DOI: 10.31359/2079-6242-2022-46-41
УДК 343.2/.7:004.056 (477)

К. А. Новікова, кандидат юридичних наук, старший науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, асистент кафедри кримінального права Національного юридичного університету імені Ярослава Мудрого
ORCID: 0000-0001-8646-3441

ДЕЯКІ ПИТАННЯ КАРАНОСТІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ЗА КРИМІНАЛЬНИМ ЗАКОНОДАВСТВОМ УКРАЇНИ*

Постановка проблеми. Спеціальні інформаційні операції та кіберзлочини стали невід'ємною складовою сучасної війни. З початку повномасштабного вторгнення рф в Україну суттєво збільшилася кількість злочинних посягань на інформаційну безпеку нашої країни, що актуалізувало дослідження кримінальних правопорушень у цій сфері, метою яких є удосконалення кримінально-правового регулювання. Одним із напрямів таких досліджень стали питання караності кримінальних правопорушень проти інформаційної безпеки та ефективності передбачених кримінальним законодавством санкцій.

Аналіз останніх досліджень і публікацій. Сучасні загальнотеоретичні питання кримінально-правової пеналізації на доктринальному рівні досліджував Ю. А. Пономаренко[1]. Що ж стосується кримінальних правопорушень проти інформаційної безпеки, то окремі їх аспекти досліджували М. В. Карчевський[2], В. С. Батиргареєва[3] та деякі інші дослідники. Нормативно-правове забезпечення інформаційної безпеки в Україні опрацьовував О. В. Олійник[4]. Щодо правопорушень у сфері інформаційних відносин у міжнародно-правових актах писав О. Амелін[5]. Зарубіжний досвід вивчався у роботі І. П. Катеринчука[6].

Інформаційну безпеку як об'єкт посягання злочинів проти основ національної безпеки України досліджував В. В. Аніщук[7]. Питання інформації як знаряддя вчинення кримінального правопорушення вивчала Д. Прокоф'єва[8]. Окремі проблеми відповідальності за кримінальні правопорушення проти інформаційної безпеки в контексті проекту КК України досліджувала К. В. Юртаєва[9].

У цей самий час питання караності кримінальних правопорушень проти інформаційної безпеки досліджувались указаними науковцями лише частково. У зв'язку з цим на сьогодні бракує знань у цій сфері.

Таким чином, **метою статті** є визначення караності кримінальних правопорушень проти інформаційної безпеки держави.

* *Примітка.* Статтю виконано в межах фундаментальної теми «Теоретичні, законодавчі та правозастосовні проблеми кримінально-правової охорони інформаційної безпеки в Україні» (номер державної реєстрації 0121U114324).

[1] Пономаренко Ю А, *Загальна теорія визначення караності кримінальних правопорушень* (Право, 2020) 720

[2] Карчевський МВ, *Кримінально-правова охорона інформаційної безпеки України* (РВВ ЛуВДС ім. Е. О. Дідоренка 2012) 528.

[3] Батиргареєва ВС, 'Концептуальна модель захисту інформаційного простору України засобами кримінального права' (2020) 1(32) Інформація і право 110–119.

[4] Олійник ОВ, 'Нормативно-правове забезпечення інформаційної безпеки в Україні' (2012) 3 *Право і суспільство* 132–137.

[5] Амелін О, 'Злочини у сфері інформаційних відносин в міжнародно-правових актах' (2016) 2 Науковий часопис Національної академії прокуратури України 1–9.

[6] Катеринчук І П, 'Кримінальна відповідальність за злочини у сфері комп'ютерних технологій: досвід зарубіжних країн' (2016) 1 Південноукраїнський правничий часопис 7–10.

[7] Аніщук ВВ, 'Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України' (2023) 2(77) Науковий вісник Ужгородського національного університету 139–143.

[8] Прокоф'єва Д, 'Інформація як знаряддя вчинення злочину та злочини проти інформаційної безпеки' (2020) 1 Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні 31–36.

[9] Юртаєва К В 'Відповідальність за злочини та проступки проти інформаційної безпеки в проєкті КК України крізь призму принципу верховенства права' *Проєкт нового Кримінального кодексу України у вимірі верховенства права* (Право 21 вересня 2021) 164–166.

