УДК 343.3/.7
DOI https://doi.org/10.51989/NUL.2026.3.33

# ПРОБЛЕМНІ АСПЕКТИ ВІДМЕЖУВАННЯ ПЕРЕДАЧІ АБО ЗБИРАННЯ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ СЛУЖБОВУ ІНФОРМАЦІЮ, ЗІБРАНУ У ПРОЦЕСІ ОПЕРАТИВНО-РОЗШУКОВОЇ, КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ, У СФЕРІ ОБОРОНИ КРАЇНИ, ВІД ІНШИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ПОСЯГАЮТЬ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

**Мелеховець Євгенія Костянтинівна,**
orcid.org/0009-0003-9398-7915
аспірант кафедри кримінального права
Національної академії внутрішніх справ

*Стаття присвячена порівняльному дослідженню передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни та низки інших кримінальних правопорушень, що посягають на інформаційну безпеку, зокрема, встановлений законом режим обігу інформації з обмеженим доступом, а також критеріям та проблемним аспектам їх розмежування в процесі кримінально-правової кваліфікації.*

*Серед іншого, проаналізовано теоретичні концепції суміжних складів кримінальних правопорушень та їх розмежування (відмежування), виокремлено основні ознаки складів кримінальних правопорушень, за якими зазвичай проводиться розмежування останніх. Досліджено поняття «інформаційна безпека» в законодавстві та науці кримінального права, та основні підходи представників доктрини до доцільності виділення кримінальних правопорушень, що посягають на інформаційну безпеку, конкретних складів кримінальних правопорушень, які до них віднесено, та варіантів їх класифікації.*

*Значну увагу приділено практичній складовій відмежування кримінального правопорушення, передбаченого статтею 330 КК України, від суміжних кримінальних правопорушень, що посягають на інформаційну безпеку – зокрема, державної зради (стаття 111), шпигунства (стаття 114), розголошення державної таємниці (стаття 328) та втрата документів, що становлять державну таємницю (стаття 329), розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (стаття 422), кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI), низки інших кримінальних правопорушень, предметом яких є інформація з обмеженим доступом. Виокремлено основні недоліки закону про кримінальну відповідальність в цій частині та сформульовано практичні рекомендації для правозастосовців.*

***Ключові слова:*** *національна безпека, інформаційна безпека, суміжні кримінальні правопорушення, службова інформація, державна таємниця, розмежування складів кримінальних правопорушень.*

## *Melekhovets Yevheniia. Problem Aspects of Distinguishing the Transmission or Collection of Official Information Obtained in the Process of Operational and Investigative Activities, Counterintelligence Activities, in the Sphere of National Defense, from other Criminal Offenses Against Information Security*

*The article presents a comparative study regarding the transmission or collection of data constituting official information – specifically information obtained during operational-investigative and counter-intelligence activities or within the sphere of national defense – and a range of other criminal offenses that infringe upon information security (particularly the statutory regime governing the handling of restricted-access information), as well as*

*the criteria and problematic aspects involved in distinguishing between them for the purposes of criminal law qualification.*

*Among other things, the study analyzes theoretical concepts regarding related criminal offenses and the criteria for distinguishing between them, identifying the key elements used to differentiate these offenses. It examines the concept of «information security» within legislation and criminal law scholarship, as well as prevailing doctrinal views on the advisability of categorizing offenses that infringe upon information security, the specific offenses included in this category, and various classification approaches.*

*Significant attention is paid to the practical aspects of distinguishing the criminal offense provided for in Article 330 of the Criminal Code of Ukraine from related criminal offenses infringing upon information security – specifically, high treason (Article 111), espionage (Article 114), disclosure of state secrets (Article 328) and loss of documents constituting state secrets (Article 329), disclosure of military information constituting state secrets or loss of documents or materials containing such information (Article 422), criminal offenses involving the use of electronic computing machines (computers), systems, computer networks, and telecommunications networks (Section XVI), as well as a number of other criminal offenses involving restricted-access information. The main shortcomings of the law on criminal liability in this regard are identified, and practical recommendations for law enforcement practitioners are formulated.*

***Key words:*** *national security, information security, related criminal offenses, official information, state secret, differentiation of the elements of criminal offenses.*

**Постановка проблеми.** Коректність кримінально-правової кваліфікації будь-якого діяння не в останню чергу залежить від вміння правильно розмежовувати між собою склади кримінальних правопорушень, наділених спільними ознаками, які в науці кримінального права іменуються суміжними. Так, з етимологічної точки зору слово «суміжний» в українській мові означає: 1) такий, який межує з ким-, чим-небудь, прилеглий до чогось; 2) розташований поруч, сусідній; 3) нерозривно пов'язаний з чим-небудь, близький до чогось; 4) має спільні ознаки з ким-, чим-небудь [1, с. 836]. Іншими словами, суміжними правовими категоріями вважаються ті, які є подібними між собою, близькими за змістом та наділені спільними ознаками [2, с. 2].

