DOI: 10.31359/2079-6242-2024-48-116
УДК 343.3/.7

М. В. Карчевський, доктор юридичних наук, професор, головний науковий співробітник відділу дослідження проблем кримінального права Науково-дослідного інституту вивчення злочинності імені академіка В. В. Сташиса Національної академії правових наук України

ПРАКТИКА ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ*

Постановка проблеми. Розширення сфери застосування комп'ютерної техніки є закономірним результатом зростання інформаційної соціальної потреби. Процеси інформатизації та комп'ютеризації сьогодні забезпечують збільшення можливостей людини, суттєву інтенсифікацію діяльності підприємств, установ та організацій. Разом із тим, підкоряючись діалектичному закону, ці процеси не є однозначними. Окрім позитивних соціальних трансформацій, широке розповсюдження інформаційних технологій призвело до появи та розвитку цілого комплексу негативних наслідків. Серед них – кіберзлочинність.

«Комп'ютерні» кримінальні правопорушення інколи визначаються як такі, що вчиняються з використанням комп'ютерів. Саме таке розуміння поняття «cybercrime» можна часто зустріти в американській науковій літературі. Певною мірою, це можна пояснити тим, що в американській кримінально-правовій доктрині матеріально-правові проблеми розглядаються в нерозривному зв'язку з процесуальними. Використання комп'ютерної техніки в процесі вчинення кримінальних правопорушень завжди зумовлює необхідність використання специфічних криміналістичних та процесуальних засобів. Саме це і виступає ключовим аргументом для такого широкого підходу до визначення «комп'ютерних» кримінальних правопорушень. Тому визначення «комп'ютерних» кримінальних правопорушень, що наводиться у зарубіжній доктрині кримінального права, має обмежене використання на національному рівні. Отже, в цій публікації під «комп'ютерними» кримінальними правопорушеннями будемо розуміти посягання, передбаченні Розділом XVI Особливої частини КК України.

Аналіз останніх досліджень і публікацій. Проблеми кримінально-правового відображення тенденцій інформатизації суспільства у своїх роботах розглядали Д. С. Азаров[1], П. П. Андрушко[2], Ю. А. Бельський[3], В. М. Бутузов[4], В. О. Голубев[5], С. В. Дрьомов[6], О. О. Кирбят'єв[7], М. О. Кравцова[8],

[1] * *Примітка.* Статтю підготовлено в межах реалізації теми фундаментального дослідження «Теоретичні, законодавчі та правозастосовні проблеми кримінально-правової охорони інформаційної безпеки в Україні» (номер державної реєстрації 0121U114324).

[1] Азаров ДС, *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)* (Атіка, 2007) 304.

[2] Андрушко ПП, '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' *Законодавство України. Науково-практичні коментарі* (2006) (1) 32–54.

[3] Бельський ЮА, '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, Національна академія внутрішніх справ, 2017) 253.

[4] Бутузов ВМ, *Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз)* (КНТ, 2010) 408.

[5] Голубєв ВО, *Інформаційна безпека: проблеми боротьби з кіберзлочинами* (ГУ «ЗІДМУ», 2003) 250.

[6] Дрьомов С, 'Комп'ютерна інформація як предмет злочину, передбаченого ст. 362 Кримінального кодексу України' *Підприємництво, господарство і право* (2005) (4) 129–132; Дрьомов С та Рендель Т, 'Несанкціоноване знищення інформації як форма об'єктивної сторони складу злочину, передбаченого ст. 362 КК України' (2006) (9) Вісник прокуратури 90–94.

[7] Кирбят'єв ОО, '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., Класичний приватний університет, 2015) 20.

[8] Кравцова МО, 'Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ' (автореф. дис. … канд. юрид. наук, Харківський національний університет внутрішніх справ, 2016) 16.

Т. В. Михайліна[1], А. А. Музика[2], М. В. Плугатир[3], С. О. Орлов[4], Н. А. Савінова[5], М. В. Рудик[6] та інші дослідники.

Певний внесок у розгляд означеної проблеми зробив і автор цієї статті[7]. Водночас стрімкий розвиток комп'ютерної техніки та сфери її використання, трансформація практичних проявів кримінальних правопорушень у сфері використання інформаційних технологій роблять актуальним продовження дослідження зазначеної проблематики. Важливим аспектом тут є дослідження практики протидії «комп'ютерним» кримінальним правопорушенням.

Метою статті є оцінка поточного стану протидії кримінальним правопорушенням, передбаченим статтями 361–363[1] КК, на основі дослідження відкритих даних офіційної статистики та аналізу судових рішень, представлених у Єдиному державному реєстрі судових рішень.