Виклад основного матеріалу. Загальновідомо, що належна кримінально-правова охорона будь-яких цінностей, у тому числі і таких цінностей, як інформаційна безпека, забезпечується лише тоді, коли створені й застосовані ефективні кримінально-правові засоби. Жодних сумнівів не виникає стосовно того, що основним кримінально-правовим засобом охорони суспільних цінностей є кримінальна відповідальність, головною складовою якої є покарання.

Традицією вітчизняного законодавства, як і законодавства більшості європейських держав, є встановлення конкретних видів і розмірів покарань за вчинення окремих кримінальних правопорушень у санкціях відповідних статей Особливої частини КК України. Таким чином, саме санкції статей Особливої частини КК і вміщують у собі основний зміст кримінально-правових засобів, за допомогою яких здійснюється охорона тих соціальних цінностей, на які посягають кримінальні правопорушення[1].

Перш ніж розпочати дослідження караності кримінальних правопорушень проти інформаційної безпеки держави, необхідно визначити, які склади кримінальних правопорушень посягають на зазначений об'єкт суспільних відносин.

У Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021, зазначено, що інформаційна безпека України – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом[2]. На підставі цього визначення можна зробити висновок, що інформаційна безпека держави є комплексним явищем, що включає в себе, зокрема, захист інформаційного простору держави від негативних інформаційних впливів, безпеку інформаційно-комунікаційних систем, в яких обробляється та зберігається інформація, а також захищеність суспільно важливої інформації з обмеженим доступом.

У чинному КК України відсутній окремий розділ, яким охоплюються кримінальні правопорушення проти інформаційної безпеки, що значно ускладнює виокремлення вичерпного переліку таких правопорушень. Однак наведене визначення інформаційної безпеки дає підстави вирізнити три групи кримінальних правопорушень, які посягають на інформаційну безпеку.

До ***першої групи*** належать кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Інформаційна безпека є родовим об'єктом цих правопорушень. Ця група включає всі кримінальні правопорушення, передбачені розділом XVI Особливої частини КК України: статті 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»), 361^1 («Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), 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»), 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»), 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») та 363^1 («Перешкоджання роботі електронно-обчислювальних

[1] Новікова К А, 'Деякі питання караності злочинів проти життя та здоров'я особи' (2016) 2 (7) *Вісник Асоціації кримінального права України* 187–201.

[2] Про Стратегію інформаційної безпеки: Указ Президента України Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року: *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку») КК України.

Слід відмітити, що зазначені правопорушення розглядатимуться як такі, що посягають на інформаційну безпеку держави, лише у тому випадку, якщо вони спрямовані на об'єкти критичної інфраструктури та інформаційно-телекомунікаційні системи, в яких обробляється суспільно важлива інформація з обмеженим доступом (наприклад, державна таємниця). Якщо ж об'єктом посягання буде приватна інформаційно-телекомунікаційна система, то відсутні підстави віднесення цих правопорушень до посягань на інформаційну безпеку саме держави.

До ***другої групи*** кримінальних правопорушень проти інформаційної безпеки належать правопорушення, що посягають на суспільні відносини у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави. Ця група включає такі склади кримінальних правопорушень, як: статті 111 («Державна зрада») – в частині шпигунства, 114 («Шпигунство»), 114^2 («Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану»), 328 («Розголошення державної таємниці»), 329 («Втрата документів, що містять державну таємницю»), 330 («Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни») – в частині інформації, зібраної у процесі контррозвідувальної діяльності та у сфері оборони країни, та 422 («Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості») КК України.

До ***третьої групи*** кримінальних правопорушень проти інформаційної безпеки держави належать ті, що посягають на інформаційний простір держави. Ця група включає такі склади кримінальних правопорушень, як: статті 109 («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади») – в частині публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, 110 («Посягання на територіальну цілісність і недоторканність України») – в частині публічних закликів чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України, 111^1 («Колабораційна діяльність»), а саме ч. 1 («Публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України»), ч. 3 («Здійснення громадянином України пропаганди у закладах освіти незалежно від типів та форм власності з метою сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України, а також дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти») та ч. 6 («Організація та проведення заходів політичного характеру, здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України, за відсутності ознак державної зради, активна участь у таких заходах») – в частині здійснення інформаційної діяльності у співпраці з державою-агресором, 436 («Пропаганда війни»), 436^1 («Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів») та 436^2 («Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників») КК України.