При цьому, як справедливо уточнює Л.П. Брич, у випадку із суміжними складами кримінальних правопорушень, їх диференціація є можливою лише за умови, що вони мають не лише певну кількість тотожних за змістом ознак, а і хоча б одну відмінну [3, с. 112]. Цю тезу уточнює В.О. Савченко, зауважуючи, що у вузькому розумінні суміжними є лише склади злочинів, які не просто характеризуються спільними ознаками, але й водночас містять протилежні взаємовиключні ознаки, які вказують на одні й ті самі характеристики складу злочину, проте набувають різного прояву [2, с. 6].

У випадку з кримінальним правопорушенням, передбаченим статтею 330 КК України, з огляду на громіздкість та складність його диспозиції, яка містить чимало обов'язкових ознак складу кримінального правопорушення, відмежування від суміжних кримінальних правопорушень набуває особливого значення та може бути викликом при правозастосуванні, що обумовлює актуальність даного дослідження.

**Аналіз останніх досліджень і публікацій.** Кримінальні правопорушення, що посягають на інформаційну безпеку загалом, та кримінальні правопорушення, що посягають на встановлений законом режим поводження з інформацією з обмеженим доступом зокрема, а також їх співвідношення та розмежування досліджувалось в окремих аспектах такими фахівцями, як В.І. Борисов, Л.П. Брич, Т.Ю. Вислоцька, М.М. Денисенко, М.В. Карчевський, О.О. Пащенко, В.О. Савченко, В.В. Сергійчук, М.І. Хавронюк та інші. Водночас, спеціалізованих досліджень, присвячених відмежуванню кримінального правопорушення, передбаченого статтею 330 КК України, від суміжних кримінальних правопорушень у сфері інформаційної безпеки, в науці кримінального права обмаль.

**Мета статті.** Метою статті є проведення порівняльного дослідження складу кримінального правопорушення, передбаченого статтею 330 КК України, та

суміжних з ним складів кримінальних правопорушень, що посягають на інформаційну безпеку, аналіз їх спільних та відмінних ознак, виявлення проблема їх розмежування на практиці та формулювання можливих шляхів їх подолання.

**Виклад основного матеріалу.** За загальною практикою в законі про кримінальну відповідальність суміжні склади кримінальних правопорушень здебільшого розташовані в межах одного розділу Особливої частини і почасти – в «сусідніх» статтях; водночас, досить поширеною є і практика поміщення, наприклад, спеціальних складів кримінального правопорушення у інших розділах, ніж загальний (зокрема, це характерно для посягань на життя та здоров'я або на власність, спеціальні склади яких, в залежності від предмета посягання (злочини проти власності) або потерпілого (злочини проти життя та здоров'я) передбачені одночасно в декількох різних розділах Особливої частини КК України.

У випадку з кримінальним правопорушенням, передбаченим статтею 330 КК України («Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни») ситуація є дещо нетиповою, оскільки розділ Особливої частини, в якому знаходиться зазначена стаття (Розділ XIV «Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації»), характеризується значною неоднорідністю об'єктів посягань, що, в свою чергу, призводить до того, що більшість статей відповідного розділу Особливої частини КК України мають замало спільних ознак, щоб говорити про суміжність з аналізованим нами в межах цієї статті складом кримінального правопорушення (за винятком лише очевидно суміжних з ним складів кримінальних правопорушень, передбачених статтями 328 та 329 КК України).

В той самий час, доволі значна кількість складів кримінальних правопорушень, поміщених в інші розділи Особливої частини КК України, мають одну чи декілька спільних ознак з правопорушенням, передбаченим статтею 330 – передусім це стосується прямо згаданих в диспозиції статті 330 державної зради та шпигунства (статті 111, 114), низки інших посягань на основи національної безпеки, посягань на встановлений законодавством режим обігу інших видів інформації з обмеженим доступом тощо.