Виклад основного матеріалу дослідження. Дані офіційної статистики[8] за останні одинадцять років (2013-2023) свідчать про те, що кількість проваджень, облікованих за ознаками кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК, зросла від половини тисячі до майже чотирьох тисяч на рік, тоді як кількість засуджених осіб змінилася від 49 до 95 на рік (рис. 1).

Розподіл кількості облікованих проваджень та кількості засуджених осіб (таблиця 1) свідчить, що найбільш поширеним «комп'ютерним» кримінальним правопорушенням є несанкціоноване втручання (ст. 361 КК). Із цим кримінальним правопорушенням пов'язана понад половина (54%) облікованих проваджень. Більше половини (53,3%) засуджених за кримінальні правопорушення, передбачені Розділом XVI, вчинили несанкціоноване втручання. Другими за поширеністю є несанкціоновані дії, вчинені особою, яка має право доступу до комп'ютерної інформації (ст. 362) (38,1% проваджень та 20,1% засуджених). Статистично значимими та майже рівними є показники, що характеризують незаконні дії зі шкідливими програмними або технічними засобами (ст. 361[1] КК) та незаконні збут або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361[2] КК) (3,9–3,5% проваджень та 12,9–12,5% засуджених).

Певну специфіку мають використані судами засоби кримінально-правового реагування. Реальні покарання у випадках засудження за досліджувані кримінальні правопорушення застосовувалися у 50% випадків. Тоді як середній показник використання репресивної форми реалізації кримінальної відповідальності складає 58%. Як правило, за «комп'ютерні» кримінальні правопорушення суди призначали штраф (75%). Позбавлення волі призначалося кожному п'ятому засудженому (21%). Порівняння цих показників із практикою призначення покарань у зазначений період за всі кримінальні правопорушення також свідчить, що до «комп'ютерних» злочинців судді ставилися більш поблажливо. За період з 2013 по 2023 рр. серед засуджених за всі кримінальні правопорушення штраф було призначено 39%, позбавлення волі – 36%. Тож до осіб, які вчинили «комп'ютерні» кримінальні правопорушення, судді застосовували в цілому менш суворі засоби кримінально-правового реагування.

---

[1] Міхайліна ТВ, '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, Київський національний університет внутрішніх справ, 2011) 20.

[2] Музика АА та Азаров ДС, *Законодавство України про відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення* (Паливода А. В., 2005) 120.

[3] Плугатир МВ, 'Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації' (автореф. дис. … канд. юрид. наук, Київський національний університет внутрішніх справ, 2010) 18.

[4] Орлов СО, 'Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах' (дис. … канд. юрид. наук, Національний університет внутрішніх справ, 2004) 213.

[5] Розенфельд НА, 'Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж' (дис. … канд. юрид. наук, Інститут держави і права ім. В. М. Корецького, 2003) 222; Савінова НА, *Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти* (ТОВ «ДКС», 2012) 340.

[6] Рудик МВ, 'Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом' (дис. … канд. юрид. наук, Національний університет «Одеська юридична академія», 2007) 229.

[7] Карчевський МВ, *Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж* (РВВ ЛАВС, 2002) 144; Карчевський МВ, *Кримінально-правова охорона інформаційної безпеки України* (РВВ ЛАВС, 2012) 528.

[8] Тут і далі для роботи з даними офіційної статистики протидії злочинності нами було використано довідник «Протидія злочинності в Україні: інфографіка» представлений у відкритому доступі на аналітичній платформі CrimeDataLab (Карчевський М, *Протидія злочинності в Україні : інфографіка (2013-2024)* (CrimeDataLab, 2024) https://karchevskiy.com/i-dovidnyk/). Даний ресурс інтегрує статистичні звіти форми 1 та 2 Офісу Генерального Прокурора України та форми 6 та 7 Державної судової адміністрації України.