Як видно, кримінальні правопорушення проти інформаційної безпеки держави розміщені у низці розділів Особливої частини КК України («Злочини проти основ національної безпеки», «Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації», «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» «Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку»), але об'єднані таким об'єктом посягання, як інформаційна безпека.

Отже, визначившись із переліком кримінальних правопорушень проти інформаційної безпеки, перейду до аналізу їх караності.

Щодо *першої групи* досліджуваних правопорушень, то всього у розділі XVI («Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку») передбачено шість кримінальних правопорушень та п'ятнадцять санкцій у складах кримінальних правопорушень.

Серед них чотири санкції (26,7%) встановлено за проступок, сім (46,7%) – за нетяжкі злочини, дві (13,3%) – за тяжкі злочини і дві (13,3%) – за особливо тяжкі злочин. Дев'ять санкцій є альтернативними, шість – безальтернативні.

Штраф передбачено у восьми санкціях, виправні роботи – у двох, обмеження волі містять п'ять санкцій, позбавлення волі – одинадцять. Всі санкції є відносно визначеними. Дві санкції містять додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю, яке суд може застосувати або, навпаки, прийняти рішення щодо незастосовування (кумулятивні санкції з альтернативним покаранням), п'ять санкцій – позбавлення права обіймати певні посади або займатися певною діяльністю як безальтернативне покарання (кумулятивна санкція).

Для визначення практики застосування зазначених покарань проаналізована судова статистика за 2021 та 2022 рр.

Загальна кількість засуджених за ці кримінальні правопорушення у 2021 р. становить 76 осіб, тоді як у 2022 р. – 74 особи. Позбавлення волі у 2021 р. призначалось 8 разів, у тому числі у розмірах понад 1 рік до 2 років включно – 2, понад 2 роки до 3 років включно – 4, понад 3 роки до 5 років включно – 1, понад 5 років до 10 років включно – 1, обмеження волі – 3 рази, штраф – 26 разів. Крім того, 39 осіб було звільнено від відбування покарання з випробуванням. Додаткові покарання були призначені 17 разів (1 раз штраф, 16 – позбавлення права обіймати певні посади або займатися певною діяльністю). Цікаво, що суд призначав штраф як додаткове покарання за ч. 3 ст. 362 КК України, тоді як санкція за цією частиною статті не містить додаткового покарання у виді штрафу, що суперечить ч. 3 ст. 53 КК України.

У 2022 р. позбавлення волі призначалося 10 разів, у тому числі у розмірах понад 1 рік до 2 років включно – 1, понад 2 роки до 3 років включно – 7, понад 3 роки до 5 років включно – 2, обмеження волі – 2 рази, виправні роботи – 1 і штраф – 23 рази. Крім того, 38 осіб було звільнено від відбування покарання з випробуванням; 20 разів призначалося додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю.

Щодо *другої групи* кримінальних правопорушень проти інформаційної безпеки, то вона включає шість правопорушень та тринадцять санкцій у складах цих правопорушень[1]. Із них – сім санкцій (53,8%) встановлено за нетяжкі правопорушення, чотири – за тяжкі (30,8%) і дві (15,4%) – за особливо тяжкі правопорушення. Дванадцять санкцій є безальтернативними і лише одна санкція є альтернативно.

Позбавлення волі передбачено в усіх тринадцяти санкціях, обмеження волі – у двох санкціях. Всі санкції є відносно визначеними. Одна санкція містить конфіскацію майна як додаткове покарання, яке суд може застосувати або ні (кумулятивні санкції з альтернативним покаранням), три санкції містять альтернативні додаткові покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю. Одна санкція передбачає позбавлення права обіймати певні посади або займатися певною діяльністю як безальтернативне додаткове покарання.