З цього приводу слід відмітити, що в науці кримінального права досить часто критикується підхід законодавця до певною мірою штучного об'єднання складів кримінальних правопорушень з різними об'єктами посягань в межах Розділу XIV Особливої частини. Зокрема, з подібною критикою виступає Т.Ю. Вислоцька, яка називає таке розміщення норм не зовсім обґрунтованим і таким, що не враховує спільності об'єкта посягання кримінальних правопорушень, які хоч і передбачені в розділах I (статті 111, 114 тощо), XIV (статті 328, 329) та XIX (стаття 422) Особливої частини КК України, проте однаковою мірою посягають саме на національну безпеку України [4, с. 94–95].

В цьому контексті не можна не звернути увагу на таке поняття, яке чинним законодавством України визначається як складова національної безпеки України, як «інформаційна безпека», і, відповідно, на таку групу суміжних складів злочинів, як кримінальні правопорушення, що посягають на інформаційну безпеку. Так, в КК України термін «інформаційна безпека» вживається одного разу – в диспозиції статті 111 «Державна зрада», в якій остання визначається як «діяння, умисно вчинене громадянином України на шкоду […] обороноздатності, державній, економічній чи *інформаційній* безпеці України». В свою чергу, Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685, визначає інформаційну безпеку як «складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави […], за якого існує ефективна система захисту і протидії нанесенню шкоди через […] несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [5].

З огляду на зазначене, кримінальні посягання на встановлений законодавством порядок обігу державної таємниці та інших видів інформації з обмеженим доступом становлять загрозу інформаційній – а отже, і національній – безпеці. Відповідно, щонайменше через наявність спільного об'єкта кримінальні посягання в сфері обігу різних видів інформації з обмеженим доступом є здебільшого суміжними складами кримінальних правопорушень, а отже, підлягають розмежуванню.

Попри відсутність відповідного розділу в Особливій частині КК України, кримінальні правопорушення, що посягають на інформаційну безпеку, досить часто виділяються в окрему групу в науці кримінального права; при цьому коло таких правопорушень різні представники доктрини окреслюють по-різному. Так, подекуди розуміння кримінальних правопорушень проти інформаційної безпеки звужується лише до кримінальних правопорушень, предметом посягання яких є державна таємниця – тобто, державної зради (стаття 111) та шпигунства (стаття 114), розголошення та втрата державної таємниці (статті 328, 329), а також розголошення відомостей військового характеру, що становлять державну таємницю). Аргументом прихильників такого підходу є те, що інформаційна безпека в контексті статті 111 КК України, яка є єдиним випадком нормативного закріплення даного поняття на рівні закону України, означає захищеність України від витоку інформації, що складає державну таємницю [6, с. 257–258], і не поширюється на інші види інформації з обмеженим доступом, навіть якщо вони є чутливим для держави та суспільства.

Водночас, низка фахівців все ж відстоюють ширші підходи до інформаційної безпеки як об'єкта посягання. Так, зокрема, М.В. Карчевський відносить до кримінальних правопорушень, що посягають на інформаційну безпеку, відносить: весь розділ Особливої частини КК України, присвячений злочинам у сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку (статті 361 – 363-1 КК України); кримінальні правопорушення, які полягають в незаконному поводженні з різними видами інформації з обмеженим доступом (ст.ст. 111, 114, 132, 145, 159, 163, 168, 182, 231, 232, 328-330, 381, 387, 422 КК); в поданні неправдивої інформації або неповідомлення певної інформації (ст.ст. 218, 383, 384 КК); в посяганні на суспільні відносини у сфері формування інформаційного ресурсу: чч. 2, 3 ст. 109, ст.ст. 110, 161, 171, 258-2, 295, 300, 301 тощо. [7, с. 28–29].

В.І. Борисов та О.О. Пащенко, окрім кримінальних правопорушень, що посягають на інформаційну безпеку як складову національної безпеки, передбачених розділом 1 Особливої частини, включають до таких діянь також кримінальні правопорушення у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави (статті 328-330, 422 КК України); кримінальні правопорушення у сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку (розділ XVI Особливої частин КК України) та окрему групу кримінальних правопорушень, пов'язаних з інформаційною сферою, що посягають на мир, безпеку людства та міжнародний правопорядок (зокрема, пропаганда війни (стаття 436), ч. 2 ст. 442 КК України (в частині публічних закликів до геноциду), окремі діяння об'єктивної сторони кримінальних правопорушень, передбачених статтями 437 (злочин агресії) та 438 (воєнні злочини) [8].