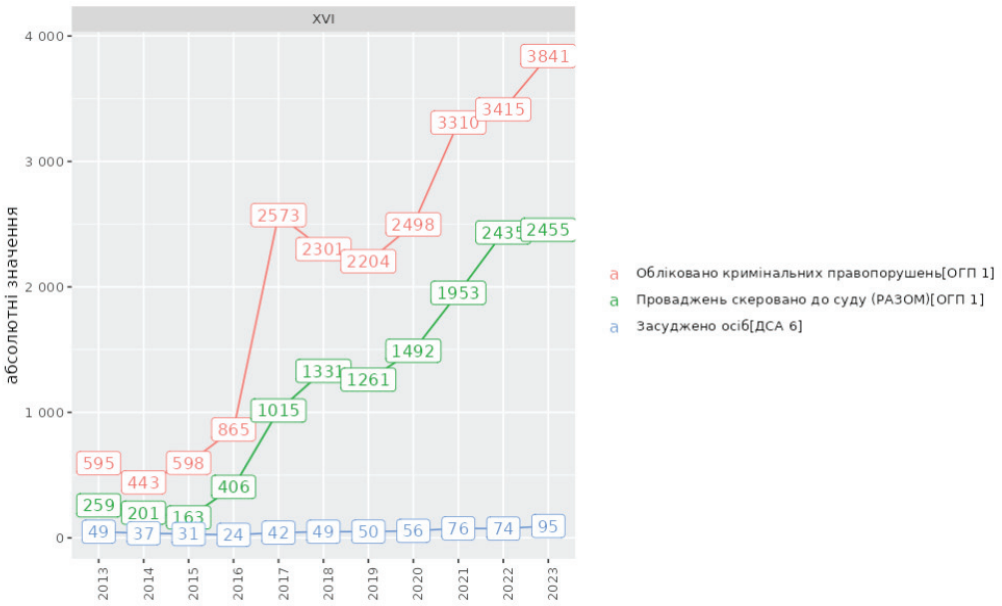

Рис. 1. Розподіл основних показників протидії кримінальним правопорушенням, передбаченим Розділом XVI Особливої частини КК

Таблиця 1.

Розподіл облікованих проваджень та кількості засуджених осіб за статтями Розділу XVI КК України (2013–2023 рр.)

Стаття КК	Кількість облікованих проваджень та частка серед всіх облікованих	Кількість засуджених осіб та частка серед всіх засуджених
Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	12 221 (54%)	311 (53,3%)
Стаття 361[1]. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут	882 (3,9%)	75 (12,9%)
Стаття 361[2]. 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	788 (3,5%)	73 (12,5%)
Стаття 362. 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	8 619 (38,1%)	117 (20,1%)
Стаття 363. 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	97 (0,4%)	1 (0,2%)
Стаття 363[1]. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку	36 (0,2%)	6 (1%)
Разом	22643	583

Для подальшого аналізу судової практики нами було сформовано запит до Єдиного державного реєстру судових рішень за такими параметрами: форма судового рішення – вирок; форма судочинства – кримінальне; категорія справи – кримінальні справи / кримінальні правопорушення в сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку/ час постановлення вироку – починаючи з 01.01.2022 р. На підставі такого запиту було отримано добірку з 244 судових рішень.

Серед отриманих судових рішень достатньо значною є частина виправдувальних рішень (4,5%). Відповідно до статистичної звітності Державної судової адміністрації середня частка виправданих серед осіб, вироки (постанови) щодо яких набрали чинності, складає 0,2%. Отже, значення цього показника в отриманій добірці судових рішень істотно відрізняється від загальних тенденцій. Дослідження змісту таких судових рішень дозволяє дійти висновку про те, що практика протидії «комп'ютерним» кримінальним правопорушенням проходить етап формування, не є сталою та розвивається під постійним впливом оновлення інформаційних технологій. Судді звертали увагу на недостаню якість формулювання обвинувачення: «суд вважає формулювання вказаного обвинувачення неконкретним та таким, що позбавляє обвинуваченого можливості розуміти його суть і відповідно захищатися від нього»[1]. Так само фіксували недостатню якість доказової бази[2]. Та з рештою, як правило, доходили висновку про те, що «стороною обвинувачення не доведено належними та достатніми доказами вчинення обвинуваченим кримінального правопорушення»[3].

Наявність такого незначного за кількістю, але важливого для аналізу сегмента судових рішень у досліджуваній добірці висвітлює кілька важливих моментів. Ефективність кримінально-правової протидії «комп'ютерним» правопорушенням потребує не лише якісного законодавства та кваліфікованих суб'єктів його застосування. Швидкість оновлення інформаційних технологій потребує постійної актуалізації професійних компетенцій працівників правоохоронних та судових органів.

Те, що «сьогодні» здається екзотикою, «завтра» перетворюється на поширену соціальну практику та, враховуючи «гнучкість» сучасної злочинності, використовується для вчинення кримінальних правопорушень. Ще 5–7 років тому використання віртуальних активів для здійснення оперативної закупки сприймалося дуже обережно, однак сьогодні це достатньо стала практика. Зараз ми досліджуємо нові можливості штучного інтелекту. Уявляється, за кілька років судова практика буде реагувати на випадки несанкціонованого втручання у роботу комп'ютерних мереж із використанням згенерованих системами штучного інтелекту шкідливих програмних засобів або давати оцінку використанню індивідуалізованих діпфейків для вчинення шахрайства, що охоплює десятки тисяч потерпілих. Назвемо цю особливість кримінально-правової протидії досліджуваним посяганням як високий рівень залежності ефективності від актуалізації професійних компетенцій працівників правоохоронних та судових органів.