Щодо практики застосування покарання за 2021 та 2022 рр., то можна сказати про таке. Загальна кількість засуджених за ці правопорушення

[1] При аналізі не досліджувалася державна зрада (ст. 111 КК України), у зв'язку з тим, що не всі форми об'єктивної сторони переважно посягають на інформаційну безпеку держави.

складає 3 особи у 2021 р., 33 – у 2022 р. При цьому у 2021 р. двом особам призначено штраф, а одна особа звільнена від відбування покарання з випробуванням. У 2022 році позбавлення волі призначалося 13 разів, у тому числі у розмірах понад 1 рік до 2 років включно 4 особам, понад 3 роки до 5 років включно так само 4 особам, понад 5 років до 10 років включно – 5 і штраф призначено 3 особам. Крім того, 16 осіб звільнено від відбування покарання з випробуванням, 1 особу звільнено з інших підстав.

Щодо *третьої групи* кримінальних правопорушень проти інформаційної безпеки, то вона включає п'ять правопорушень та дев'ять санкцій[1]. Із них 1 (11,1%) – за проступок, 6 (66,7%) – за нетяжкий злочин, 2 (22,2%) – за тяжкі злочини. Шість санкцій альтернативні, а 3 із них є безальтернативними.

Позбавлення волі міститься у 8 санкціях, обмеження волі – у 3, арешт – у 3, виправні роботи – у 3, позбавлення права обіймати певні посади або займатися певною діяльністю – у 1. Всі санкції є відносно визначеними. П'ять санкцій містять конфіскацію майна як додаткове покарання, яке суд може застосувати або ні (кумулятивні санкції з альтернативним покаранням). Одна санкція передбачає позбавлення права обіймати певні посади або займатися певною діяльністю як безальтернативне додаткове покарання.

Щодо практики застосування покарання за 2021 та 2022 рр., то можна сказати про таке. У 2021 р. за вказані кримінальні правопорушення було засуджено 14 осіб, а у 2022 р. – 373 особи. У 2021 році – п'ятьом особам призначений штраф, 9 осіб звільнені від відбування покарання з випробуванням.

У 2022 році довічне позбавлення волі застосовувалося 1 раз, позбавлення волі призначалося 23 рази, у тому числі у розмірах 1 рік – 2 рази, понад 1 рік до 2 років включно – 4, понад 2 роки до 3 років включно – 11, понад 3 роки до 5 років включно – 5, понад 5 років до 10 років включно – 1, обмеження волі – 3, арешт – 4, виправні роботи – 3, громадські роботи – 1, позбавлення права обіймати певні посади або займатися певною діяльністю – 133, і штраф – 10 разів, інші види – 1. Крім того, 208 осіб звільнені від відбування покарання з випробуванням. Додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю призначалося 1 раз, конфіскація майна – 4 рази.

Отже, кримінальні правопорушення проти інформаційної безпеки сумарно включають у себе 17 кримінальних правопорушень, які містять 37 санкцій у складах цих правопорушень. Серед яких: 5 проступків (13,5%), 20 нетяжких злочинів (54,1%), 8 тяжких (21,6%) і 4 особливо тяжких (10,8%). У 8 санкціях міститься штраф (21,6%), в 1 – позбавлення права обіймати певні посади або займатися певною діяльністю (2,7%), в 5 – виправні роботи (13,5%), в 3 – арешт (8,1%), в 10 – обмеження волі (27%) і в 32 – позбавлення волі (86,5%).

Проведене дослідження дозволило зробити такі **висновки:**

1. Кримінальні правопорушення проти інформаційної безпеки можна умовно поділити на три групи: кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361, 361^1, 361^2, 362, 363, 363^1 КК України); кримінальні правопорушення, що посягають на суспільні відносини у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави (статті 111 – у частині шпигунства, 114, 114^2, 328, 329, 330 – у частині інформації зібраної у процесі контррозвідувальної діяльності та у сфері оборони країни, та ст. 422 КК України); кримінальні правопорушення, спрямовані на інформаційний простір держави (статті 109 – у частині публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, 110 – в частині публічних закликів чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України, 111^1 (ч. 1, ч. 3 та ч. 6 – у частині здійснення інформаційної діяльності у співпраці з державою-агресором), 436, 436^1 та 436^2 КК України).

