим його способом є вилучення речей і документів (здійснення їх виїмки). Проаналізовано прикладні проблеми його реалізації, наведено позиції вчених та запропоновано шляхи усунення наявних у КПК України прогалин.

Ключові слова: *цивільний позов; тимчасовий доступ до речей та документів; забезпечення відшкодування шкоди; заходи забезпечення кримінального провадження.*

Постановка проблеми. Ефективне й своєчасне виконання завдань кримінального провадження не можливе без застосування відповідних заходів його забезпечення. Для цього до КПК України 2012 року запроваджено інститут заходів забезпечення кримінального провадження, одним з яких є тимчасовий доступ до речей і документів (гл. 15 КПК). Безумовно, що здійснення цієї процесуальної діє створює певні передумови для забезпечення цивільного позову в кримінальному провадженні, а отже є важливою умовою здійснення правосуддя.

Аналіз останніх досліджень і публікацій. З часу прийняття чинного КПК України питання здійснення тимчасового доступу до речей і