Також дослідження показало, що «комп'ютерні» кримінальні правопорушення можна класифікувати за трьома рівнями поширеності.

Правопорушення високої поширеності (64%). До цієї групи належать правопорушення, що стосуються зміни даних особами, які мають право доступу до комп'ютерної інформації (23%), несанкціонованих транзакцій (22%), а також розповсюдження або збуту комп'ютерної інформації з обмеженим доступом (19%).

Правопорушення середньої поширеності (25%). Сюди входять правопорушення, пов'язані з отриманням або використанням авторизаційних даних (9%), копіюванням інформації, що призвело до її витоку (6%), внесенням даних до реєстрів загальним суб'єктом (5%), а також розповсюдженням або збутом шкідливих програмних засобів (5%).

Правопорушення низької поширеності (11%). До цієї категорії віднесено решту кримінальних правопорушень у сфері використання інформаційних технологій.

Аналіз судової практики дозволив виявити серед кримінальних правопорушень у сфері використання інформаційних технологій дві основні групи за специфікою використовуваних засобів кримінально-правового реагування.

[1] Вирок Кіровського районного суду м. Кіровограда від 20.07.2022 року (справа № 404/2447/22). URL: https://reyestr.court.gov.ua/Review/105322891

[2] Вирок Бучацького районного суду Тернопільської області від 28.06.2023 року (справа № 595/671/21). URL: https://reyestr.court.gov.ua/Review/111824835

[3] Вирок Жовтневого районного суду м. Запоріжжя від 27.10.2023 року (справа № 331/814/21). URL: https://reyestr.court.gov.ua/Review/115096847

Перша група характеризується переважним використанням реальних покарань (67–69%) у виді штрафів та частим укладанням угод про визнання винуватості (69–79%). Ця група охоплює правопорушення, передбачені статтями 361^1 та 361^2 КК України, та складає 27,6% від загальної кількості обвинувальних вироків.

Друга група відзначається більш широким використанням звільнення від покарання (63–68%) та меншою частотою укладання угод про визнання винуватості (37–54%). Ця група охоплює правопорушення, передбачені статтями 361 та 362 КК України, і становить 72% від загальної кількості обвинувальних вироків.

Встановлено, що однією з найбільш важливих проблем протидії «комп'ютерним» кримінальним правопорушенням є примітивізація. Аналіз судової практики показує, що у поле зору кримінальної юстиції переважно потрапляють найпростіші та найменш небезпечні форми комп'ютерних злочинів, які часто є лише допоміжними засобами для вчинення інших правопорушень, таких як шахрайство або крадіжка. Це свідчить про недостатню ефективність сучасної системи кримінально-правового реагування, яка не завжди встигає адекватно реагувати на більш складні та технологічно витончені форми комп'ютерних злочинів. Примітивізація підходів у правозастосуванні може призвести до того, що значні соціальні ресурси будуть спрямовані на боротьбу з менш небезпечними проявами злочинності, тоді як більш серйозні кіберзагрози залишаються без належної уваги. Ця тенденція вимагає переосмислення існуючих підходів до кримінально-правового регулювання у сфері використання інформаційних технологій та вдосконалення правозастосовної практики для підвищення ефективності протидії реальним загрозам кібербезпеки.

Саме примітивізацією може бути пояснена проблема тисяч матеріалів, надісланих до національних судів з обвинуваченням осіб у вчиненні кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК, та всього лише близько сотні засуджених (рис 1). Причина в особливостях статистичного обліку, який здійснює Державна судова адміністрація України (ДСА). Судові рішення фіксуються у звітах за найтяжчим обвинуваченням. Можливо, звинувачення в незаконних діях з інформаційними технологіями у переважній більшості супроводжуються звинуваченнями в більш серйозних злочинах (шахрайство, вимагання тощо). Тому в статистичних звітах Офісу Генерального Прокурора відповідні обвинувальні матеріали фіксуються, а в звітах ДСА – ні. Така гіпотеза потребує подальшої перевірки, але якщо вона підтвердиться, цілком слушним буде провокаційне, на перший погляд, запитання: «Може настав час замислитися, чи існують насправді «комп'ютерні» злочини?». Якщо переважна більшість випадків супроводжується звинуваченням у вчиненні більш тяжких кримінальних правопорушень, якщо «самостійні» звинувачення характеризуються переважно звільненням від покарання та застосуванням штрафів, чи не буде правильним розглядати «комп'ютерні» кримінальні правопорушення просто як спосіб старої, добре відомої крадіжки або вимагання чи шахрайства? Зрозуміло, порушені питання потребують самостійного дослідження, однак їх актуальність є значною, особливо в контексті проблеми ефективного використання соціальних ресурсів для протидії злочинності