2. Зазначені правопорушення містять 37 санкцій, серед яких: 5 проступків (13,5%), 20 нетяжких злочинів (54,1%), 8 тяжких (21,6%) і 4 особливо тяжких (10,8%). Отже, переважно

[1] При аналізі не досліджувалося посягання на територіальну цілісність і недоторканність України, у зв'язку з тим, що неможливо окремо виокремити правопорушення проти інформаційної безпеки.

кримінальні правопорушення проти інформаційної безпеки є нетяжкими або тяжкими злочинами.

3. У санкціях цих правопорушень переважають позбавлення волі (86%), обмеження волі (27%) та штраф (21,6%).

REFERENCES

List of legal documents

Legislation

1. Pro Stratehiiu informatsiinoi bezpeky: Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku: Verkhovna Rada Ukrainy. Zakonodavstvo Ukrainy: of. vebsait. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

Bibliography

Authored books

1. Bytiak YuP, Barabash YuH and Baranova LM, *Problemy pravovoi vidpovidalnosti* [Problems of Legal Liability] (VIa Tatsii, AP Hetman and VI Borysova ed, Pravo 2014) 176 (in Ukrainian)
2. Karchevskyi MV, *Kryminalno-pravova okhorona informatsiinoi bezpeky Ukrainy* [Criminal law protection of information security in Ukraine] (RVV LuSIA im. E. O. Didorenka 2012) 528 (in Ukrainian)
3. Ponomarenko YuA, *Zahalna teoriia vyznachennia karanosti kryminalnykh pravoporushen* [General theory of determining the punishability of criminal offenses] (Pravo, 2020) (in Ukrainian)

Journal articles

4. Amelin O, 'Zlochyny u sferi informatsiinykh vidnosyn v mizhnarodno-pravovykh aktakh' [Crimes in the sphere of information relations in international legal acts] (2016) 2 Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy – Scientific Journal of the National Academy of Prosecutor's Office of Ukraine 1–9 (in Ukrainian)
5. Anishchuk VV, 'Informatsiina bezpeka yak ob'iekt posiahannia zlochyniv proty osnov natsionalnoi bezpeky Ukrainy' [Information security as an object of encroachment of crimes against the foundations of national security of Ukraine] (2023) 2(77) Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu – Scientific Bulletin of Uzhhorod National University 139–143 (in Ukrainian)
6. Batyrhareieva VS, 'Kontseptualna model zakhystu informatsiinoho prostoru Ukrainy zasobamy kryminalnoho prava' [Conceptual Model of Protection of the Information Space of Ukraine by Means of Criminal Law] (2020) 1(32) Informatsiia i pravo – Informatsiia i pravo 110–119 (in Ukrainian)
7. Katerynchuk IP, 'Kryminalna vidpovidalnist za zlochyny u sferi kompiuternykh tekhnolohii: dosvid zarubizhnykh krain' [Criminal liability for crimes in the field of computer technology: the experience of foreign countries] (2016) 1 Pivdennoukrainskyi pravnychyi chasopys – The South Ukrainian Law Journal 7–10 (in Ukrainian)
8. Novikova KA, 'Deiaki pytannia karanosti zlochyniv proty zhyttia ta zdorovia osoby' [Some issues of punishability of crimes against life and health of a person] (2016) 2 (7) Visnyk Asotsiatsii kryminalnoho prava Ukrainy – Herald of the Association of Criminal Law of Ukraine 187–201 (in Ukrainian)
9. Oliinyk OV, 'Normatyvno-pravove zabezpechennia informatsiinoi bezpeky v Ukraini' [Regulatory and Legal Support of Information Security in Ukraine] (2012) 3 Pravo i suspilstvo – Law and Society 132–137 (in Ukrainian)
10. Prokofieva D, 'Informatsiia yak znariaddia vchynennia zlochynu ta zlochyny proty informatsiinoi bezpeky' [Information as a tool for committing a crime and crimes against information security] (2020) 1 Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini – Legal, regulatory and metrological support of the information security system in Ukraine 31–36 (in Ukrainian)