Ще один варіант групування кримінальних правопорушень проти інформаційної безпеки пропонує М.М. Денисенко, класифікуючи їх на кримінальні правопорушення, які посягають на інформаційну безпеку держави або її органів (статті 111, 111-1, 114, 114-2; ч. 2 ст. 163; статті 328-330, 359, 387, 422, 436-2); кримінальні правопорушення, які посягають на інформаційну безпеку суспільства: (статті 161, 238, 300, 436-1); кримінальні правопорушення, які посягають на інформаційну безпеку людини або юридичних осіб приватного права: (статті 132, 145, 163, 168, 182, 231, 232, 232-2) та кримінальні правопорушення, які посягають на безпеку інформаційної технічної інфраструктури

або на достовірність інформації, що міститься на матеріальних носіях: (розділ XVI) [9, с. 13].

Не вдаючись в глибокий аналіз обґрунтованості тієї чи іншої з представлених вище класифікацій кримінальних правопорушень проти інформаційної безпеки, в межах нашого дослідження сконцентруємось на тих з них, які спрямовані саме на порушення встановленого законодавством режиму зберігання та поширення того чи іншого виду інформації з обмеженим доступом, оскільки, приміром, в складах кримінальних правопорушень, пов'язаних з поширенням закликів до геноциду, агресивної війни чи повалення конституційного ладу України інформація є скоріше засобом вчинення кримінального правопорушення, ніж предметом посягання, а отже, такі правопорушення не мають достатньої кількості спільних ознак з кримінальним правопорушенням, передбаченим статтею 330 КК України.

З-поміж суміжних з досліджуваним нами кримінальних правопорушень, що посягають на інформаційну безпеку, передусім слід відмежувати передачу або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, від державної зради та шпигунства, оскільки відповідні кримінальні правопорушення прямо згадані в диспозиції самої статті 330 КК України (що, до речі, є досить нетиповою для КК України правовою конструкцією).

Склади кримінальних правопорушень, передбачених статтями 114 та 330, та статтею 111 (в частині шпигунства) є очевидно суміжними, оскільки мають спільні ознаки об'єктивної сторони (діяння). Водночас, найбільш очевидним критерієм розмежування між ними є предмет кримінального правопорушення, яким в усіх трьох складах кримінальних правопорушень є інформація з обмеженим доступом, проте в статтях 111 та 114 – виключно відомості, що становлять державну таємницю, тоді як в ст. 330 – службова інформація чітко визначених в диспозиції зазначеної статті різновидів. Крім того, в якості додаткових критеріїв відмежування можна відзначити коло суб'єктів (в статті 330 суб'єкт є спеціальним, в статті 111 – загальний (будь-який громадянин України), в статті 114 – лише іноземець або особа без громадянства). Варто також відзначити, що мета зазначених діянь хоча і є близькою, проте не тотожною, оскільки основною метою вчинення державної зради, в тому числі у формі шпигунства, є завдання шкоди суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України, тоді як диспозиція статті 330 КК України такої спеціальної мети не містить.

Аналогічно передусім за предметом посягання відмежовуються від складу кримінального правопорушення, передбаченого статтею 330 КК України, кримінальні правопорушення, передбачені статтями 328, 329 та 422 КК України, оскільки в усіх трьох останніх предметом є відомості, що становлять державну таємницю. Водночас, окрім предмету, між зазначеними складами кримінальних правопорушень існують і інші відмінні ознаки. Зокрема, складам кримінальних правопорушень, передбачених статтями 328, 329 та 330 КК України, притаманні різні конструкції суб'єктивної сторони, а саме форми вини. Так, якщо діяння, передбачене статтею 330 КК України, може бути вчинено лише з прямим умислом, то втрата документів, що містять державну таємницю (стаття 329) може бути вчинено лише з необережності, а діяння, передбачене статтею 328 КК України, може мати змішану форму вини, а саме, умисел щодо діяння, а необережність щодо наслідку (наприклад, у випадках, коли розголошення відомостей, що становлять державну таємницю, сталось внаслідок умисного порушення умов зберігання вказаної інформації, і як наслідок, сталось необережне розголошення таких відомостей іншій особі, яка отримала доступ до неї) [10].