Розв'язання проблеми примітивізації протидії «комп'ютерним» кримінальним правопорушенням визначає кілька перспективних напрямів вдосконалення законодавства: встановлення чітких критеріїв суспільної небезпечності; заміна складних переліків технічних засобів більш узагальненим поняттям «комп'ютерна система»; перегляд та оптимізація норм щодо інформації з обмеженим доступом.

Наприкінці зауважимо, що примітивізація – не єдина проблема протидії «комп'ютерним» кримінальним правопорушенням. До інших масштабних проблем, що у сукупності, на нашу думку, представляють собою достатньо повне розуміння протидії досліджуваним кримінальним правопорушенням в Україні, належать: 1) недостатня готовність законодавства та органів кримінальної юстиції до протидії злочинному використанню віртуальних активів і технологій штучного інтелекту; 2) формування єдиного міжнародного правового простору, що є критично важливим для ефективної протидії «комп'ютерним» злочинам, які не обмежуються територіальними кордонами.

Дослідження статистичних даних із необхідністю потребує ще одного важливого уточнення. Так, не можна не відзначити, що предметом подібного аналізу стали тільки зареєстровані «комп'ютерні» кримінальні правопорушення. Вод-

ночас на рівні монографічних досліджень доведена надзвичайна латентність таких посягань[1]. Susann W. Brenner відзначає, що правоохоронні органи сьогодні не мають достатніх відомостей про стан кіберзлочинності, а також про використовувані злочинцями моделі вчинення злочинів. Це негативно позначається на ефективності розподілу ресурсів та значно зменшує результативність правоохоронної діяльності[2]. Kristin Finklea та Catherine Theohary звертають увагу на відсутність вичерпних даних про кіберзлочинність і, відповідно, неможливість оцінити ступінь її загрози[3]. У свою чергу, Bruce Schneier стверджує, що дійсна небезпека цієї групи злочинів ігнорується, а реальний масштаб кіберзлочинності залишається невідомим[4].

Висновок. Проведений нами аналіз даних офіційної статистики та змісту судових рішень дає достатньо повне уявлення про діяльність правоохоронних і судових органів щодо протидії злочинності в сфері використання інформаційних технологій. Водночас проблема латентності «комп'ютерних» кримінальних правопорушень, реального масштабу та фактичної поширеності посягань на кібербезпеку в Україні дійсно потребує самостійного аналізу.

Комплексне розв'язання проблем примітивізації, готовності до використання нових технологій зі злочинною метою, формування єдиного міжнародно-правового простору протидії «комп'ютерним» кримінальним правопорушенням та оцінки дійсного масштабу суспільно небезпечних посягань у сфері використання інформаційних технологій в Україні дозволить забезпечити мінімізацію негативних наслідків інформатизації та створити умови для максимально ефективного використання інформаційних технологій.

[1] Yar M, *Cybercrime and society* (SAGE Publications Ltd, 2006) <https://doi.org/10.4135/9781446212196>; Williams M, *Virtually Criminal: Crime, Deviance and Regulation Online* (Routledge, 2006); Wall D, '*Cybercrime: The Transformation of Crime in the Information Age*' (Polity, 2007) 17–19; McCusker R, 'E-commerce, business and crime: Inextricably linked, diametrically opposed' *The Company Lawyer* (2002) 23 (1) 3–8; Gragido W and Pirc J, '*Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*' (Syngress, 2011) 272; Pittaro M, 'Cyber Stalking Typology, Etiology, and Victims' in Jaishankar K (ed) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (CRC Press, Taylor & Francis Group, 2011) 279–280; Jupp V, 'Hidden crimes' in McLaughlin E and Muncie J (eds) *The Sage Dictionary of Criminology*, *Third Edition* (Sage Publications, 2013) 220; Kunz M and Wilson P, *Computer Crime and Computer Fraud* (Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland 2004) 146 <www.academia.edu/8901471/Report_to_the_Montgomery_County_Criminal_Justice_Coordinating_Commission>.