Conference paper

11. Yurtaieva KV 'Vidpovidalnist za zlochyny ta prostupky proty informatsiinoi bezpeky v proiekti KK Ukrainy kriz pryzmu pryntsypu verkhovenstva prava' [Liability for crimes and misdemeanors against information security in the draft Criminal Code of Ukraine through the prism of the rule of law] *Proiekt novoho Kryminalnoho kodeksu Ukrainy u vymiri verkhovenstva prava – Draft of the new Criminal Code of Ukraine in the dimension of the rule of law* (Pravo 21 veresnia 2021) 164–166 (in Ukrainian)

Новікова К. А.

Питання караності кримінальних правопорушень проти інформаційної безпеки держави за кримінальним законодавством України

У статті розглядаються покарання за вчинення кримінальних правопорушень проти інформаційної безпеки. Встановлено, що кримінальні правопорушення проти інформаційної безпеки можна умовно поділити на три

групи: кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361, 361[1], 361[2], 362, 363, 363[1] КК України); кримінальні правопорушення, що посягають на суспільні відносини у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави (статті 111 – у частині шпигунства, 114, 114[2], 328, 329, 330 – у частині інформації, зібраної у процесі контррозвідувальної діяльності та у сфері оборони країни, та 422 КК України); кримінальні правопорушення, спрямовані на інформаційний простір держави (статті 109 – у частині публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, 110 – у частині публічних закликів чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України, 111[1] (ч. 1, ч. 3 та ч. 6 – у частині здійснення інформаційної діяльності у співпраці з державою-агресором), 436, 436[1] та 436[2] КК України). Зазначені правопорушення містять 37 санкцій, серед яких: 5 проступків (13,5%), 20 нетяжких злочинів (54,1%), 8 тяжких (21,6%) і 4 особливо тяжких (10,8%). Отже, переважно кримінальні правопорушення проти інформаційної безпеки є нетяжкими або тяжкими злочинами. У санкціях цих правопорушень переважають позбавлення волі (86%), обмеження волі (27%), штраф (21,6%). Досліджується практика застосування покарань за ці кримінальні правопорушення.

***Ключові слова**: кримінальне право, кримінальне законодавство, кримінальні правопорушення проти інформаційної безпеки, інформаційна безпека, караність, кримінальна відповідальність, покарання.*

Novikova K. A.

Issues of punishment of criminal offenses against information security of the state under the criminal legislation of Ukraine

The article deals with punishments for committing criminal offenses against information security. It was established that criminal offenses against information security can be conditionally divided into three groups: criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and telecommunications networks (Articles 361, 361[1], 361[2], 362, 363, 363[1] of the Criminal Code of Ukraine); criminal offenses encroaching on public relations in the sphere of protection of state secrets and other information that ensures the state's defense capability (Article 111 – in the part of espionage, 114, 114[2], 328, 329, 330 – in the part of information collected in the process counter-intelligence activities and in the field of defense of the country, and 422 of the Criminal Code of Ukraine); criminal offenses aimed at the information space of the state (art. 109 – in the part of public calls for violent change or overthrow of the constitutional order or for the seizure of state power, as well as the distribution of materials with calls for such actions, 110 – in the part of public calls or distribution materials with appeals to change the boundaries of the territory or the state border of Ukraine, 111[1] (part 1, part 3 and part 6 – in the part of information activities in cooperation with the aggressor state), 436, 436[1] and 436[2] Criminal Code of Ukraine). The specified offenses include 37 sanctions, including: 5 misdemeanors (13.5%), 20 minor crimes (54.1%), 8 serious (21.6%) and 4 particularly serious (10.8%). Therefore, mostly criminal offenses against information security are minor or serious crimes. Sanctions for these offenses are dominated by deprivation of liberty (86%), restriction of liberty (27%), and fines (21.6%). The practice of applying punishments for these criminal offenses is being studied.

***Key words**: criminal law, criminal legislation, criminal offenses against information security, information security, punishment, criminal liability, punishment.*

Стаття надійшла до редакції:25.10.2023 р.
Прийнята до друку: 20.11.2023 р.