Ще дві розмежувальних ознаки між зазначеними трьома складами кримінальних правопорушень стосуються їх кваліфікованих складів. Так, першою з таких ознак є наслідки – адже на відміну від злочинів, передбачених ст. 328 і ст. 329 КК, у злочині, передбаченому ст. 330, згадано не загалом про тяжкі наслідки,

а про «тяжкі наслідки для інтересів держави» – отже, йдеться лише про випадки, коли в результаті розголошення відповідних відомостей саме державі в особі того чи іншого органу державної влади було заподіяно значної матеріальної шкоди чи шкоди організаційного характеру [6, с. 826]. Другою ж з таких ознак може виступати наявність у суб'єкта корисливого мотиву, яке передбачено в якості кваліфікуючої ознаки кримінального правопорушення, передбаченого статтею 330, проте не згадується як така в статтях 328 та 329 відповідно [10].

Всі наведені вище висновки щодо відмежування від кримінального правопорушення, передбаченого статтею 330 КК України, кримінальних правопорушень, передбачених статтями 328 та 329 КК України, рівною мірою стосуються і кримінального правопорушення, передбаченого статтею 422 КК України («Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості»), яке по суті повністю дублює диспозиції статей 328 та 329 КК України та є спеціальною відносно них, з єдиною відмінністю – в складі кримінального правопорушення, передбаченого у статті 422, спеціальним суб'єктом є військовослужбовець.

Ще одним складом кримінального правопорушення, який є суміжним з кримінальним правопорушенням, передбаченим статтею 330 КК України, є 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 (стаття 114-2 КК України). Так, зважаючи на те, що предметом зазначеного кримінального правопорушення є інформація у сфері оборони України, а саме інформація про направлення, переміщення зброї, озброєння та бойових припасів; про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, на практиці таку інформацію може бути доволі складно відрізнити від «відомостей, що становлять службову інформацію у сфері оборони країни», яка є предметом кримінального правопорушення, передбаченого статтею 330 КК України.

В даному випадку, на нашу думку, визначальним фактором має бути факт присвоєння відповідній інформації грифу «Для службового користування» (в разі відсутності в інформації оборонного характеру такого статусу її розголошення, за відповідності іншим вимогам, викладеним в диспозиціях частин 1, 2 статті 114-2 КК України, може бути кваліфіковано за відповідною частиною статті, і водночас однозначно не може кваліфікуватись за статтею 330 КК України) та факт наявності мети передачі такої інформації саме іноземній фізичній чи юридичній особі (на відміну від статті 330 КК України, в статті 114-2 КК України така мета не є обов'язковою ознакою). В якості додаткових критеріїв розмежування між зазначеними статтями можна також використовувати обстановку (кваліфікація за статтею 114-2 КК України можлива лише за умови вчинення передбаченого нею діяння в умовах воєнного або надзвичайного стану, тоді як для кваліфікації за статтею 330 КК України така умова не є обов'язковою) та ознаку спеціального суб'єкта (яка, на відміну від складу кримінального правопорушення, передбаченого статтею 330 КК України, у статті 114-2 КК України відсутня).

Менш проблематичним є відмежування кримінального правопорушення, передбаченого статтею 330 КК України, від діянь, що полягають в несанкціонованому збиранні та/або розголошенні інших видів інформації з обмеженим доступом (наприклад, лікарської, комерційної, банківської таємниць, інсайдерської інформації, професійної таємниці адвоката, таємниці усиновлення (удочеріння) тощо) – в такому випадку достатнім критерієм розмежування є предмет кримінального правопорушення, який доволі чітко відрізняється на практиці.

Певні труднощі при правозастосуванні може викликати відмежування від досліджуваного нами складу кримінальн-

ного правопорушення діяння, передбаченого статтею 387 КК України («Розголошення даних оперативно-розшукової діяльності, досудового розслідування»), предмет яких перетинається в частині інформації, створеної в процесі оперативно-розшукової діяльності (в статті 387 використано поняття «даних оперативно-розшукової діяльності»). Видається, що в даному випадку визначальною ознакою для кваліфікації відповідного діяння за статтею 387 КК України, як і у випадку з розмежуванням зі статтею 114-2 КК України, є факт відсутності грифу «Для службового користування», присвоєного відповідній інформації, а також відсутність мети передачі відповідної інформації іноземним фізичним та юридичним особам. Крім того, в порівнюваних складах кримінальних правопорушень також по-різному сформульовано ознаку спеціального суб'єкта, хоч на практиці «особи, яким така інформація була довірена або стала відома» частково перетинатимуться з колом суб'єктів, вказаних у статті 387 КК України, якими є судді, прокурори, слідчі, дізнавачі тощо, а також особи, яких було попереджено в установленому порядку про обов'язок не розголошувати такі дані.