[2] Brenner S, '*Cybercrime : criminal threats from cyberspace'* (Praeger, 2006) 271

[3] Finklea K and Theohary C, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement* (CRS Report for Congress, 15 January 2015) <http://www.fas.org/sgp/crs/misc/R42547.pdf>

[4] Eugene Chow 'Attackers have advantage in cyberspace, says cybersecurity expert' (*Homeland Security News Wire*, August 12, 2011) <http://www.homelandsecuritynewswire.com/attackers-have-advantage-cyberspace-says-cybersecurity-expert>

REFERENCES

List of legal documents

Cases

1. Vyrok Kirovskoho raionnoho sudu m. Kirovohrada vid 20.07.2022 roku (sprava № 404/2447/22). URL: https://reyestr.court.gov.ua/Review/105322891
2. Vyrok Buchatskoho raionnoho sudu Ternopilskoi oblasti vid 28.06.2023 roku (sprava № 595/671/21). URL: https://reyestr.court.gov.ua/Review/111824835
3. Vyrok Zhovtnevoho raionnoho sudu m. Zaporizhzhia vid 27.10.2023 roku (sprava № 331/814/21). URL: https://reyestr.court.gov.ua/Review/115096847

Bibliography

Authored books

1. Brenner S, *Cybercrime : criminal threats from cyberspace* (Praeger, 2006) 271
2. Gragido W and Pirc J, *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats* (Syngress, 2011) 272 (in English).
3. Wall D, *Cybercrime: The Transformation of Crime in the Information Age* (Polity, 2007) 17–19 (in English).
4. Williams M, *Virtually Criminal: Crime, Deviance and Regulation Online* (Routledge, 2006) (in English).
5. Yar M, *Cybercrime and society* (SAGE Publications Ltd, 2006) <https://doi.org/10.4135/9781446212196> (in English).
6. Azarov DS*, Zlochyny u sferi kompiuternoi informatsii (kryminalno-pravove doslidzhennia)* [Crimes in the field of computer information (criminal law study)] (Atika, 2007)304 (in Ukrainian).
7. Brenner SW, *Cybercrime: Criminal Threats from Cyberspace* (Praeger, 2010) 283 <http://dx.doi.org/10.5040/9798400636554> (in English).

8. Butuzov VM, *Protydiia kompiuternii zlochynnosti v Ukraini (systemno-strukturnyi analiz)* [Counteraction to computer crime in Ukraine (systemic and structural analysis)] (KNT, 2010) 408 (in Ukrainian).
9. Holubiev VO, *Informatsiina bezpeka: problemy borotby z kiberzlochynamy* [Information security: problems of combating cybercrime] (HU «ZIDMU», 2003) 250 (in Ukrainian).
10. Karchevskyi MV, *Kryminalno-pravova okhorona informatsiinoi bezpeky Ukrainy* [Criminal Law Protection of Information Security of Ukraine] (RVV LAVS, 2012) 528 (in Ukrainian).
11. Karchevskyi MV, *Kryminalna vidpovidalnist za nezakonne vtruchannia v robotu elektronno-obchysliuvalnykh mashyn, system ta kompiuternykh merezh* [Criminal liability for unlawful interference with the operation of electronic computers, systems and computer networks] (RVV LAVS, 2002) 144 (in Ukrainian).
12. Muzyka AA and Azarov DS, *Zakonodavstvo Ukrainy pro vidpovidalnist za «kompiuterni» zlochyny: naukovo-praktychnyi komentar i shliakhy vdoskonalennia* [Legislation of Ukraine on liability for «computer» crimes: scientific and practical commentary and ways of improvement] (Palyvoda A. V., 2005) 120 (in Ukrainian).
13. Savinova NA, *Kryminalno-pravove zabezpechennia rozvytku informatsiinoho suspilstva v Ukraini: teoretychni ta praktychni aspekty* [Criminal Law Support for the Development of Information Society in Ukraine: Theoretical and Practical Aspects] (TOV «DKS», 2012) 340 (in Ukrainian).

Part of the books

14. Jupp V, 'Hidden crimes' in McLaughlin E and Muncie J (eds) *The Sage Dictionary of Criminology*, *Third Edition* (Sage Publications, 2013) 220 (in English).
15. Pittaro M, 'Cyber Stalking Typology, Etiology, and Victims' in Jaishankar K (ed) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (CRC Press, Taylor & Francis Group, 2011) 279–280 (in English).