На окрему увагу заслуговує питання відмежування кримінального правопорушення, передбаченого статтею 330 КК України, від так званих «комп'ютерних злочинів», передбачених розділом XVI, передусім – статтями 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») та 362 КК України («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»), зокрема, її ч. 2, яка передбачає кримінальну відповідальність за несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації.

Обидва вищезазначених склади кримінальних правопорушень мають суміжні ознаки з кримінальним правопорушенням, передбаченим статтею 330 КК України – зокрема, діяння, яке в статті 361-2 є різновидом передачі інформації, а в статті 362 – різновидом її збирання; крім того, предметом кримінального правопорушення, передбаченого статтею 361-2, також є інформація з обмеженим доступом, а в частині 2 статті 362 дещо подібним чином до диспозиції статті 330 визначено спеціального суб'єкта («особа, яка має право доступу до такої інформації»).

Зважаючи на наявність низки подібних ознак, відмежування зазначених складів кримінальних правопорушень від складу кримінального правопорушення, передбаченого статтею 330 КК України, на практиці може викликати певні труднощі. Як справедливо зазначає з цього приводу В.В. Денисенко, норми статей 361-2 та 362 КК фактично конкурують з усіма нормами, що охороняють ре жим обмеженого доступу до інформації (включаючи службову інформацію, яка є предметом кримінального правопорушення, передбаченого статтею 330 КК України), оскільки така інформація може бути розміщена на електронному носії. Така конкуренція норм обумовлюється в тому числі недоліками диспозицій статей розділу XIV Особливої частини КК України, які є, по-перше, надміру перевантаженими технічними термінами (до того ж досить застарілими станом на сьогодні, як приміром, «електронно-обчислювальна машина»), які ускладнюють кваліфікацію і в тому числі відмежування від суміжних кримінальних правопорушень, а по-друге, тим, що при визначенні предмета злочину за статтями 361-2 та 362 КК як критерій використано носій інформації, тоді як в інших розділах для визначення предмета використано зміст самої інформації або інші її характеристики. А оскільки ці критерії не є взаємовиключ-

ними - інформація, що становить предмет злочину, передбаченого ст. 330 КК, також може бути предметом злочину, передбаченого ст. 361-2 КК, оскільки може зберігатися в електронно-обчислювальних машинах [9, с. 15–16] – це робить фактично неможливим розмежування зазначених кримінальних правопорушень саме за предметом.

М.М. Денисенко пропонує все-таки проводити відмежування кримінальних правопорушень, передбачених статтями 361-2 та 362 КК України, від інших кримінальних правопорушень проти інформаційної безпеки, саме за предметом, пропонуючи відносити до предмету кримінальних правопорушень, передбачених зазначеними статтями, лише таку інформацію, яка не може існувати в іншому вигляді, ніж електронний, або не може бути використана інакше, ніж за допомогою комп'ютерів, як-то: програмне забезпечення, бази даних (їхні дампи), великі масиви персональних даних користувачів тощо [9, с. 15–16]. Однак така думка видається нам хибною, оскільки невиправдано звужує зміст зазначених статей закону про кримінальну відповідальність порівняно зі змістом, який вочевидь було закладено в них законодавцем.

Тому відмежування кримінальних правопорушень, передбачених статтями 361-2 та 362 КК України від кримінального правопорушення, передбаченого статтею 330 КК України, необхідно все ж проводити за іншими ознаками. Зокрема, обов'язковою ознакою суб'єктивної сторони кримінального правопорушення, передбаченого статтею 330 КК України, є мета передачі такої інформації іноземній фізичній чи юридичній особі, тоді як «комп'ютерні» злочини такої мети не мають [11]. Крім того, кримінальні правопорушення, передбачені статтями 361-2 та 330 відповідно, можуть також бути розмежовані за ознакою спеціального суб'єкта – перше із зазначених діянь може бути вчинено загальним суб'єктом, безвідносно того, в якому порядку такий суб'єкт отримав доступ до відповідної інформації.

**Висновки та рекомендації.** Таким чином, переважна більшість кримінальних правопорушень, які є суміжними з кримінальним правопорушенням, передбаченим статтею 330 КК України, можуть бути віднесені до умовної групи «кримінальних правопорушень, що посягають на інформаційну безпеку», яка, однак, не виділяється прямо законом про кримінальну відповідальність. Серед таких кримінальних правопорушень найбільш близькими до передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, є державна зрада (ст. 111), шпигунство (ст. 114), розголошення державної таємниці (ст. 328) та розголошення відомостей військового характеру, що становлять державну таємницю (ст. 422), основним критерієм відмежування яких від досліджуваного кримінального правопорушення є предмет посягання – державна таємниця та службова інформація відповідно. Також доволі непроблематичним на практиці є відмежування за предметом посягання від кримінальних правопорушень, предметом посягання в яких є інші види інформації з обмеженим доступом (зокрема, банківська, комерційна, професійна таємниці, інсайдерська інформація тощо).

Дещо складнішими на практиці є випадки відмежування суміжних кримінальних правопорушень від кримінального правопорушення, передбаченого статтею 330 КК України, за іншими ознаками – зокрема, метою та спеціальним суб'єктом, до яких правозастосовцям здебільшого доводиться звертатись у випадках, коли розмежування кримінальних правопорушень за предметом є неможливим (зокрема, у випадку з «комп'ютерними злочинами», які можуть стосуватись будь-яких видів інформації, розміщених на електронному носії), або ускладненим (зокрема, при відмежуванні від кримінальних правопорушень, передбачених статтею 387 КК України (предметом якої є дані оперативно-розшукової діяльності, що є подібним до «службової інформації, отриманої в процесі оперативно-розшукової діяльності») та статтею 114-2 КК України, предмет якої частково перетинається з «службовою

інформацією в сфері оборони країни». У випадках з останніми двома складами кримінальних правопорушень визначальним є факт наявності чи відсутності присвоєного відповідній інформації грифу «Для службового користування», проте не менше значення має також і наявність чи відсутність мети передачі такої інформації саме іноземним фізичним чи юридичним особам.

**ЛІТЕРАТУРА:**

1. Словник української мови : в 11 т. / [І. К. Білодід, А. А. Бурячок, В. О. Винник та ін.]. Київ : Наукова думка, 1970–1980. Т. IX : С. 1978. 916 с.

2. Савченко В. О. Суміжність складів злочинів у контексті ухилення від відбування покарання, не пов'язаного з позбавленням волі. URL: https://jes.nuoua.od.ua/archive/3_2016/24.pdf

3. Брич Л.П. Теорія розмежування складів злочинів: монографія / Л.П. Брич. – Львів: ЛДУВС, 2013. 712 с.

4. Вислоцька Т. Ю. Кримінально-правова охорона таємниці в Україні : дис. ... канд. юрид. наук: 12.00.08. Львів, 2017. 275 с.

5. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685. *Урядовий кур'єр* від 30.12.2021 № 251.

6. Науково-практичний коментар до Кримінального кодексу України: за ред. М.І. Мельника, М.І. Хавронюка. – 8-е вид., перероб. і доп. Х. : Фактор, 2011. 1280 с.

7. Кримінально-правова охорона інформаційної безпеки України: монограф. / М.В. Карчевський; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.

8. Кримінально-правова охорона інформаційної безпеки в Україні: монографія / [В. І. Борисов, О. О. Пащенко, Д. П. Євтєєва та ін.]; за заг. ред. В. І. Борисова, О. О. Пащенка; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2024. 328 с. DOI: https://doi.org/10.31359/9786178518899.

9. Денисенко М.М. (2025) Проблеми кримінально-правового забезпечення інформаційної безпеки людини, суспільства, держави. URL: https://journals.uran.ua/ispss/article/view/312694

10. Сергійчук В.В. Розмежування розголошення державної таємниці від суміжних злочинів за суб'єктивною стороною. URL: http://molodyvcheny.in.ua/files/conf/law/41dec2019/33.pdf

11. Карчевський М.В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (тези лекцій). URL: http://it-crime.at.ua/index/tezi_lekcij/0-31.

Дата першого надходження статті до видання: 26.06.2026
Дата прийняття статті до друку після рецензування: 18.07.2026
Дата публікації (оприлюднення) статті: 26.08.2026