Journal articles

16. McCusker R, 'E-commerce, business and crime: Inextricably linked, diametrically opposed' *The Company Lawyer* (2002) 23 (1) 3–8 (in English).
17. Andrushko PP, 'Komentar do rozdilu XVI «Zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system, kompiuternykh merezh i merezh elektrozviazku» Osoblyvoi chastyny Kryminalnoho kodeksu Ukrainy' [Commentary to Chapter XVI «Crimes in the sphere of use of electronic computers, systems, computer networks and telecommunication networks» of the Special Part of the Criminal Code of Ukraine' Legislation of Ukraine] *Zakonodavstvo Ukrainy Naukovo-praktychni komentari – Scientific and Practical Commentaries* (2006) (1) 32–54 (in Ukrainian).
18. Dromov S, 'Kompiuterna informatsiia yak predmet zlochynu, peredbachenoho st. 362 Kryminalnoho kodeksu Ukrainy' [Computer information as a subject of a crime under Article 362 of the Criminal Code of Ukraine] *Pidpryiemnytstvo, hospodarstvo i pravo – Entrepreneurship, Economy and Law* (2005) (4) 129–132 (in Ukrainian).
19. Dromov S and Rendel T, 'Nesanktsionovane znyshchennia informatsii yak forma obiektyvnoi storony skladu zlochynu, peredbachenoho st. 362 KK Ukrainy' [nauthorized destruction of information as a form of objective side of the crime under Article 362 of the Criminal Code of Ukraine] *Visnyk prokuratury – Bulletin of the Prosecutor's Office* (2006) (9) 90–94 (in Ukrainian).

Theses of the dissertation

20. Belskyi YuA, 'Kryminalna vidpovidalnist za nesanktsionovane vtruchannia v robotu elektronno-obchysliuvalnykh mashyn (kompiuteriv), avtomatyzovanykh system, kompiuternykh merezh chy merezh elektrozviazku' [Criminal liability for unauthorized interference with the operation of electronic computers, automated systems, computer networks or telecommunication networks] (PhD thesis, Natsionalna akademiia vnutrishnikh sprav – National Academy of Internal Affairs, 2017) 253 (in Ukrainian).
21. Kyrbiatiev OO, 'Kryminalna vidpovidalnist za stvorennia z metoiu vykorystannia, rozpovsiudzhennia abo zbutu shkidlyvykh prohramnykh chy tekhnichnykh zasobiv, a takozh yikh rozpovsiudzhennia abo zbut' [Criminal liability for the creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale] (PhD thesis, Klasychnyi pryvatnyi universytet – Classic Private University, 2015) 20 (in Ukrainian).
22. Kravtsova MO, 'Kiberzlochynnist: kryminolohichna kharakterystyka ta zapobihannia orhanamy vnutrishnikh sprav' [Cybercrime: Criminological Characterization and Prevention by Internal Affairs] (PhD thesis, Kharkivskyi natsionalnyi universytet vnutrishnikh sprav – Kharkiv National University of Internal Affairs, 2016) 16 (in Ukrainian).
23. Mikhailina TV, 'Kryminalna vidpovidalnist za stvorennia z metoiu vykorystannia, rozpovsiudzhennia abo zbutu shkidlyvykh prohramnykh chy tekhnichnykh zasobiv, a takozh yikh rozpovsiudzhennia abo zbut' [Criminal liability for the creation with the purpose of use, distribution or sale of malicious software or hardware, as well as their

distribution or sale] (PhD thesis, Kyivskyi natsionalnyi universytet vnutrishnikh sprav – Kyiv National University of Internal Affairs, 2011) 20 (in Ukrainian).
24. Orlov SO, 'Kryminalno-pravova okhorona informatsii v kompiuternykh systemakh ta telekomunikatsiinykh merezhakh [Criminal Law Protection of Information in Computer Systems and Telecommunication Networks] (PhD thesis, Natsionalnyi universytet vnutrishnikh sprav – National University of Internal Affairs, 2004) 213 (in Ukrainian).
25. Pluhatyr MV, 'Implementatsiia Ukrainoiu mizhnarodno-pravovykh zoboviazan shchodo vidpovidalnosti za zlochyny u sferi kompiuternoi informatsii' [Implementation by Ukraine of International Legal Obligations on Liability for Crimes in the Field of Computer Information] (PhD thesis, Kyivskyi natsionalnyi universytet vnutrishnikh sprav – Kyiv National University of Internal Affairs, 2010) 18 (in Ukrainian).
26. Rozenfeld NA, 'Kryminalno-pravova kharakterystyka nezakonnoho vtruchannia v robotu elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh' [Criminal Law Characteristics of Unlawful Interference with Electronic Computers, Systems and Computer Networks] (PhD thesis, V. M. Koretsky Institute of State and Law, 2003) 222 (in Ukrainian).
27. Rudyk MV, 'Nezakonnyi zbut, rozpovsiudzhennia kompiuternoi informatsii z obmezhenym dostupom'[Illegal sale, distribution of computer information with limited access] (PhD thesis, Natsionalnyi universytet «Odeska yurydychna akademiia» – National University «'Odesa Law Academy», 2007) 229 (in Ukrainian).

Websites

28. Eugene Chow 'Attackers have advantage in cyberspace, says cybersecurity expert' (*Homeland Security News Wire*, August 12, 2011) <http://www.homelandsecuritynewswire.com/attackers-have-advantage-cyberspace-says-cybersecurity-expert> (in English)

Reports

29. Finklea K and Theohary C, *Cybercrime: Conceptual Issues for Congress and U. S. Law Enforcement* (CRS Report for Congress, 15 January 2015) <http://www.fas.org/sgp/crs/misc/R42547.pdf> (in English)
30. Kunz M and Wilson P, *Computer Crime and Computer Fraud* (Report to the Montgomery County Criminal Justice Coordinating Commission, University of Maryland 2004) 146 <www.academia.edu/8901471/Report_to_the_Montgomery_County_Criminal_Justice_Coordinating_Commission> (in English)
31. Karchevskyi M, *Protydiia zlochynnosti v Ukraini : infohrafika (2013-2024)* [Countering crime in Ukraine: infographics (2013-2024)](CrimeDataLab, 2024) <https://karchevskiy.com/i-dovidnyk/> (in Ukrainian).

Карчевський М. В.
Практика протидії кримінальним правопорушенням у сфері використання інформаційних технологій

У статті на основі аналізу відкритих даних оцінюється поточний стан протидії кримінальним правопорушенням, відповідальність за які передбачена статтями 361–363[1] КК України. Залежно від рівня поширеності такі суспільно небезпечні діяння класифіковано на три види: високої, середньої та низької поширеності.

Установлено, що до осіб, які вчинили «комп'ютерні» кримінальні правопорушення, застосовуються порівняно менш суворі засоби кримінально-правового регулювання. При цьому за специфікою використання таких засобів кримінально карані діяння в сфері використання інформаційних технологій поділено на дві групи. До першої включено правопорушення, що характеризуються застосуванням штрафів та частим укладанням угод про визнання винуватості, до другої – такі, за які частіше використовується звільнення від покарання, і ті, щодо яких із меншою частотою укладаються угоди.

Зроблено висновок, що практика протидії такому виду злочинності проходить етап формування, не є сталою та розвивається під постійним впливом оновлення інформаційних технологій. Закцентовано увагу, що однією із найбільш важливих проблем у цьому аспекті є примітивізація. У зв'язку з цим запропоновано перспективні напрями вдосконалення законодавства: встановлення чітких критеріїв суспільної небезпечності; заміна складних переліків технічних засобів більш узагальненим поняттям «комп'ютерна система»; перегляд та оптимізація норм щодо інформації з обмеженим доступом.

***Ключові слова**: інформатизація, кіберзлочинність, «комп'ютерні» кримінальні правопорушення, примітивізація.*

Karchevskyi M. V.
The practice of counteraction to criminal offences in the sphere of information technology

Based on the analysis of open data, the article assesses the current state of the fight against crimes for which liability is provided by Articles 361-363-1 of the Criminal Code. Depending on the degree of prevalence, such socially dangerous acts are classified into three types: high, medium and low prevalence.

The author establishes that comparatively less severe means of criminal law regulation are applied to persons who have committed 'computer' criminal offences. At the same time, according to the specifics of the use of such means, criminal offences in the field of information technology use are divided into two groups. The first group includes offences characterised by fines and frequent plea bargaining, while the second group includes offences for which exemption from punishment is more often used and those for which plea bargaining is less frequent.

It is concluded that the practice of combating this type of crime is in the process of formation, is not sustainable and is developing under the constant influence of information technology updates. The author emphasises that one of the most important problems in this respect is primitivisation. In this regard, the author suggests promising areas for improvement of legislation, including the establishment of clear criteria of public danger; replacement of complex lists of technical means by a more generalized concept of «computer system»; revision and optimisation of the rules on restricted information.

Keywords: *informatisation, cybercrime, computer crime, primitivisation.*

Стаття надійшла до редакції:31.10.2024 р.
Прийнята до друку: 20.11.2024 р.